

VA REQUEST
FOR LEASE
PROPOSALS
NO.

36C26221R0007
SAN DIEGO, CA

**Offers due
by
1/25/2021**

In order to be considered for award, offers conforming to the requirements of the RLP shall be received no later than **4:00 pm PST** on the date above. See "Receipt Of Lease Proposals" herein for additional information.

This Request for Lease Proposals ("RLP") sets forth instructions and requirements for proposals for a Lease described in the RLP documents. Proposals conforming to the RLP requirements will be evaluated in accordance with the Method of Award set forth herein to select an Offeror for award. The Government will award the Lease to the selected Offeror, subject to the conditions herein.

The information collection requirements contained in this Solicitation/Contract, that are not required by the regulation, have been approved by the Office of Management and Budget pursuant to the Paperwork Reduction Act and assigned the OMB Control No. 3090-0163.

**GLOBAL RLP
GSA TEMPLATE R100 (10/20)**

TABLE OF CONTENTS

GLOBAL RLP 1

SECTION 1 STATEMENT OF REQUIREMENTS 1

 1.01 GENERAL INFORMATION (OCT 2020) 1

 1.02 AMOUNT AND TYPE OF SPACE, LEASE TERM, AND OCCUPANCY DATE (OCT 2016)..... 1

 1.03 AREA OF CONSIDERATION (JUN 2012)..... 2

 1.04 NEIGHBORHOOD, PARKING, LOCATION AMENITIES, AND PUBLIC TRANSPORTATION (DEC 2015).....2

 1.05 LIST OF RLP DOCUMENTS (OCT 2020)..... 3

 1.06 AMENDMENTS TO THE RLP (JUN 2012)..... 3

 1.07 LEASE DESCRIPTION (OCT 2020) 3

 1.08 RELATIONSHIP OF RLP BUILDING MINIMUM REQUIREMENTS AND LEASE OBLIGATIONS (OCT 2016)4

 1.09 PRICING OF SECURITY REQUIREMENTS (OCT 2016) 4

 1.10 SECURITY LEVEL DETERMINATION FOR FACILITY HOUSING OTHER FEDERAL TENANTS (APR 2011)4

 1.11 INSPECTION—RIGHT OF ENTRY (JUN 2012)..... 4

 1.12 AUTHORIZED REPRESENTATIVES (OCT 2020) 5

 1.13 NORTH AMERICAN INDUSTRY CLASSIFICATION SYSTEM (NAICS) CODE AND SMALL BUSINESS SIZE
STANDARD (OCT 2020) 5

 1.14 UNIQUE ENTITY IDENTIFIER (OCT 2020) 5

SECTION 2 ELIGIBILITY AND PREFERENCES FOR AWARD 6

 2.01 EFFICIENCY OF LAYOUT (AUG 2011) 6

 2.02 FLOOD PLAINS (OCT 2017)..... 6

 2.03 SEISMIC SAFETY – HIGH SEISMICITY (OCT 2017)..... 6

 2.04 HISTORIC PREFERENCE (SEP 2013)..... 7

 2.05 ASBESTOS (JUN 2012) 8

 2.06 ACCESSIBILITY (SEP 2013) 8

 2.07 FIRE PROTECTION AND LIFE SAFETY (SEP 2013) 9

 2.08 ENERGY INDEPENDENCE AND SECURITY ACT (OCT 2016) 9

 2.09 ENVIRONMENTAL CONSIDERATIONS (SEP 2013)..... 10

SECTION 3 HOW TO OFFER 11

 3.01 GENERAL INSTRUCTIONS (JUN 2012)..... 11

 3.02 RECEIPT OF LEASE PROPOSALS (OCT 2020) 11

 3.03 PRICING TERMS (OCT 2020)..... 12

 3.04 BUDGET SCOREKEEPING; OPERATING LEASE TREATMENT (APR 2011)..... 13

 3.05 ADDITIONAL SUBMITTALS (OCT 2020)..... 13

3.06	TENANT IMPROVEMENTS INCLUDED IN OFFER (OCT 2020)	15
3.07	OPERATING COSTS REQUIREMENTS INCLUDED IN OFFER (JUN 2012)	16
SECTION 4	METHOD OF AWARD	17
4.01	NEGOTIATIONS (JUN 2012)	17
4.02	HUBZONE SMALL BUSINESS CONCERN ADDITIONAL PERFORMANCE REQUIREMENTS (SEP 2015)	17
4.03	AWARD BASED ON PRICE (JUN 2012)	17
4.04	PRESENT VALUE PRICE EVALUATION (OCT 2016)	17
4.05	AWARD (OCT 2018)	18
SECTION 5	ADDITIONAL TERMS AND CONDITIONS	20
5.01	MODIFIED RLP PARAGRAPHS (OCT 2016)	20

REQUEST FOR LEASE PROPOSALS NO. 36C26221R0007

1/25/2021
GLOBAL RLP GSA TEMPLATE R100 (OCT 2020)

SECTION 1 STATEMENT OF REQUIREMENTS

1.01 GENERAL INFORMATION (OCT 2020)

A. This Request for Lease Proposals (RLP) sets forth instructions and requirements for proposals for a Lease described in the RLP documents. The Government will evaluate proposals conforming to the RLP requirements in accordance with the Method of Award set forth below to select an Offeror for award. The Government will award the Lease to the selected Offeror, subject to the conditions below.

B. Included in the RLP documents is a lease template setting forth the lease term and other terms and conditions of the Lease contemplated by this RLP and a GSA Proposal to Lease Space (GSA Form 1364) on which Offeror shall submit its offered rent and other price data, together with required information and submissions. The Lease paragraph titled "Definitions and General Terms" shall apply to the terms of this RLP.

C. Do not attempt to complete the lease template. Upon selection for award, GSA will transcribe the successful Offeror's final offered rent and other price data included on the GSA Form 1364 into the lease and transmit the completed Lease, including any appropriate attachments, to the successful Offeror for execution. Neither the RLP nor any other part of an Offeror's proposal shall be part of the Lease except to the extent expressly incorporated therein. The Offeror should review the completed Lease for accuracy and consistency with his or her proposal, sign and date the first page, initial each subsequent page of the Lease, and return it to the Lease Contracting Officer (LCO).

D. The Offeror's executed Lease shall constitute a firm offer. No Lease shall be formed until the LCO executes the Lease and delivers a signed copy to the Offeror.

1.02 AMOUNT AND TYPE OF SPACE, LEASE TERM, AND OCCUPANCY DATE (OCT 2016)

A. The Government is seeking a minimum of **7,800** to a maximum of **10,213** of American National Standards Institute/Building Owners and Managers Association (ANSI/BOMA) Office Area (ABOA) square feet (SF) of contiguous space within the Area of Consideration set forth below. See Section 2 of the Lease for applicable ANSI/BOMA standards.

B. The Space shall be located in a modern quality Building of sound and substantial construction with a facade of stone, marble, brick, stainless steel, aluminum or other permanent materials in good condition and acceptable to the LCO. If not a new Building, the Space offered shall be in a Building that has undergone, or will complete by occupancy, modernization or adaptive reuse for the Space with modern conveniences.

C. The Government requires **00** structured/inside parking spaces and **80** surface/outside parking spaces, reserved for the exclusive use of the Government. These spaces must be secured and lit in accordance with the Security Requirements set forth in the Lease. Offeror shall include the cost of this parking as part of the rental consideration.

D. As part of the rental consideration, the Government may require use of part of the Building roof for the installation of antenna(s). If antenna space is required, specifications regarding the type of antenna(s) and mounting requirements are included in the agency requirements information provided with this RLP.

E. Approximately **00** ABOA SF will be used for the operation of a vending facility under the provisions of the Randolph-Sheppard Act (20 USC 107 et. seq.). The Government will control the number, kind, and locations of vending facilities and will control and receive income from all automatic vending machines. Offeror shall provide necessary utilities and make related alterations. The cost of the improvements is part of Tenant Improvement (TI) costs. The Government will not compete with other facilities having exclusive rights in the Building. The Offeror shall advise the Government if such rights exist.

E. The Government may provide vending machines within the Government's leased area under the provisions of the Randolph-Sheppard Act (20 USC 107 et. seq.). If the Government chooses to provide vending facilities, the Government will control the number, kind, and locations of vending facilities and will control and receive income from all automatic vending machines. Offeror shall provide necessary utilities and make related alterations. The cost of the improvements is part of Tenant Improvement (TI) costs. The Government will not compete with other facilities having exclusive rights in the Building. The Offeror shall advise the Government if such rights exist.

F. The lease term shall be up to **20** Years, **10** Years Firm, with Government termination rights, in whole or in parts, effective at any time after the Firm Term of the Lease by providing not less than **180** days' prior written notice. This Lease may be renewed at the option of the Government for **0, 0**-year terms. The Government reserves the right in the Lease to not include an option, or to reduce the length of an option, if inclusion of the option would cause the Lease to score as a capital lease, in accordance with the Budget

Scorekeeping: Operating Lease Treatment paragraph of this RLP. Should the Government make the determination to modify the term or option(s), an amendment to the RLP will be issued.

G. The Lease Term Commencement Date will be on or about **08-01-2021**, or upon acceptance of the Space, whichever is later.

1.03 AREA OF CONSIDERATION (JUN 2012)

The Government requests Space in an area bounded as follows:

- North: FWY 56
- South: I-8
- East: Camino Ruiz -> I-805 -> FWY 163 -> I-805 (refer to Delineated Area Map)
- West: Torrey Pine Rd -> La Jolla Blvd -> Mission Blvd -> Mission Bay Dr. (along the coast line)

Buildings that have frontage on the boundary streets are deemed to be within the delineated Area of Consideration.

1.04 NEIGHBORHOOD, PARKING, LOCATION AMENITIES, AND PUBLIC TRANSPORTATION (DEC 2015)

A. Neighborhood and Parking: Inside City Center:

Space shall be located in a prime commercial office district with attractive, prestigious, and professional surroundings with a prevalence of modern design and/or tasteful rehabilitation in modern use. Streets and public sidewalks shall be well maintained. The parking-to-square-foot ratio available on-site shall at least meet current local code requirements, or in the absence of a local code requirement, on-site parking shall be available at a ratio of one (1) space for every **165** RSF of Space.

B. Neighborhood and Parking: Outside City Center:

Space shall be located 1) in an office, research, technology, or business park that is modern in design with a campus-like atmosphere; or, 2) on an attractively landscaped site containing one or more modern office Buildings that are professional and prestigious in appearance with the surrounding development well maintained and in consonance with a professional image. The parking-to-square-foot ratio available on-site shall at least meet current local code requirements, or, in the absence of a local code requirement, on-site parking shall be available at a ratio of one (1) space for every **165** RSF of Space.

C. Walkability and Amenities:

1. Employee and visitor entrances of the Building must be connected to public sidewalks by continuous, accessible sidewalks.
2. A variety of employee services, such as restaurants, retail shops, cleaners, and banks, shall be located within the immediate vicinity of the Building. The primary functional entrance of the Building shall be within safely accessible, walkable 2,640 foot distance of at least **two (2)** instances of amenities, two of which must be inexpensive or moderately priced fast-food or eat-in restaurants. The remaining **zero (0)** instances must fall within at least 2 of the Diverse Use Categories shown below:

Diverse Use Category	Uses
Food Retail	Supermarket, Other food store with produce
Community-Serving Retail	Clothing store or department store selling clothes, Convenience store, Farmer's market, Hardware store, Pharmacy, Other retail
Services	Bank, Gym, Health club, Exercise studio, Hair care, Laundry, Dry cleaner, Restaurant, Café, Diner (excluding establishments with only drive-throughs)
Civic and Community Facilities	Adult or senior care (licensed), Child care (licensed), Community or recreation center, Cultural arts facility (museum, performing arts), Educational facility (including K-12 school, university, adult education center, vocational school, community college), Family entertainment venue (theater, sports), Government office that serves public on-site, Place of worship, Medical clinic or office that treats patients, Police or fire station, Post office, Public library, Public park, Social services center

To be considered, amenities must be accessible from the Building by continuous sidewalks, walkways, or pedestrian crosswalks. Amenities must be existing or the Offeror must demonstrate to the Government's reasonable satisfaction that such amenities will exist by the Government's required occupancy date.

D. Transit Accessibility: A subway, light rail, or bus rapid transit stop shall be located within the immediate vicinity of the Building, but generally not exceeding a safely accessible, walkable 2,640 feet from the principal functional entrance of the building, as determined by the LCO.

1.05 LIST OF RLP DOCUMENTS (OCT 2020)

A. The following documents are attached to and included as part of this RLP package:

DOCUMENT NAME	NO. OF PAGES	EXHIBIT
Lease No. 36C26221L0002 (Template L100)	43	A
Agency's Requirements	55	B
Security Requirements for Level 2	109	C
GSA Form 3516, Solicitation Provisions	5	D
GSA Form 3517B, General Clauses	15	E
Proposal to Lease Space (GSA Form 1364)	6	F
GSA Form 1217, Lessor's Annual Cost Statement	4	G
GSA Form 12000 for Prelease Fire Protection and Life Safety Evaluation for an Office Building (Part A or Part B) (See Section 3 for applicable requirements)	7	H
Seismic Offer Forms	10	I
Covered Telecommunications Equipment or Services Representation	1	J
ADA Certification	1	K
Pre Lease Building Security Plan	6	L
Safety Environmental Checklist	4	M
Infection Control Risk Assessment	10	N
Rate for Routine Cleaning and Disinfecting Requirements	1	O

B. In addition to the documents identified above, this RLP package includes additional agency requirements containing sensitive information that is only available to Offerors upon request to the LCO or Alternate Government Contact as listed under Section 1 of this RLP.

1.06 AMENDMENTS TO THE RLP (JUN 2012)

This RLP may be amended by notice from the LCO. Amendments may modify the terms of this RLP, or the terms, conditions, and requirements of the Lease contemplated by the RLP.

1.07 LEASE DESCRIPTION (OCT 2020)

A. Offeror shall examine the Lease template included in the RLP documents to understand the Government's and the Lessor's respective rights and responsibilities under the contemplated Lease.

B. The Lease contemplated by this RLP includes:

1. The term of the Lease, and renewal option, if any.
2. Terms and Conditions of the Lease, including Definitions, Standards, and Formulas applicable to the Lease and this RLP.
3. Building Shell standards and requirements.
4. Information concerning the tenant agency's buildout requirements, to be supplemented after award.
5. Security Requirements.
6. A description of all services to be provided by the Lessor.

C. Should the Offeror be awarded the Lease, the terms of the Lease shall be binding upon the Lessor without regard to any statements contained in this RLP.

D. The Lease contemplated by this RLP is a fully serviced, turnkey Lease with rent that covers all Lessor costs including all shell upgrades, TIs, operating costs, real estate taxes, and security upgrades. Rent will be based upon a proposed rental rate per rentable square foot (RSF), limited by the offered rate and the maximum ABOA SF solicited under this RLP. The Tenant Improvements to be delivered by the Lessor shall be based upon information provided with this RLP and Lease, including Agency Specific Requirements (ASR). The Lessor shall design and build the TIs and will be compensated for the TI costs based upon turnkey pricing established under the Lease. Offerors are encouraged to consider the use of existing fit-out and other improvements to minimize waste. However, any existing improvements must be equivalent to Lease requirements for new installation, and Offerors are cautioned to consider those requirements before assuming efficiencies in its TI costs resulting from use of existing improvements.

Offerors are required to prepare Design Intent Drawings (DIDs) prior to Lease Award. See Paragraph TURNKEY PRICING WITH DESIGN INTENT DRAWINGS PRIOR TO AWARD for further details.

E. The security pricing process is described in a separate paragraph.

F. Upon completion and acceptance of the leased Space, the Space will be measured for establishing the actual annual rent, and the lease term shall commence. During the term of the Lease, rent will be adjusted for changes to the Lessor's operating costs and real estate taxes, pursuant to paragraphs set forth in Section 2 of the Lease.

G. Offerors are advised that doing business with the Government carries special responsibilities with respect to sustainability, fire protection and life safety, and security, as well as other requirements not typically found in private commercial leases. These are set forth both in the lease template and in the GSA Form 3517B, which will be part of the Lease.

1.08 RELATIONSHIP OF RLP BUILDING MINIMUM REQUIREMENTS AND LEASE OBLIGATIONS (OCT 2016)

The Lease establishes various requirements relating to the Building shell. Such requirements are not deemed TIs. There are certain Building requirements that are established as minimum requirements in this RLP. If the Lessor's Building does not meet the requirements at the time of award, the Lessor may still be awarded the Lease. However, as a condition of award, the Government will require Lessor to identify those Building improvements that will bring the Building into compliance with RLP requirements. Upon award of the Lease, completion of those Building improvements will become Lease obligations.

1.09 PRICING OF SECURITY REQUIREMENTS (OCT 2016)

A. The proposed Lease contains an attachment with the security requirements and obligations for the Building, which are based on the facility security level (FSL). The Federal Government determines the facility's FSL rating, which ranges from FSL I to FSL IV. The FSL is based on client agency mix, required size of space, number of employees, use of the space, location, configuration of the site and lot, and public access into and around the facility.

B. The security requirements attached to this Lease includes a list of security countermeasures that must be installed in the leased Space. The Offeror shall use the Security Unit Price List to provide the Government with itemized costs of these security countermeasures, and he or she shall amortize the cost of any Building Specific Amortized Capital (BSAC) into the rent..

C. There shall be no charge to the Government for any items that already exist in the offered Building or facility.

1.10 SECURITY LEVEL DETERMINATION FOR FACILITY HOUSING OTHER FEDERAL TENANTS (APR 2011)

If an Offeror is offering Space in a facility currently housing a Federal agency, the security requirements of the facility may be increased and the Offeror may be required to adhere to a higher security standard than other Offerors competing for the same space requirement. If two or more Federal space requirements are being competed at the same time, an Offeror submitting on both or more space requirements may be subject to a higher security standard if the Offeror is determined to be the successful Offeror on more than one space requirement. It is incumbent upon the Offeror to prepare the Offeror's proposal accordingly.

1.11 INSPECTION—RIGHT OF ENTRY (JUN 2012)

A. At any time and from time to time after receipt of an offer (until the same has been duly withdrawn or rejected), the agents, employees and contractors of the Government may, upon reasonable prior notice to Offeror, enter upon the offered Space or the Premises, and all other areas of the Building access to which is necessary to accomplish the purposes of entry, to determine the potential or actual compliance by the Offeror with the requirements of the RLP and its attachments, which purposes shall include, but not be limited to:

1. Inspecting, sampling, and analyzing of suspected asbestos-containing materials and air monitoring for asbestos fibers.
2. Inspecting the heating, ventilation and air conditioning system, maintenance records, and mechanical rooms for the offered Space or the Premises.
3. Inspecting for any leaks, spills, or other potentially hazardous conditions which may involve tenant exposure to hazardous or toxic substances.
4. Inspecting for any current or past hazardous waste operations, to ensure that appropriate actions were taken to alleviate any environmentally unsound activities in accordance with Federal, state, and local law.

B. Nothing in this paragraph shall be construed to create a Government duty to inspect for toxic materials or to impose a higher standard of care on the Government than on other lessees. The purpose of this paragraph is to promote the ease with which the Government may inspect the Building. Nothing in this paragraph shall act to relieve the Offeror of any duty to inspect or liability which might arise because of Offeror's failure to inspect for or correct a hazardous condition.

1.12 AUTHORIZED REPRESENTATIVES (OCT 2020)

With respect to all matters relating to this RLP, only the Government's LCO designated below shall have the authority to amend the RLP and award a Lease. The Government shall have the right to substitute its LCO by notice, without an express delegation by the prior LCO.

Lease LCO:

Alan Trinh
4811 Airport Plaza Dr., Suite 600
562-766-2274
562-481-5283
alan.trinh@va.gov

As to all other matters, Offerors may contact the Alternate Government Contact designated below.

Alternate Government Contact:

Ralph Fontela
4811 Airport Plaza Dr., Suite 600
562-766-2282
562-419-2145
Raphael.fontela@va.gov

1.13 NORTH AMERICAN INDUSTRY CLASSIFICATION SYSTEM (NAICS) CODE AND SMALL BUSINESS SIZE STANDARD (OCT 2020)

A. The North American Industry Classification System (NAICS) code for this acquisition is 531120, unless the real property is self-storage (#531130), land (#531190), or residential (#531110).

B. The small business size standard for the applicable NAICS code is found [HTTPS://WWW.SBA.GOV/SIZE-STANDARDS/](https://www.sba.gov/size-standards/).

1.14 UNIQUE ENTITY IDENTIFIER (OCT 2020)

An offeror may obtain a Unique Entity Identifier, currently DUNS number, (i) via the Internet at <http://fedgov.dnb.com/webform> or if the offeror does not have internet access, it may call Dun and Bradstreet at 1-866-705-5711 if located within the United States; or (ii) If located outside the United States, by contacting the local Dun and Bradstreet office. The offeror should indicate that it is an offeror for a U.S. Government contract when contacting the local Dun and Bradstreet office. This process of obtaining a Unique Entity Identifier is subject to change.

SECTION 2 ELIGIBILITY AND PREFERENCES FOR AWARD

2.01 EFFICIENCY OF LAYOUT (AUG 2011)

- A. In order to be acceptable for award, the offered Space must provide for an efficient layout as determined by the LCO.
- B. To demonstrate potential for efficient layout, GSA may request the Offeror to provide a test fit layout at the Offeror's expense. The Government will advise the Offeror if the test fit layout demonstrates that the Government's requirement cannot be accommodated within the Space offered. The Offeror will have the option of increasing the ABOA square footage offered, if it does not exceed the maximum ABOA square footage in this RLP offer package. If the Offeror is already providing the maximum ABOA square footage and cannot house the Government's space requirements efficiently, then the Government will advise the Offeror that the offer is unacceptable.

2.02 FLOOD PLAINS (OCT 2017)

A Lease will not be awarded for any offered Property located within a 100-year floodplain unless the Government has determined that there is no practicable alternative. An Offeror may offer less than its entire site in order to exclude a portion of the site that falls within a floodplain, so long as the portion offered meets all the requirements of this RLP and does not impact the Government's full use and enjoyment of the Premises. If an Offeror intends that the offered Property that will become the Premises for purposes of this Lease will be something other than the entire site as recorded in tax or other property records the Offeror shall clearly demarcate the offered Property on its site plan/map submissions and shall propose an adjustment to property taxes on an appropriate pro rata basis. For such an offer, the LCO may, in his or her sole discretion, determine that the offered Property does not adequately avoid development in a 100-year floodplain.

In addition, a Lease will not be awarded for any offered Property adjacent to 100-year floodplain, where such an adjacency would, as determined by the LCO, in his or her sole discretion, restrict ingress or egress to the Premises in the event of a flood, unless there is no practicable alternative.

2.03 SEISMIC SAFETY – HIGH SEISMICITY (OCT 2017)

- A. The Government intends to award a Lease to an Offeror of a Building that is in compliance with the Seismic Standards. If an offer is received which is in compliance with the Seismic Standards and the other requirements of this RLP, then other offers which do not comply with the Seismic Standards must not be considered. If none of the offers is in compliance with the Standards, the LCO will make the award to the Offeror whose offer meets the other requirements of this RLP and provides the best value to the Government, taking into account price, seismic safety and any other award factors specified in this RLP.
- B. An offered Building will be considered to be in compliance with the Seismic Standards if it meets one of the following conditions:
1. The offer includes a representation that the Premises will be in a one-story Building of steel light frame or wood construction with less than 3,000 ABOA SF of space in the Building (Seismic Form D).
 2. The offer includes a Seismic Certificate certifying that the Building is a Benchmark Building (Seismic Form A).
 3. The offer includes a Seismic Certificate based on a Tier I Evaluation showing that the Building meets the Seismic Standards (Seismic Form B). The submission must include the checklists and backup calculations from the Tier 1 Evaluation.
 4. The offer includes a Seismic Certificate based on a Tier 2 or Tier 3 Evaluation showing that the Building complies with the Seismic Standards (Seismic Form B). If the certificate is based on a Tier 2 or Tier 3 Evaluation, the data, working papers, calculations and reports from the evaluation must be made available to the Government.
 5. The offer includes a commitment to retrofit the Building to satisfy all of the Basic Safety Objective requirements of ASCE/SEI 41 (Seismic Form C, Part 1). If the Offeror proposes to retrofit the Building, the offer must include a Tier 1 report with all supporting documents, a narrative explaining the process and scope of retrofit and a schedule for the seismic retrofit. The Offeror shall provide a construction schedule, concept design for the seismic upgrade and supporting documents for the retrofit, including structural calculations, drawings, specifications, and geotechnical report to the Government for review and approval prior to award. The documentation must demonstrate the seismic retrofit will meet the seismic standards and be completed within the time frame required.
 6. The offer includes a pre-award commitment to construct a new Building, using local building codes (Seismic Form C, Part 2).
- C. The LCO may allow an Offeror to submit a Seismic Certificate after the deadline for final proposal revisions. However, the LCO is not obligated to delay award in order to enable an Offeror to submit a Seismic Certificate.
- D. **Definitions.** For the purpose of this paragraph:
- "ASCE/SEI 31" means the American Society of Civil Engineers standard, Seismic Evaluation of Existing Buildings. You can purchase ASCE/SEI from ASCE at (800) 548-2723 or by visiting [HTTP://WWW.ASCE.ORG/PUBLICATIONS/](http://www.asce.org/publications/).

- “ASCE/SEI 41” means American Society of Civil Engineers standard, Seismic Rehabilitation of Existing Buildings. You can purchase ASCE/SEI from ASCE at (800) 548-2723 or by visiting [HTTP://WWW.ASCE.ORG/PUBLICATIONS/](http://WWW.ASCE.ORG/PUBLICATIONS/).
- “Benchmark Building” means a building that was designed and built, or retrofitted, in accordance with the seismic provisions of the applicable codes specified in Section 1.3.1 of RP 8.
- “Engineer” means a professional engineer who is licensed in Civil or Structural Engineering and qualified in the structural design of buildings. They must be licensed in the state where the property is located.
- “RP 8” means “*Standards of Seismic Safety for Existing Federally Owned and Leased Buildings ICSSC Recommended Practice 8 (RP 8)*,” issued by the Interagency Committee on Seismic Safety in Construction as ICSSC RP 8 and the National Institute of Standards and Technology as NIST GCR 11-917-12. RP 8 can be obtained from [HTTP://WWW.WBDG.ORG/CCB/NIST/NIST_GCR11_917_12.PDF](http://WWW.WBDG.ORG/CCB/NIST/NIST_GCR11_917_12.PDF)
- “Seismic Certificate” means a certificate executed and stamped by an Engineer on the appropriate Certificate of Seismic Compliance form included with this RLP together with any required attachments.
- “Seismic Standards” means the requirements of RP 8 Section 2.2 for Life Safety Performance Level in ASCE/SEI 31 or the Basic Safety Objective in ASCE/SEI 41, unless otherwise specified.
- “Tier 1 Evaluation” means an evaluation by an Engineer in accordance with Chapters 2.0 and 3.0 of ASCE/SEI 31. A Tier 1 Evaluation must include the appropriate Structural, Nonstructural and Geologic Site Hazards and Foundation Checklists.
- “Tier 2 Evaluation” means an evaluation by an Engineer in accordance with Chapter 4.0 of ASCE/SEI 31.
- “Tier 3 Evaluation” means an evaluation by an Engineer in accordance with Chapter 5.0 of ASCE/SEI 31.

2.04 HISTORIC PREFERENCE (SEP 2013)

A. The Government will give preference to offers of Space in Historic Properties and/or Historic Districts following this hierarchy of consideration:

1. Historic Properties within Historic Districts.
2. Non-historic developed sites and non-historic undeveloped sites within Historic Districts.
3. Historic Properties outside of Historic Districts.

B. Definitions:

1. Determination of eligibility means a decision by the Department of the Interior that a district, site, Building, structure or object meets the National Register criteria for evaluation although the Property is not formally listed in the National Register (36 CFR 60.3(c)).
2. Historic District means a geographically definable area, urban or rural, possessing a significant concentration, linkage, or continuity of sites, Buildings, structures, or objects united by past events or aesthetically by plan or physical development. A district may also comprise individual elements separated geographically but linked by association or history (36 CFR 60.3(d)). The Historic District must be included in or be determined eligible for inclusion in the National Register of Historic Places (NRHP).
3. Historic Property means any prehistoric or Historic District, site, building, structure, or object included in or been determined eligible for inclusion in the NRHP maintained by the Secretary of the Interior (36 CFR 800.16(l)).
4. National Register of Historic Places means the National Register of districts, sites, buildings, structures and objects significant in American history, architecture, archeology, engineering and culture that the Secretary of the Interior is authorized to expand and maintain under the National Historic Preservation Act (36 CFR 60.1).

C. The offer of Space must meet the terms and conditions of this RLP package and its attachments. The LCO has discretion to accept alternatives to certain architectural characteristics and safety features defined elsewhere in this RLP package to maintain the historical integrity of an Historic Building, such as high ceilings and wooden floors, or to maintain the integrity of an Historic District, such as setbacks, floor-to-ceiling heights, and location and appearance of parking.

D. When award will be based on the lowest price technically acceptable source selection process, the Government will give a price evaluation preference, based on the total annual ABOA SF present value cost to the Government, to Historic Properties as follows:

1. First to suitable Historic Properties within Historic Districts, a 10 percent price preference.

2. If no suitable Historic Property within an Historic District is offered, or the 10 percent preference does not result in such property being the lowest price technically acceptable offer, the Government will give a 2.5 percent price preference to suitable non-historic developed or undeveloped sites within Historic Districts.

3. If no suitable, non-historic, developed, or undeveloped site within a Historic District is offered, or the 2.5 percent preference does not result in such property being the lowest price technically acceptable offer, the Government will give a 10 percent price preference to suitable Historic Properties outside of Historic Districts.

4. Finally, if no suitable Historic Property outside of Historic Districts is offered, no historic price preference will be given to any property offered.

E. When award will be based on the best value tradeoff source selection process, which permits tradeoffs among price and non-price factors, the Government will give a price evaluation preference, based on the total annual ABOA SF present value cost to the Government, to Historic Properties as follows:

1. First, to suitable Historic Properties within Historic Districts, a 10 percent price preference.

2. If no suitable Historic Property within a Historic District is offered or remains in the competition, the Government will give a 2.5 percent price preference to suitable non-historic developed or undeveloped sites within Historic Districts.

3. If no suitable, non-historic developed or undeveloped site within an Historic District is offered or remains in the competition, the Government will give a 10 percent price preference to suitable Historic Properties outside of Historic Districts.

4. Finally, if no suitable Historic Property outside of Historic Districts is offered, no historic price preference will be given to any property offered.

F. The Government will compute price evaluation preferences by reducing the price(s) of the Offerors qualifying for a price evaluation preference by the applicable percentage provided in this provision. The price evaluation preference will be used for price evaluation purposes only. The Government will award a Lease for the actual prices proposed by the successful Offeror and accepted by the Government.

G. To qualify for a price evaluation preference, Offeror must provide satisfactory documentation in their offer that their property qualifies as one of the following:

1. A Historic Property within a Historic District.

2. A non-historic developed or undeveloped site within a Historic District.

3. A Historic Property outside of a Historic District.

2.05 ASBESTOS (JUN 2012)

A. Government requests space with no asbestos-containing materials (ACM), or with ACM in a stable, solid matrix (e.g., asbestos flooring or asbestos cement panels), which is not damaged or subject to damage by routine operations. For purposes of this paragraph, "space" includes the 1) space offered for lease; 2) common building area; 3) ventilation systems and zones serving the space offered; and 4) the area above suspended ceilings and engineering space in the same ventilation zone as the space offered. If no offers are received for such space, the Government may consider space with thermal system insulation ACM (e.g., wrapped pipe or boiler lagging), which is not damaged or subject to damage by routine operations.

B. ACM is defined as any materials with a concentration of greater than 1 percent by dry weight of asbestos.

C. Space with ACM of any type or condition may be upgraded by the Offeror to meet conditions described in sub-paragraph A by abatement (removal, enclosure, encapsulation, or repair) of ACM not meeting those conditions. If any offer involving abatement of ACM is accepted by the Government, the successful Offeror will be required to successfully complete the abatement in accordance with OSHA, EPA, Department of Transportation (DOT), state, and local regulations and guidance prior to occupancy.

D. Management Plan. If space is offered which contains ACM, the Offeror shall submit an asbestos-related management plan for acceptance by the Government prior to lease award. This plan shall conform to EPA guidance.

2.06 ACCESSIBILITY (SEP 2013)

The Lease contemplated by this RLP contains requirements for Accessibility. In order to be eligible for award, Offeror must either:

A. Verify in the Lease proposal that the Building, offered Space, and areas serving the offered Space meet the Lease accessibility requirements, or

B. Include as a specific obligation in its Lease proposal that improvements to bring the Building, offered Space, and areas serving the offered Space into compliance with Lease accessibility requirements will be completed prior to acceptance of the Space.

2.07 FIRE PROTECTION AND LIFE SAFETY (SEP 2013)

The Lease contemplated by this RLP contains Building requirements for Means of Egress, Automatic Fire Sprinkler System, and Fire Alarm System. In order to be eligible for award, Offeror must either:

- A. Verify in the Lease proposal that the Building in which Space is offered meets the Means of Egress, Automatic Fire Sprinkler System, and Fire Alarm System requirements of the Lease; or
- B. Include as a specific obligation in its Lease proposal that improvements to bring the Building into compliance with Lease requirements will be completed prior to acceptance of the Space.

2.08 ENERGY INDEPENDENCE AND SECURITY ACT (OCT 2016)

A. The Energy Independence and Security Act (EISA) establishes requirements for Government leases relating to energy efficiency standards and potential cost effective energy efficiency and conservation improvements.

B. Unless one of the statutory exceptions listed in sub-paragraph C below applies, GSA may award a lease for a Building only if the Building has earned the ENERGY STAR® label conferred by the U.S. Environmental Protection Agency (EPA) within the most recent year prior to the due date for final proposal revisions. The term "most recent year" means that the date of award of the ENERGY STAR® label by EPA must not be more than 1 year prior to the due date of final proposal revisions. For example, an ENERGY STAR® label awarded by EPA on October 1, 2010, is valid for all lease procurements where final proposal revisions are due on or before September 30, 2011. In lieu of the above, all new Buildings being specifically constructed for the Government must achieve an ENERGY STAR® label within 18 months after occupancy by the Government. In addition, Offerors of the following Buildings shall also have up to 18 months after occupancy by the Government, or as soon thereafter as the Building is eligible for Energy Star® consideration, to achieve an Energy Star® label: 1) All existing Buildings that have had an Energy Star® label but are unable to obtain a label in the most recent year (i.e., within 12 months prior to the due date for final proposal revisions) because of insufficient occupancy; 2) Newly built Buildings that have used Energy® Star's Target Finder tool and either achieved a "Designed to Earn the Energy Star®" certification or received an unofficial score (in strict adherence to Target Finder's usage instructions, including the use of required energy modeling) of 75 or higher prior to the due date for final proposal revisions and who are unable to obtain a label in the most recent year because of insufficient occupancy; 3) An existing Building that is unable to obtain a label because of insufficient occupancy but that can produce an indication, through the use of energy modeling or past utility and occupancy data input into Energy Star's® Portfolio Manager tool or Target Finder, that it can receive an unofficial score of 75 or higher using all other requirements of Target Finder or Portfolio Manager, except for actual data from the most recent year. ENERGY STAR® tools and resources can be found at <HTTPS://WWW.ENERGYSTAR.GOV/>.

C. EISA allows a Federal agency to lease Space in a Building that does not have an ENERGY STAR® Label if:

1. No Space is offered in a Building with an ENERGY STAR® Label that meets RLP requirements, including locational needs;
2. The agency will remain in a Building it currently occupies;
3. The Lease will be in a Building of historical, architectural, or cultural significance listed or eligible to be listed on the National Register of Historic Places; or
4. The Lease is for 10,000 RSF or less.

D. If one or more of the statutory exceptions applies, and the offered Space is not in a Building that has earned the ENERGY STAR® Label within one year prior to the due date for final proposal revisions, Offerors are required to include in their lease proposal an agreement to renovate the Building for all energy efficiency and conservation improvements that it has determined would be cost effective over the Firm Term of the Lease, if any, prior to acceptance of the Space (or not later than one year after the Lease Award Date of a succeeding or superseding lease). Such improvements may consist of, but are not limited to, the following:

1. Heating, Ventilating, and Air Conditioning (HVAC) upgrades, including boilers, chillers, and Building Automation System (BAS)/Monitoring/Control System (EMCS).
2. Lighting Improvements.
3. Building Envelope Modifications.

NOTE: Additional information can be found on <http://www.gsa.gov/leasing> under "Green Leasing."

E. The term "cost effective" means an improvement that will result in substantial operational cost savings to the landlord by reducing electricity or fossil fuel consumption, water, or other utility costs. The term "operational cost savings" means a reduction in operational costs to the landlord through the application of Building improvements that achieve cost savings over the Firm Term of the Lease sufficient to pay the incremental additional costs of making the Building improvements.

F. Instructions for obtaining an ENERGY STAR® Label are provided at <http://www.energystar.gov/buildings/facility-owners-and-managers/existing-buildings/earn-recognition/energy-star-certification> (use "Portfolio Manager" to apply). ENERGY STAR® tools and resources can be found at <HTTPS://WWW.ENERGYSTAR.GOV/>. The ENERGY STAR® Building Upgrade Manual (<http://www.energystar.gov/buildings/facility-owners-and-managers/existing-buildings/save-energy/comprehensive-approach/energy-star>) and Building Upgrade Value Calculator (<http://www.energystar.gov/buildings/tools-and-resources/building-upgrade-value-calculator>) are tools which can be useful in considering energy efficiency and conservation improvements to Buildings.

G. If one or more of the statutory exceptions applies, and the offered Space is not in a Building that has earned the ENERGY STAR® Label within one year prior to the due date for final proposal revisions, the successful Offeror will be excused from performing any agreed-to energy efficiency and conservation renovations, and benchmarking with public disclosure (as provided in (I) below, if it obtains the ENERGY STAR® Label prior to the Government's acceptance of the Space (or not later than one year after the Lease Award Date for succeeding and superseding leases).

H. If no improvements are proposed, the Offeror must demonstrate to the Government using the ENERGY STAR® Online Tools why no energy efficiency and conservation improvements are cost effective. If such explanation is unreasonable, the offer may be rejected.

I. As described in Section 3 of the Lease, successful Offerors meeting one of the statutory exceptions above must agree to benchmark and publicly disclose the Building's current ENERGY STAR® score, using EPA's Portfolio Manager online software application. See the Lease for additional details.

J. All new Buildings being specifically constructed for the Government must achieve the ENERGY STAR® Label within 18 months after occupancy by the Government.

K. INTENTIONALLY DELETED

2.09 ENVIRONMENTAL CONSIDERATIONS (SEP 2013)

A. The Government requests space with no known hazardous conditions or recognized environmental conditions that would pose a health and safety risk or environmental liability to the Government.

B. Upon request by the Government, Offeror must provide all known previous use of the Building.

C. Offeror must indicate in its written offer any known hazardous conditions or environmental releases with/from the offered Space, Building or Property.

SECTION 3 HOW TO OFFER

3.01 GENERAL INSTRUCTIONS (JUN 2012)

Offeror shall prepare a complete offer, using the forms provided with this RLP, and submit the completed lease proposal package to the Government as indicated below.

3.02 RECEIPT OF LEASE PROPOSALS (OCT 2020)

A. Non-electronic method:

1. Offeror is authorized to transmit its lease proposal as an attachment to an email. Offeror's email shall include the name, address and telephone number of the Offeror, and identify the name and title of the individual signing on behalf of the Offeror. Offeror's signed lease proposal must be saved in a generally accessible format (such as portable document format (pdf)), which displays a visible image of all original document signatures, and must be transmitted as an attachment to the email. Only emails transmitted to, and received at, the GSA email address identified in the RLP will be accepted. Offeror submitting a lease proposal by email shall retain in its possession, and make available upon GSA's request, its original signed proposal. Offeror choosing not to submit its proposal via email may still submit its lease proposal by United States mail or other express delivery service of Offeror's choosing.

2. In order to be considered for award, offers conforming to the requirements of the RLP shall be received in one of the following ways:

a) No later than **[4:00 pm] [PST]** on the date specified below at the following designated office and address:

Date: 1-25-2021
Office: NCO 22 Long Beach
Address: 4811 Airport Plaza Dr., Suite 600, Long Beach, CA 90815

b) No later than **[4:00 pm] [PST]** on the date specified below at the following email address:

Date: 1-25-2021
Email: RAPHAEL.FONTELA@VA.GOV
Address:

3. Offers sent by United States mail or hand delivered (including delivery by commercial carrier) shall be deemed late if delivered to the address of the office designated for receipt of offers after the date and time established for receipt of offers.

4. Offers transmitted through email shall be deemed late if received at the designated email address after the date and time established for receipt of offers unless it was received at the initial point of entry to the Government infrastructure not later than 5:00 p.m. one Working Day prior to the date specified for receipt of proposals.

5. Offers delivered through any means authorized by the RLP may be also deemed timely if there is acceptable evidence to establish that it was received at the Government installation designated for receipt of proposals and was under the Government's control prior to the time set for receipt of proposals; or if it was the only proposal received.

A. Submission through Lease Offer Platform (LOP):

1. Unless otherwise authorized by the LCO or his/her designated representative, offers may only be submitted electronically to GSA using the Lease Offer Platform (Application, Requirement Specific Acquisition Platform (LOP/RSAP) located at <https://lop.gsa.gov/RSAP>. LOP enables Offerors to electronically offer space for lease to the Federal Government. The offer submission process is web-enabled, allowing all registered participants to submit and update offers to lease space to the Government in response to a single RLP for a specific space requirement.

2. In order to be considered for award, offers conforming to the requirements of the RLP shall be submitted through LOP/RSAP no later than **1-25-2021, 4:00 pm, PST**.

3. Offerors must submit all documentation identified in this RLP using the LOP/RSAP Application. The LOP/RSAP generates the Lessor's Annual Cost Statement (GSA Form 1217) and Proposal to Lease Space (GSA Form 1364) based on the entered data. These auto-populated forms are available for review at the end of the Application workflow and should be uploaded by the Offeror as part of his/her offer; there is no need for the Offeror to manually complete the attached blank version of these two forms. Any subsequent revisions to offer documents must be submitted through the LOP platform.

There is no paper-based submission process under this RLP and paper submissions will not be considered, unless otherwise authorized by the LCO.

B. There will be no public opening of offers, and all offers will be confidential until the Lease has been awarded. However, the Government may release proposals outside the Government such as to support contractors to assist in the evaluation of offers. Such Government contractors shall be required to protect the data from unauthorized disclosure.

3.03 PRICING TERMS (OCT 2020)

Offeror shall provide the following pricing information with its offer:

- A. GSA Form 1217, Lessor's Annual Cost Statement. Complete all sections of the 1217.
- B. GSA Form 1364, Proposal to Lease Space. Complete all sections of the 1364, including, but not limited to:
1. A fully serviced Lease rate (gross rate) per ABOA and RSF, clearly itemizing the total Building shell rental, TI rate, Building Specific Amortized Capital (BSAC) rate, operating costs, and parking (itemizing all costs of parking above base local code requirements or otherwise already included in shell rent).
 2. Improvements. All improvements in the base Building, lobbies, common areas, and core areas shall be provided by the Lessor, at the Lessor's expense. This Building shell rental rate shall also include, but is not limited to, property financing (exclusive of TIs and BSAC), insurance, taxes, management, profit, etc., for the Building. The Building shell rental rate shall also include all basic Building systems and common area buildout, including base Building lobbies, common areas, core areas, etc., exclusive of the ABOA Space offered as required in this RLP.
 3. The annual cost per ABOA and rentable square foot (RSF) for the cost of services and utilities. This equals line 27 of GSA Form 1217, Lessor's Annual Cost Statement, divided by the Building size (shown on the top of both GSA Form 1364, Proposal to Lease Space, and Form 1217) for ABOA and RSF, respectively.
 4. The annual rent to amortize the Tenant Improvements. Such amortization shall be expressed as a cost per ABOA and RSF per year. This shall be all alterations for the Space above the Building shell and BSAC build-out. Such alterations shall be described and identified in the drawings used to construct the Space. If the Offeror chooses to amortize the TI for a period exceeding the Firm Term of the Lease, the Offeror shall indicate the extended time in the offer. If the Government terminates the Lease after the Firm Term or does not otherwise renew or extend the term beyond the Firm Term, the Government shall not be liable for any unamortized TI costs resulting from an extended amortization period.
 5. The annual rent to amortize the Building Specific Amortized Capital (BSAC) costs, if any. Such amortization shall be expressed as a rate per ABOA and RSF per year. Refer to the security requirements attached to the Lease.
 6. A shell rate per ABOA and RSF for that portion of the lease term extending beyond the Firm Term. The rate proposed for this portion of the term shall not reflect any TIs or BSAC as they will have been fully amortized over the Firm Term.
 7. An hourly overtime rate for overtime use of heating and cooling, and, if applicable, Adjustment for Reduced Services. **NOTE:** Refer to the Lease document for additional guidance.
 8. Adjustment for Vacant Leased Premises. **NOTE:** Refer to the Lease document for additional guidance.
 9. INTENTIONALLY DELETED
 10. Rent concessions being offered. Indicate either on the GSA Form 1364 Proposal to Lease Space or in separate correspondence.
 11. Compensation (expressed as either % or \$) to Offeror's broker and/or representative arising from an agreement between the Offeror and the Offeror's representative, agent(s), broker(s), property manager, developer, employee, or any other agent or representative in connection with the Lease contemplated herein shall be entered in block 25.b., and if GSA is using a Tenant Representative Broker, compensation (expressed as either % or \$) to GSA's Broker reflecting the agreement between Offeror and GSA's Broker, shall be entered in block 25.a.
- C. Security Unit Price List. The Offeror shall use the Security Unit Price list to provide a cost breakdown of the security countermeasures, which were outlined in the security requirements attachment. The Security Unit Price list includes various improvements and services to be provided by the Lessor. Each item is classified as part of the shell, tenant improvements, or BSAC. There shall be no charge to the Government for any items that already exist in the offered Building or facility.
- D. TI Unit Price List
- E. INTENTIONALLY DELETED

F Additional rent, expressed as a rate per ABOA and per RSF per year, to provide the additional "Routine Cleaning and Disinfecting Requirements for the Premises" as described under the paragraph "Janitorial Services." This rent component is not subject to CPI operating costs adjustments. The Government reserves the right to cancel this routine disinfecting service and reduce the rent accordingly. This rate shall be entered on the submittal form entitled Rate for Routine Cleaning and Disinfecting Services.

3.04 BUDGET SCOREKEEPING; OPERATING LEASE TREATMENT (APR 2011)

The Government will award a Lease pursuant to this RLP only if the Lease will score as an operating lease under Office of Management and Budget Circular A-11, Appendix B. Only offers that are compliant with operating lease limitations will be eligible for award. Offerors are obligated to provide supporting documentation at the request of the LCO to facilitate the Government's determination in this regard.

3.05 ADDITIONAL SUBMITTALS (OCT 2020)

Offeror shall also submit with its offer the following:

A. If the offeror is not the owner of the Property, authorization from the ownership entity to submit an offer on the ownership entity's behalf.

B. Satisfactory evidence of at least a conditional commitment of funds in an amount necessary to prepare the Space, including Shell, TI, and BSAC improvements. Such commitments shall be signed by an authorized bank officer, or other legally authorized financing official, and at a minimum shall state: amount of loan, term in years, annual percentage rate, and length of loan commitment.

C. Evidence that the Property is zoned in compliance with local zoning laws, including evidence of variances, if any, approved by the proper local authority. If the current zoning is not in compliance, the Offeror must submit a plan and time schedule outlining how they will obtain all necessary zoning approvals prior to construction and how long the necessary zoning approvals will take.

D. Evidence of ownership or control of Building or site. If the Offeror owns the Property being offered or has a long-term leasehold interest, the deed or lease must be submitted to the LCO evidencing the Offeror's stated interest in the Property and any encumbrances on the Property.

E. If the Offeror does not yet have a vested interest in the Property, but rather has a written agreement to acquire an interest, then the Offeror shall submit a fully executed copy of the written agreement with its offer, together with a statement from the current owner that the agreement is in full force and effect and that the Offeror has performed all conditions precedent to closing, or other form of documentation satisfactory to the LCO prior to award. These submittals must remain current. The Offeror is required to submit updated documents as required.

F. Required Proof of Signing Authority: As a condition of lease award, the Government will require one of the following forms of proof of signing authority before the Government executes the Lease:

1. Corporation – Copy of Articles of Incorporation and bylaws. In addition, a copy of the resolution, signed by the necessary directors of the corporation authorizing the corporate officer who will sign the lease to bind the corporation to the Lease.
2. Partnership -- Copy of Partnership Agreement, Statement of Partnership, or Statement of Limited Partnership and evidence of authority of signatory to bind the partnership if not expressly authorized by the Partnership Agreement.
3. Limited Liability Company – Copy of the Articles of Organization and Operating Agreement. Also, evidence of the authority of the signing manager (if company is manager owned) or member (if the company is member managed) to sign, if not expressly authorized by the Articles of Organization and/or Operating Agreement.
4. Joint Venture -- Copy of Joint Venture Agreement and evidence of authority of signatory to bind the Joint Venture to the Lease.

G. If claiming an historic preference in accordance with the Historic Preference paragraph in RLP Section 2, Eligibility and Preferences for Award, Offeror must submit one of the following as documentation that the Property is historic or the site of the offered Property is within a Historic District: a letter from the National Park Service stating that the Property is listed in the National Register of Historic Places (NRHP) or eligible for listing, with a date of the listing/decision; a letter from the State Historic Preservation Office stating that the Property is listed in the NRHP, or on a statewide register, or eligible for inclusion, with a date of the listing/decision; or, the NRHP Identification Number and date of listing available from the NRHP Database found at www.nps.gov/nr.

H. If there is a potential for conflict of interest because of a single agent representing multiple owners, present evidence that the agent disclosed the multiple representation to each entity and has authorization from each ownership entity offering in response to this RLP package. Owners and agents in conflicting interest situations are advised to exercise due diligence with regard to ethics, independent pricing, and Government procurement integrity requirements. In such cases, the Government reserves the right to negotiate with the owner directly.

I. The Offeror must have an active registration in the System for Award Management (SAM), via the Internet at [HTTP://WWW.SAM.GOV](http://WWW.SAM.GOV) prior to the Lease Award Date. Offerors must be registered for purposes of "All Awards," including completion of all required representations and certifications within SAM. This registration service is free of charge.

J. The Offeror must submit the Fire Protection and Life Safety (FPLS) Information in subparagraph 1, unless the Building meets either exemption in subparagraphs 2 or 3 below.

1. FPLS Submittal Information
 - a. Completed GSA Form 12000, Prelease Fire Protection and Life Safety Evaluation for an Office Building (Part A or Part B, as applicable).
 - b. A copy of the previous year's fire alarm system maintenance record showing compliance with the requirements in NFPA 72 (if a system is installed in the Building).
 - c. A copy of the previous year's automatic fire sprinkler system maintenance record showing compliance with the requirements in NFPA 25 (if a system is installed in the Building).
 - d. A valid Building Certificate of Occupancy (C of O) issued by the local jurisdiction. If the Building C of O is not available or the local jurisdiction does not issue a Building C of O, provide either:
 - i. A report prepared by a licensed fire protection engineer with their assessment of the Building regarding compliance with all applicable local Fire Protection and Life Safety-related codes and ordinances or,
 - ii. For offers of new construction only, documentation indicating the Building Code (including edition) to which the Building is being constructed and a written commitment to meet all of the mandatory FPLS lease requirements in the Lease.
2. If the Space offered is 10,000 RSF or less in area and is located on the 1st floor of the Building, Offeror is not required to submit to GSA the Fire Protection and Life Safety (FPLS) Submittal Information listed in 1.a through 1.d above.
3. If the Offeror provides a Building C of O obtained under any edition of the International Building Code (IBC), and the offered Space meets or will meet all the requirements of the Lease with regard to Means of Egress, Automatic Fire Sprinkler System, and Fire Alarm System prior to occupancy, then the Offeror is not required to submit to GSA the FPLS Submittal Information listed in 1 above.

K. The legal description of the Property and tax ID number associated with the Property, copies of prior year tax notices and prior year tax bills, as well as any other information (such as a fact sheet, 5" wide x 3" high or larger color photograph, site plan, location map, and tax parcel map) in case of multiple tax parcels for an offered Building, or multiple buildings on a tax parcel, and any other information that may affect the assessed value, in order for the Government to perform a complete and adequate analysis of the offered Property. The Offeror is to provide a detailed overview and documentation of any Tax Abatements on the Property as outlined in the "Real Estate Tax Adjustment" paragraph of the Lease.

L. A plan and short narrative as necessary to explain how the Offeror will meet the parking requirements.

M. The architectural plans for modernization, if the offered Building is not a modern office Building.

N. An asbestos management plan, if the offered Building contains asbestos-containing materials.

O. Computer generated plans set to 1/8" = 1'-0" (preferred meeting sub-paragraphs 1 through 5 noted below):

1. All plans submitted for consideration shall include floor plan(s) for which Space is being offered and floor plan(s) of the floor(s) of exit discharge (e.g., street level(s)). Each plan submitted shall include the locations of all exit stairs, elevators, and the Space(s) being offered to the Government. In addition, where Building exit stairs are interrupted or discontinued before the level of exit discharge, additional floor plans for the level(s) where exit stairs are interrupted or discontinued must also be provided.
2. All plans submitted for consideration shall have been generated by a Computer Aided Design (CAD) program which is compatible with the latest release of AutoCAD. The required file extension is .DWG. Plans shall include a proposed corridor pattern for typical floors and/or partial floors. The CAD file showing the offered Space should show the Poly-Line utilized to determine the square footage on a separate and unique layer. All submissions shall be accompanied with a written matrix indicating the layering standard to verify that all information is recoverable. All architectural features of the Space shall be accurately shown.
3. All architectural features of the Space shall be accurately shown. If conversion or renovation of the Building is planned, alterations to meet this RLP shall be indicated.
4. Plans shall reflect corridors in place or the proposed corridor pattern for both a typical full (single-tenant) floor and/or partial (multi-tenant) floor. The corridors in place or proposed corridors shall meet local code requirements for issuance of occupancy permits.
5. GSA will review all plans submitted to determine if an acceptable level of safety is provided. In addition, GSA will review the common corridors in place and/or proposed corridor pattern to determine whether these achieve an acceptable level of safety as well as to verify that the corridors provide public access to all essential Building elements. The Offeror will be advised of any adjustments that are required to the corridors for determining the ABOA Space. The required corridors may or may not be defined by ceiling-high partitions. Actual corridors in the approved layout for the successful Offeror's Space may differ from the corridors used in determining the ABOA square footage for the lease award. Additional egress corridors required by the tenant agency's design intent drawings will not be deducted from the ABOA square footage that the most efficient corridor pattern would have yielded.

P. As provided in the "Amount and Type of Space, Lease Term, and Occupancy Date" paragraph in the RLP, advise whether there are existing vending facilities in the offered Building which have exclusive rights in the Building.

Q. Provide evidence demonstrating amenities do or will exist by the Government's required occupancy date. Such evidence shall include copies of signed leases, construction contracts, or other documentation as deemed acceptable by the LCO.

R. No later than the due date for final proposal revisions, the Offeror must submit to the LCO:

1. Evidence of an Energy Star® label obtained within the 12 months prior to the due date of final proposal revisions,
2. Offerors falling under a statutory exception must also indicate by the due date for final proposal revisions what cost effective energy efficiency and conservation improvements they are proposing to make.
3. If no cost-effective improvements can be made, the Offeror must demonstrate to the Government using the ENERGY STAR® Online Tools referenced in the RLP paragraph, entitled "ENERGY INDEPENDENCE AND SECURITY ACT," why no energy efficiency and conservation improvements are cost effective. This explanation will be subject to review by the LCO. If the explanation is considered unreasonable, the offer may be considered technically unacceptable.
4. If the Offeror is claiming eligibility for additional time to obtain the Energy Star® label per sub-paragraph B of the RLP paragraph entitled "Energy Independence and Security Act," then the Offeror shall provide such indication with its initial offer and also must provide by the due date for final proposal revisions evidence substantiating their claim for additional time to obtain the Energy Star® label and substantiating their capability of earning the Energy Star®.
5. For new construction, the Offeror need not submit anything regarding compliance with EISA by the date of final proposal revisions, but shall be required to produce prior to the issuance of a permit for building construction a Statement of Energy Design Intent (SEDI) using Energy Star's® Target Finder online tool reflecting an Energy Star® benchmark score of 75 or higher and a certification from EPA of being Designed to Earn the Energy Star®.

U. Evidence of seismic safety compliance as required in Section 2 of this RLP.

X. If the Offeror requests any deviations, all deviations must be documented on Form 1364 in block labeled "Additional Remarks or Conditions with Respect to this Offer." GSA at its sole discretion will make the decision whether or not to accept the deviation. Any deviations must be requested prior to the request for final proposal revisions. If the Offeror requests any deviations, GSA at its sole discretion will make the decision whether to accept the deviation.

Y. If more than 5,000 square feet of land area is to be disturbed in order to meet the Government's requirements, (as more fully described in the lease paragraph named ENERGY INDEPENDENCE AND SECURITY ACT, sub-paragraph (B)(1)(b)), a statement from Offeror that the Offeror is aware of and will comply with the specific lease requirements concerning maintenance and restoration of the real property's hydrology.

Z. INTENTIONALLY DELETED

AB. FAR 52.204-24, Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment , as applicable.

3.06 TENANT IMPROVEMENTS INCLUDED IN OFFER (OCT 2020)

A. TENANT IMPROVEMENT TURNKEY PRICING

An Agency Specific Requirements (ASR) package is provided with this RLP to all Offerors upon which to base their TI pricing. (TIs are the finishes and fixtures that typically take Space from the "shell" condition to a finished, usable condition.) All TIs required by the Government for occupancy shall be performed by the successful Offeror as part of the rental consideration and all improvements shall meet the quality standards and requirements of this RLP and its attachments.

B. The Tenant Improvements shall include all the Offeror's administrative costs, general contractor fees, subcontractor's profit and overhead costs, Offeror's Project Management fee, design costs, and other associated project fees necessary to prepare construction documents and to complete the TIs. It is the successful Offeror's responsibility to prepare all documentation (working/construction drawings, etc.) required to receive construction permits. NO COSTS ASSOCIATED WITH THE BUILDING SHELL SHALL BE INCLUDED IN THE TI PRICING.

3.07 TURNKEY PRICING WITH DESIGN INTENT DRAWINGS PRIOR TO AWARD (OCT 2017)

A. Following the receipt of initial offers, Offerors must coordinate a DID workshop with their respective design and construction team and the tenant agency to develop, review, and complete final DIDs before final pricing is established and prior to award of the Lease. The Government will advise Offerors when the workshop should commence. The Offeror shall base the TI portion of its overall pricing on the final approved DIDs and the specifications in this RLP and attachments. This TI price will become a fixed price which the Offeror will include in the final lease proposal as an amortized rent over the Firm Term. Offerors should not price TIs until DIDs are approved in writing by the LCO. The Government reserves the right to make no-cost tradeoffs in the TIs after award. No costs associated with the Building shell or building-specific security shall be included in the TI pricing.

B. DIDs, for the purposes of the Lease, are defined as layout line drawings of the leased Space, reflecting all Lease requirements, showing partitions and doors; schematic demolition; voice, data, and electrical outlet locations; finishes; generic furniture layout, and any additional details necessary to communicate the design intent to the lessor's architect for the purpose of preparing the construction documents (CDs). A full DID set must include the following elements:

Level 1:

1. Cover Sheet;
2. Demolition Plan (if applicable);
3. Construction (Partition) Plan;
4. Power/Communication (Electrical) Plan;
5. Furniture Plan; and
6. Finish Plan.

3.08 OPERATING COSTS REQUIREMENTS INCLUDED IN OFFER (JUN 2012)

The Government requires a fully serviced Lease as part of the rental consideration. The base for the operating costs adjustment will be established during negotiations based upon rentable SF. The proposed methodology for operating costs adjustment shall include all items specified in the attached Lease document. The minimum requirements for normal hours, utilities, and janitorial services are specified in the attached Lease document. The offer shall clearly state whether the rental is firm throughout the term of the Lease or if it is subject to annual adjustment of operating costs as indicated above. If operating costs will be subject to adjustment, those costs shall be specified in the proposal.

SECTION 4 METHOD OF AWARD

4.01 NEGOTIATIONS (JUN 2012)

Negotiations may be conducted on behalf of the Government by the GSA LCO or designated representative. When negotiations are conducted, GSA will negotiate the rental price for the initial term, any renewal periods, and any other aspect of the offer as deemed necessary. The Offeror shall not enter into negotiations concerning the Space leased or to be leased with representatives of Federal agencies other than the LCO or their designee. The LCO or their designated representative will conduct oral or written negotiations with all Offerors that are within the competitive range. The competitive range will be established by the LCO based on cost or price and other factors (if any) that are stated in this RLP and will include all of the most highly rated proposals, unless the range is further reduced for purposes of efficiency. Prior to eliminating an Offeror that is a HUBZone small business concern (SBC) and which has not waived its entitlement to a price evaluation preference from the competitive range, the LCO shall adjust the evaluated prices of all non-small business Offerors proposed for inclusion in the competitive range by increasing the prices by ten (10) percent, solely for the purpose of determining whether the HUBZone SBC Offeror should be included or excluded from the competitive range. Offerors who are not included in the competitive range will be notified in writing.

All Offerors within the competitive range will be provided a reasonable opportunity to submit revisions to their initial offer including any cost or price, technical, or other revisions that may result from the negotiations. Negotiations will be closed with submission of final proposal revisions.

4.02 HUBZONE SMALL BUSINESS CONCERN ADDITIONAL PERFORMANCE REQUIREMENTS (SEP 2015)

A HUBZone small business concern (SBC) Offeror may elect to waive the price evaluation preference provided in the "Award Based On Price" paragraph or the "Other Award Factors" paragraph of the RLP by so indicating on the GSA Form 1364, Proposal to Lease Space. In such a case, no price evaluation preference shall apply to the evaluation of the HUBZone SBC, and the performance of work requirements set forth in Section 1 of the Lease shall not be applicable should the HUBZone SBC be awarded the Lease. A HUBZone SBC Offeror acknowledges that a prospective HUBZone SBC awardee must be a qualified HUBZone SBC at the time of award of this contract in order to be eligible for the price evaluation preference. The HUBZone SBC Offeror shall provide the LCO a copy of the notice required by 13 CFR 126.501 if material changes occur before contract award that could affect its HUBZone eligibility. If it is determined, prior to award, that the apparently successful HUBZone SBC Offeror is not an eligible HUBZone SBC, the LCO will reevaluate proposals without regard to any price preference provided for the previously identified HUBZone SBC Offeror, and make an award consistent with the solicitation and the evaluation factors set forth herein.

If a HUBZone SBC that has not waived the price preference is awarded the Lease, the certification required by the "Additional Financial and Technical Capability" paragraph of the Lease must be provided within 10 days of award. If it is determined within 20 days of award that a HUBZone SBC Offeror that has been awarded the Lease was not an eligible HUBZone SBC at the time of award, and the HUBZone SBC Lessor failed to provide the LCO with information regarding a change to its HUBZone eligibility prior to award, then the Lease shall be subject, at the LCO's discretion, to termination, and the Government will be relieved of all obligations to the Lessor in such an event and not be liable to the Lessor for any costs, claims or damages of any nature whatsoever.

4.03 AWARD BASED ON PRICE (JUN 2012)

A. The Lease will be awarded to the responsible Offeror whose offer conforms to the requirements of this RLP and the Lease documents and is the lowest priced technically acceptable offer submitted. Refer to the "Present Value Price Evaluation" paragraph of this RLP.

B. If after completion of the Price Evaluation, award is proposed to a non-small business Offeror, and there exists as part of the procurement another technically acceptable proposal submitted by a responsible Offeror that is a qualified HUBZone small business concern (SBC) which has not waived its entitlement to a price evaluation preference, the evaluated price of the non-small business Offeror's proposal shall be increased by ten (10) percent, solely for the purpose of determining whether award should be made to the HUBZone SBC Offeror. In such a case, the proposals of the apparently successful non-small business Offeror and the HUBZone SBC Offeror shall be considered in light of the applied price preference, and award made to the lower priced offer. The LCO shall document his/her application of the price preference and further consideration of the offers under this subparagraph.

C. If an offer contains terms taking exception to or modifying any Lease provision, the Government will not be under any obligation to award a Lease in response to that offer.

4.04 PRESENT VALUE PRICE EVALUATION (OCT 2016)

A. If annual CPI adjustments in operating expenses are included, the Offeror shall be required to submit the offer with the total "gross" annual price per RSF and per ABOA SF and a breakout of the "base" price per RSF and ABOA SF for services and utilities

(operating expenses) to be provided by the Lessor. The "gross" price shall include the "base" price. The base price per ABOA SF from which adjustments are made will be the base price for the term of the Lease, including any option periods.

B. The Offeror must submit plans and any other information to demonstrate that the Rentable Space yields ABOA space within the required ABOA range. The Government will verify the amount of ABOA SF and will convert the rentable prices offered to ABOA prices, which will subsequently be used in the price evaluation.

C. Evaluation of offered prices will be based on the annual price per ABOA SF, including all required option periods. The Government will perform present value price evaluation by reducing the prices per ABOA SF to a composite annual ABOA SF price, as follows:

1. Parking and wareyard areas will be excluded from the total square footage but not from the price. For different types of space, the gross annual per ABOA SF price will be determined by dividing the total annual rental by the total ABOA square footage excluding these areas.

2. Free rent will be evaluated in the year in which it is offered. The gross annual price is adjusted to reflect free rent.

3. Prior to the discounting procedure below, the total dollar amount of the Commission Credit (if applicable) will be subtracted from the first year's gross annual rent, unless the provision of free rent causes the credit to apply against rent beyond the first year's term, in which case the Commission Credit will be allocated proportionately against the appropriate year's gross rent.

4. Also as stated in the "Broker Commission and Commission Credit" paragraph, the amount of any commission paid to GSA's Broker will not be considered separately as part of this price evaluation since the value of the commission is subsumed in the gross rent rate.

5. If annual adjustments in operating expenses will not be made, the gross annual price, minus the Commission Credit (if applicable), will be discounted annually at 5 percent to yield a gross present value cost (PVC).

6. If annual adjustments in operating expenses will be made, the annual price, minus the Commission Credit (if applicable) and minus the base cost of operating expenses, will be discounted annually at 5 percent to yield net PVC. The operating expenses will be both escalated at 2.5 percent compounded annually and discounted annually at 5 percent, then added to the net PVC to yield the gross PVC.

7. To the gross PVC will be added:

a. For lease acquisitions where the Government is considering less than fully-serviced offers, the cost of Government-provided services (e.g., utilities, janitorial) not included in the rental escalated at 2.5 percent compounded annually and discounted annually at 5 percent.

b. The annualized (over the full term) cost of any items, which are to be reimbursed in a lump sum payment. (The cost of these items is present value; therefore, it will not be discounted.)

c. The annual price for parking to accommodate the minimum number of spaces required for government vehicles, if not included in the shell rent and charged separately. The price will be discounted annually at 5 percent.

d. The cost of relocation of furniture, telecommunications, replications costs, and other move-related costs, if applicable.

e. INTENTIONALLY DELETED

f. The annual cost of overtime HVAC based on the offered hourly overtime rate and an estimated usage of 600 hours of overtime HVAC per year for the Space. This cost will be discounted annually at 5 percent.

8. The sum of either sub-paragraphs 5 and 7 or sub-paragraphs 6 and 7, divided by the ABOA SF will be the present value cost per ABOA SF of the offer for price evaluation purposes.

4.05 AWARD (OCT 2018)

A. To document the agreement between the parties, the successful Offeror and the GSA LCO will execute a Lease prepared by GSA, which incorporates the agreement of the parties. The Lease shall consist of the following:

1. Lease No. 36C26221L0002 and any associated Lease amendments.

2. GSA Form 3517B, General Clauses.

3. The pertinent provisions of the offer.

4. Approved DIDs.

4. Foreign Ownership and Financing Representation.

B. The acceptance of the offer and award of the Lease by the Government occurs upon execution of the Lease by the LCO and mailing or otherwise furnishing written notification of the executed Lease to the successful Offeror.

SECTION 5 ADDITIONAL TERMS AND CONDITIONS

5.01 MODIFIED RLP PARAGRAPHS (OCT 2016)

The following paragraphs have been modified in this RLP:

LEASE NO. 36C26221L0002

INSTRUCTIONS TO OFFEROR: Do not attempt to complete this lease (GSA Lease Template L100, hereinafter Lease Template). Upon selection for award, GSA will transcribe the successful Offeror's final offered rent and other price data included on Offeror's submitted GSA Lease Proposal Form 1364, (hereinafter Lease Proposal Form) into a Lease Template, and transmit the completed Lease Template, together with appropriate attachments, to the successful Offeror for execution.

A. This Lease is made and entered into between

Lessor's Name

(Lessor), whose principal place of business is [ADDRESS], and whose interest in the Property described herein is that of Fee Owner, and
The United States of America

(Government), acting by and through the designated representative of the General Services Administration (GSA), upon the terms and conditions set forth herein.

B. Witnesseth: The parties hereto, for the consideration hereinafter mentioned, covenant and agree as follows:

Lessor hereby leases to the Government the Premises described herein, being all or a portion of the Property located at

[Address]

and more fully described in Section 1 and Exhibit B, together with rights to the use of parking and other areas as set forth herein, to be used for such purposes as determined by GSA.

C. LEASE TERM

To Have and To Hold the said Premises with its appurtenances for the term beginning upon acceptance of the Premises as required by this Lease and continuing for a period of

X Years, X Years Firm,

In Witness Whereof, the parties to this Lease evidence their agreement to all terms and conditions set forth herein by their signatures below, to be effective as of the date of delivery of the fully executed Lease to the Lessor.

FOR THE LESSOR:

FOR THE GOVERNMENT:

Name: _____
Title: _____
Entity: _____
Date: _____

Name: _____
Title: Lease Contracting Officer
General Services Administration, Public Buildings Service
Date: _____

WITNESSED FOR THE LESSOR BY:

Name: _____
Title: _____
Date: _____

The information collection requirements contained in this Solicitation/Contract, that are not required by the regulation, have been approved by the Office of Management and Budget pursuant to the Paperwork Reduction Act and assigned the OMB Control No. 3090-0163.

Exhibit A

subject to termination and renewal rights as may be hereinafter set forth. The commencement date of this Lease, along with any applicable termination and renewal rights, shall be more specifically set forth in a Lease Amendment upon substantial completion and acceptance of the Space by the Government.

SECTION 1	THE PREMISES, RENT, AND OTHER TERMS	5
1.01	THE PREMISES (OCT 2016)	5
1.02	EXPRESS APPURTENANT RIGHTS (SEP 2013)	5
1.03	RENT AND OTHER CONSIDERATION (OCT 2020)	6
1.04	BROKER COMMISSION AND COMMISSION CREDIT (OCT 2016) INTENTIONALLY DELETED	7
1.05	TERMINATION RIGHTS (OCT 2016)	7
1.06	RENEWAL RIGHTS (OCT 2016)	7
1.07	DOCUMENTS INCORPORATED IN THE LEASE (OCT 2020)	7
1.08	TENANT IMPROVEMENT RENTAL ADJUSTMENT (OCT 2016)	8
1.09	TENANT IMPROVEMENT FEE SCHEDULE (OCT 2020) INTENTIONALLY DELETED	8
1.10	BUILDING SPECIFIC AMORTIZED CAPITAL (SEP 2012) INTENTIONALLY DELETED	8
1.11	BUILDING SPECIFIC AMORTIZED CAPITAL RENTAL ADJUSTMENT (SEP 2013) INTENTIONALLY DELETED	8
1.12	PERCENTAGE OF OCCUPANCY FOR TAX ADJUSTMENT (OCT 2018)	8
1.13	REAL ESTATE TAX BASE (SEP 2013)	8
1.14	OPERATING COST BASE (OCT 2016)	9
1.15	RATE FOR ADJUSTMENT FOR VACANT LEASED PREMISES (SEP 2013)	9
1.16	HOURLY OVERTIME HVAC RATES (OCT 2016)	9
1.17	ADJUSTMENT FOR REDUCED SERVICES (OCT 2018)	9
1.18	BUILDING IMPROVEMENTS (MAR 2016)	9
1.19	HUBZONE SMALL BUSINESS CONCERNS ADDITIONAL PERFORMANCE REQUIREMENTS (MAR 2012)	9
1.20	LESSOR'S UNIQUE ENTITY IDENTIFIER (OCT 2020)	9
SECTION 2	GENERAL TERMS, CONDITIONS, AND STANDARDS	10
2.01	DEFINITIONS AND GENERAL TERMS (OCT 2016)	10
2.02	AUTHORIZED REPRESENTATIVES (OCT 2016)	11
2.03	ALTERATIONS REQUESTED BY THE GOVERNMENT (OCT 2018)	11
2.04	WAIVER OF RESTORATION (OCT 2018)	11
2.05	PAYMENT OF BROKER (JUL 2014) INTENTIONALLY DELETED	11
2.06	CHANGE OF OWNERSHIP/NOVATION (OCT 2020)	11
2.07	REAL ESTATE TAX ADJUSTMENT (JUN 2012)	11
2.08	ADJUSTMENT FOR VACANT PREMISES (OCT 2017)	13
2.09	OPERATING COSTS ADJUSTMENT (JUN 2012)	13
2.10	ADDITIONAL POST-AWARD FINANCIAL AND TECHNICAL DELIVERABLES (JUN 2012)	14
2.11	RELOCATION ASSISTANCE ACT (APR 2014) INTENTIONALLY DELETED	14
SECTION 3	CONSTRUCTION STANDARDS AND SHELL COMPONENTS	15
3.01	LABOR STANDARDS (OCT 2016) INTENTIONALLY DELETED	15
3.02	WORK PERFORMANCE (JUN 2012)	15
3.03	EXISTING FIT-OUT, SALVAGED, OR REUSED BUILDING MATERIAL (OCT 2019)	15
3.04	CONSTRUCTION WASTE MANAGEMENT (OCT 2019)	15
3.05	WOOD PRODUCTS (OCT 2019)	15
3.06	ADHESIVES AND SEALANTS (OCT 2019)	15
3.07	BUILDING SHELL REQUIREMENTS (OCT 2016)	16
3.08	RESPONSIBILITY OF THE LESSOR AND LESSOR'S ARCHITECT/ENGINEER (JUN 2012)	16
3.09	QUALITY AND APPEARANCE OF BUILDING (JUN 2012)	16
3.10	VESTIBULES (OCT 2020)	16
3.11	MEANS OF EGRESS (MAY 2015)	16
3.12	AUTOMATIC FIRE SPRINKLER SYSTEM (SEP 2013)	17
3.13	FIRE ALARM SYSTEM (SEP 2013)	17
3.14	ENERGY INDEPENDENCE AND SECURITY ACT (MAR 2016)	17
3.15	ELEVATORS (OCT 2020)	18
3.16	BUILDING DIRECTORY (APR 2011)	19
3.17	FLAGPOLE (SEP 2013)	Error! Bookmark not defined.
3.18	DEMOLITION (JUN 2012)	19
3.19	ACCESSIBILITY (FEB 2007)	19
3.20	CEILINGS (OCT 2019)	19
3.21	EXTERIOR AND COMMON AREA DOORS AND HARDWARE (SEP 2013)	19
3.22	DOORS: IDENTIFICATION (APR 2011)	19
3.23	WINDOWS (OCT 2020)	20
3.24	PARTITIONS: GENERAL (OCT 2019)	20
3.25	PARTITIONS: PERMANENT (OCT 2019)	20
3.26	INSULATION: THERMAL, ACOUSTIC, AND HVAC (OCT 2019)	20
3.27	WALL FINISHES – SHELL (SEP 2015)	20
3.28	PAINTING – SHELL (OCT 2019)	20
3.29	FLOORS AND FLOOR LOAD (OCT 2019)	21
3.30	FLOOR COVERING AND PERIMETERS – SHELL (SEP 2013)	21
3.31	MECHANICAL, ELECTRICAL, PLUMBING: GENERAL (APR 2011)	21
3.32	BUILDING SYSTEMS (APR 2011)	21
3.33	ELECTRICAL (OCT 2019)	21

3.34	ADDITIONAL ELECTRICAL CONTROLS (JUN 2012) INTENTIONALLY DELETED	21
3.35	PLUMBING (JUN 2012)	21
3.36	DRINKING FOUNTAINS (OCT 2018)	21
3.37	RESTROOMS (OCT 2020)	22
3.38	PLUMBING FIXTURES: WATER CONSERVATION (OCT 2019)	22
3.39	JANITOR CLOSETS (SEP 2015)	22
3.40	HEATING, VENTILATION, AND AIR CONDITIONING - SHELL (OCT 2020)	22
3.41	TELECOMMUNICATIONS: DISTRIBUTION AND EQUIPMENT (SEP 2015)	23
3.42	TELECOMMUNICATIONS: LOCAL EXCHANGE ACCESS (JUN 2012)	23
3.43	LIGHTING: INTERIOR AND PARKING - SHELL (OCT 2020)	23
3.44	ACOUSTICAL REQUIREMENTS (JUN 2012)	24
3.45	SECURITY FOR NEW CONSTRUCTION (OCT 2019) INTENTIONALLY DELETED	25
3.46	SEISMIC SAFETY FOR NEW CONSTRUCTION (OCT 2020) INTENTIONALLY DELETED	25
3.47	FIRE PROTECTION FOR NEW CONSTRUCTION (APR 2015) INTENTIONALLY DELETED	25
3.48	GREEN BUILDING RATING CERTIFICATION FOR NEW CONSTRUCTION (OCT 2016) INTENTIONALLY DELETED	25
3.49	GREEN BUILDING RATING CERTIFICATION FOR TENANT INTERIORS (OCT 2016)	25
3.50	INDOOR AIR QUALITY DURING CONSTRUCTION (OCT 2020)	25
3.51	SYSTEMS COMMISSIONING (APR 2011)	26
3.52	DUE DILIGENCE AND NATIONAL ENVIRONMENTAL POLICY ACT REQUIREMENTS – LEASE (SEP 2014)	26
3.53	NATIONAL HISTORIC PRESERVATION ACT REQUIREMENTS - LEASE (SEP 2014)	26
3.54	DESIGN EXCELLENCE – LEASE (OCT 2016) INTENTIONALLY DELETED	26
SECTION 4 DESIGN, CONSTRUCTION, AND POST AWARD ACTIVITIES		27
4.01	SCHEDULE FOR COMPLETION OF SPACE (OCT 2020)	27
4.02	CONSTRUCTION DOCUMENTS (SEP 2012)	28
4.03	TENANT IMPROVEMENTS PRICE PROPOSAL (OCT 2020) INTENTIONALLY DELETED	28
4.04	BUILDING SPECIFIC AMORTIZED CAPITAL (BSAC) PRICE PROPOSAL (SEP 2015) INTENTIONALLY DELETED	28
4.05	GREEN LEASE SUBMITTALS (OCT 2019)	28
4.06	CONSTRUCTION SCHEDULE AND INITIAL CONSTRUCTION MEETING (OCT 2020)	29
4.07	PROGRESS REPORTS (OCT 2020)	29
4.08	CONSTRUCTION INSPECTIONS (SEP 2015)	29
4.09	ACCESS BY THE GOVERNMENT PRIOR TO ACCEPTANCE (SEP 2013)	29
4.10	ACCEPTANCE OF SPACE AND CERTIFICATE OF OCCUPANCY (SEP 2015)	29
4.11	LEASE TERM COMMENCEMENT DATE AND RENT RECONCILIATION (JUN 2012)	29
4.12	AS-BUILT DRAWINGS (OCT 2019)	29
4.13	LIQUIDATED DAMAGES (JUN 2012)	30
4.14	SEISMIC RETROFIT (SEP 2013)	30
4.15	LESSOR'S PROJECT MANAGEMENT RESPONSIBILITIES (OCT 2020) INTENTIONALLY DELETED	30
SECTION 5 TENANT IMPROVEMENT COMPONENTS		31
5.01	TENANT IMPROVEMENT REQUIREMENTS (OCT 2016)	31
5.02	TENANT IMPROVEMENT SPECIFICATIONS (SEP 2015) INTENTIONALLY DELETED	31
5.03	FINISH SELECTIONS (SEP 2015)	31
5.04	WINDOW COVERINGS (JUN 2012)	31
5.05	DOORS: SUITE ENTRY (OCT 2019)	31
5.06	DOORS: INTERIOR (OCT 2019)	31
5.07	DOORS: HARDWARE (SEP 2013)	32
5.08	DOORS: IDENTIFICATION (JUN 2012)	32
5.09	PARTITIONS: SUBDIVIDING (OCT 2020)	32
5.10	WALL FINISHES (OCT 2019)	32
5.11	PAINTING – TI (OCT 2019)	32
5.12	FLOOR COVERINGS AND PERIMETERS (OCT 2019)	32
5.13	HEATING AND AIR CONDITIONING (JUN 2012)	33
5.14	ELECTRICAL: DISTRIBUTION (SEP 2015)	33
5.15	TELECOMMUNICATIONS: DISTRIBUTION AND EQUIPMENT (JUN 2012)	33
5.16	TELECOMMUNICATIONS: LOCAL EXCHANGE ACCESS (AUG 2008)	33
5.17	DATA DISTRIBUTION (OCT 2020)	33
5.18	ELECTRICAL, TELEPHONE, DATA FOR SYSTEMS FURNITURE (OCT 2020)	34
5.19	LIGHTING: INTERIOR AND PARKING – TI (SEP 2015)	34
5.20	AUTOMATIC FIRE SPRINKLER SYSTEM - TI (OCT 2016)	34
SECTION 6 UTILITIES, SERVICES, AND OBLIGATIONS DURING THE LEASE TERM		35
6.01	PROVISION OF SERVICES, ACCESS, AND NORMAL HOURS (JUN 2012)	35
6.02	UTILITIES (APR 2011)	35
6.03	UTILITIES SEPARATE FROM RENTAL BUILDING OPERATING PLAN (OCT 2020) INTENTIONALLY DELETED	35
6.04	UTILITY CONSUMPTION REPORTING (OCT 2016)	35
6.05	HEATING AND AIR CONDITIONING (OCT 2020)	35
6.06	OVERTIME HVAC USAGE (OCT 2020)	35
6.07	JANITORIAL SERVICES (JUL 2020)	36

Exhibit A

B. Antennas, Satellite Dishes, and Related Transmission Devices: (1) Space located on the roof of the Building sufficient in size for the installation and placement of telecommunications equipment, (2) the right to access the roof of the Building, and (3) use of all Building areas (e.g., chases, plenums, etc.) necessary for the use, operation, and maintenance of such telecommunications equipment at all times during the term of this Lease.

1.03 RENT AND OTHER CONSIDERATION (OCT 2020)

A. The Government shall pay the Lessor annual rent, payable in monthly installments in arrears, at the following rates:

	FIRM TERM	NON FIRM TERM
	ANNUAL RENT	ANNUAL RENT
SHELL RENT ¹	\$XXX,XXX.XX	\$XXX,XXX.XX
OPERATING COSTS ²	\$ XXX,XXX.XX	\$ XXX,XXX.XX
TENANT IMPROVEMENTS RENT ³	\$ XXX,XXX.XX	\$0.00
BUILDING SPECIFIC AMORTIZED CAPITAL (BSAC) ⁴	\$ XXX,XXX.XX	\$0.00
PARKING ⁵	\$ XXX,XXX.XX	\$ XXX,XXX.XX
ROUTINE CLEANING & DISINFECTING SERVICES ⁶	\$ XXX,XXX.XX	\$ XXX,XXX.XX
TOTAL ANNUAL RENT⁷	\$XXX,XXX.XX	\$XXX,XXX.XX

¹Shell rent calculation:

(Firm Term) \$XX per RSF multiplied by the RSF stated under Paragraph 1.01

(Non Firm Term) \$XX per RSF multiplied by the RSF stated under Paragraph 1.01

²Operating Costs rent calculation: \$XX per RSF multiplied by the RSF stated under Paragraph 1.01

³Tenant Improvements of \$XX are amortized at a rate of X percent per annum over XX years.

⁴Building Specific Amortized Capital (BSAC) of \$XX are amortized at a rate of X percent per annum over XX years

⁵Parking costs described under sub-paragraph B below

⁶Routine disinfecting rent described under sub-paragraph L below

⁷Total Annual Rent does not reflect reduction for free rent (if applicable). See subparagraph C below.

B. Parking shall be provided at a rate of \$XX per parking space per month (structured/inside), and \$XX per parking space per month (surface/outside).

C. The Lessor has offered free rent for the first XX (X) months of the Lease (free rent includes shell, operating, TI, BSAC and parking rent). Therefore, the first XX (X) months of the Lease shall be provided at no cost to the Government.

D. In instances where the Lessor amortizes either the TI or Building Specific Amortized Capital (BSAC) for a period exceeding the Firm Term of the Lease, should the Government terminate the Lease after the Firm Term or does not otherwise renew or extend the term beyond the Firm Term, the Government shall not be liable for any costs, including unamortized costs beyond the Firm Term.

E. Rent is subject to adjustment based upon a mutual on-site measurement of the Space upon acceptance, not to exceed XX ABOA SF based upon the methodology outlined under the "Payment" clause of GSA Form 3517.

F. Rent is subject to adjustment upon reconciliation from quantities in the Lease to the approved DIDs and post-DID change orders, based on unit prices negotiated and agreed upon prior to Lease award.

G. INTENTIONALLY DELETED

H. If the Government leases the Premises for less than a full calendar month, then rent shall be prorated based on the actual number of days leased for that month.

I. Rent shall be paid to Lessor by electronic funds transfer (EFT) in accordance with the provisions of the General Clauses. Rent shall be payable using the EFT information contained in the System for Award Management (SAM). In the event the EFT information changes, the Lessor shall be responsible for providing the updated information to SAM. Failure by the Lessor to maintain an active registration in SAM may result in delay of rental payments until such time as the SAM registration is activated.

J. Lessor shall provide to the Government, in exchange for the payment of rental and other specified consideration, the following:

1. The leasehold interest in the Property described herein in the paragraph entitled "The Premises."

2. All costs, expenses and fees to perform the work required for acceptance of the Premises in accordance with this Lease, including all costs for labor, materials, and equipment, professional fees, contractor fees, attorney fees, permit fees, inspection fees, and similar such fees, and all related expenses.

3. Performance or satisfaction of all other obligations set forth in this Lease; and all services, utilities, and maintenance required for the proper operation of the Property, the Building, and the Premises in accordance with the terms of the Lease, including, but not limited to, all inspections, modifications, repairs, replacements, and improvements required to be made thereto to meet the requirements of this Lease.

Exhibit A

VERSION 2: USE

K. For succeeding Leases with an incumbent Lessor where the Government is currently in occupancy and possession of the leased Premises and where the Lease requires the Lessor to perform alterations using either the TIA or BSAC, the amortized tenant improvement rent and/or BSAC rent will not commence until the alterations are complete and accepted by the Government. Upon acceptance of these improvements, the Government will commence payment of the tenant improvement and/or BSAC rent as stipulated under the Lease, in addition to payment of the tenant improvement and/or BSAC rent for the period starting from the Lease Term Commencement Date to the date of tenant improvements/BSAC acceptance by the Government (such rent payment will not include any additional interest). Alternatively, the Government may elect to re-amortize the tenant improvements/BSAC over the remaining Firm Term of the Lease, at the amortization rate stipulated in the Lease. In the event the Government does not use all the TIA or BSAC, then the rental payments will be adjusted in accordance with the provisions of the Lease (e.g., de-amortization).

L. The Lessor shall provide routine cleaning and disinfecting services, as outlined under sub-paragraph N of the paragraph entitled "Janitorial Services," at a rate of \$X.XX per rentable square foot. The Government reserves the right to issue notice to unilaterally cancel the routine cleaning and disinfecting at any time during the Lease term and, in such a case, the rental rate will be reduced by this amount. This reduction shall occur after the Government gives 30 calendar days notice to the Lessor and shall continue in effect until the Lease expires or is terminated.

1.04 ~~BROKER COMMISSION AND COMMISSION CREDIT (OCT 2016)~~ INTENTIONALLY DELETED

1.05 TERMINATION RIGHTS (OCT 2016)

The Government may terminate this Lease, in whole or in parts, at any time effective after the Firm Term of this Lease, by providing not less than XX days' prior written notice to the Lessor. The effective date of the termination shall be the day following the expiration of the required notice period or the termination date set forth in the notice, whichever is later. No rental shall accrue after the effective date of termination.

1.06 RENEWAL RIGHTS (OCT 2016)

A. This Lease may be renewed at the option of the Government for a term of XX YEARS at the following rental rate(s):

	OPTION TERM, YEARS XX - XX	
	ANNUAL RENT	ANNUAL RATE / RSF
SHELL RENTAL RATE	\$XX	\$XX
OPERATING COSTS	OPERATING COST BASE SHALL CONTINUE FROM THE EFFECTIVE YEAR OF THE LEASE. OPTION TERM IS SUBJECT TO CONTINUING ANNUAL ADJUSTMENTS.	

provided notice is given to the Lessor at least XX days before the end of the original Lease term or any extension thereof; all other terms and conditions of this Lease, as same may have been amended, shall remain in full force and effect during any renewal term.

B. Termination rights outlined in the "Termination Rights" paragraph apply to all renewal terms.

1.07 DOCUMENTS INCORPORATED IN THE LEASE (OCT 2020)

The following documents are attached to and made part of the Lease:

DOCUMENT NAME	NO. OF PAGES	EXHIBIT
LEASE NO. 36C26221L002 (TEMPLATE L100)	43	A
AGENCY'S REQUIREMENTS	56	B
SECURITY REQUIREMENTS FOR LEVEL 2	109	C
GSA FORM 3516, SOLICITATION PROVISIONS	5	D
GSA FORM 3517B, GENERAL CLAUSES	15	E
PROPOSAL TO LEASE SPACE (GSA FORM 1364)	6	F
GSA FORM 1217, LESSOR'S ANNUAL COST STATEMENT	4	G
GSA FORM 12000 FOR PRELEASE FIRE PROTECTION AND LIFE SAFETY EVALUATION FOR AN OFFICE BUILDING (PART A OR PART B) (SEE SECTION 3 FOR APPLICABLE REQUIREMENTS)	7	H
SEISMIC OFFER FORMS	10	I
COVERED TELECOMMUNICATIONS EQUIPMENT OR SERVICES REPRESENTATION	1	J
ADA CERTIFICATION	1	K
PRE LEASE BUILDING SECURITY PLAN	6	L
SAFETY ENVIRONMENTAL CHECKLIST	4	M
INFECTION CONTROL RISK ASSESSMENT	10	N
RATE FOR ROUTINE CLEANING AND DISINFECTING REQUIREMENTS	1	O

1.08 TENANT IMPROVEMENT RENTAL ADJUSTMENT (OCT 2016)

- A. The Lessor has agreed to total TI pricing of **\$XX,XXX** based on the Agency's Requirements and design schematic included in Exhibit **X**. This amount is amortized in the rent over the Firm Term of this Lease at an interest rate of **X** percent per year.
- B. The TI Unit Prices listed in Exhibit **X** will be used to make the adjustment for variances between TI turnkey pricing based on the Agency's Requirements and the approved design intent drawings. The prices quoted will also be used to order alterations during the first year of the Lease. The prices quoted shall be the cost to furnish, install, and maintain each item, unless otherwise specified. These prices may be indexed or renegotiated to apply to subsequent years of the Lease upon mutual agreement of the Lessor and the Government. Final rent calculations will be reconciled and the Lease will be amended after acceptance of the Space.
- C. The Government may elect to make lump sum payments for any or all work covered by the TI scope. That part of the TI amortized in the rent shall be reduced accordingly. At any time after occupancy and during the Firm Term of the Lease, the Government, at its sole discretion, may elect to pay lump sum for any part or all of the remaining unpaid amortized balance of the TI. If the Government elects to make a lump sum payment for the TI after occupancy, the payment of the TI by the Government will result in a decrease in the rent according to the amortization rate over the Firm Term of the Lease.

1.09 ~~TENANT IMPROVEMENT FEE SCHEDULE (OCT 2020)~~ INTENTIONALLY DELETED

1.10 ~~BUILDING SPECIFIC AMORTIZED CAPITAL (SEP 2012)~~ INTENTIONALLY DELETED

1.11 ~~BUILDING SPECIFIC AMORTIZED CAPITAL RENTAL ADJUSTMENT (SEP 2013)~~ INTENTIONALLY DELETED

1.12 PERCENTAGE OF OCCUPANCY FOR TAX ADJUSTMENT (OCT 2018)

- A. As of the Lease Award Date, the Government's Percentage of Occupancy, as defined in the "Real Estate Tax Adjustment" paragraph of this Lease is **XX** percent. The Percentage of Occupancy is derived by dividing the total Government Space of **XX** RSF by the total Building space of **XX** RSF. The tax parcel number is **XX**.
- B. All relevant tax adjustment documentation (e.g., copies of paid tax receipts, invoices) must be submitted online via the GSA Real Estate Tax Portal at RET.GSA.GOV.

1.13 REAL ESTATE TAX BASE (SEP 2013)

The Real Estate Tax Base, as defined in the "Real Estate Tax Adjustment" paragraph of the Lease is **\$XX**. Tax adjustments shall not occur until the tax year following lease commencement has passed.

Exhibit A

1.14 OPERATING COST BASE (OCT 2016)

The parties agree, for the purpose of applying the paragraph titled "Operating Costs Adjustment," that the Lessor's base rate for operating costs shall be \$XX.XX per RSF.

1.15 RATE FOR ADJUSTMENT FOR VACANT LEASED PREMISES (SEP 2013)

In accordance with the paragraph entitled "Adjustment for Vacant Premises," if the Government fails to occupy or vacates the entire or any portion of the Premises prior to expiration of the term of the Lease, the operating costs paid by the Government as part of the rent shall be reduced by \$XX.XX per ABOA SF of Space vacated by the Government.

1.16 HOURLY OVERTIME HVAC RATES (OCT 2016)

A. The following rates shall apply in the application of the paragraph titled "Overtime HVAC Usage:"

- \$X.XX per hour per zone
- No. of zones: X
- \$ X.XX per hour for the entire Space.

B. There is no overtime charge during the following weekend hours:

Saturday: X AM through X PM

Sunday: X AM through X PM.

1.17 ADJUSTMENT FOR REDUCED SERVICES (OCT 2018)

This Lease provides for normal hours of operation as outlined under Lease Paragraph 6.01, Provision of Services, Access, and Normal Hours. In the event the Government requires the following normal hours of operations: [XX AM to XX PM, Monday through Friday, with the exception of Federal holidays], the rental rate and the base for operating cost adjustments will be reduced by \$XX per ABOA SF, adjusted to include any CPI adjustment as outlined under Lease paragraph entitled Operating Costs Adjustment. This reduction shall occur after the Government gives 30 calendar days' prior notice to the Lessor and shall continue in effect until the Lease expires or is terminated.

1.18 BUILDING IMPROVEMENTS (MAR 2016)

Before the Government accepts the Space, the Lessor shall complete the following additional Building improvements:

- A. _____
- B. _____
- C. _____

1.19 HUBZONE SMALL BUSINESS CONCERNS ADDITIONAL PERFORMANCE REQUIREMENTS (MAR 2012)

If the Lessor is a qualified HUBZone small business concern (SBC) that did not waive the price evaluation preference then as required by 13 C.F.R. 126.700, the HUBZone SBC must spend at least 50% of the cost of the contract incurred for personnel on its own employees or employees of other qualified HUBZone SBC's and must meet the performance of the work requirements for subcontracting in 13 C.F.R. § 125.6(c). If the Lessor is a HUBZone joint venture, the aggregate of the qualified HUBZone SBC's to the joint venture, not each concern separately, must perform the applicable percentage of work required by this clause.

1.20 LESSOR'S UNIQUE ENTITY IDENTIFIER (OCT 2020)

Lessor's Unique Entity Identifier (currently referred to as a Dun & Bradstreet DUNS Number): XXXXXXXXX.

SECTION 2 GENERAL TERMS, CONDITIONS, AND STANDARDS

2.01 DEFINITIONS AND GENERAL TERMS (OCT 2016)

Unless otherwise specifically noted, all terms and conditions set forth in this Lease shall be interpreted by reference to the following definitions, standards, and formulas:

- A. Appurtenant Areas. Appurtenant Areas are defined as those areas and facilities on the Property that are not located within the Premises, but for which rights are expressly granted under this Lease, or for which rights to use are reasonably necessary or reasonably anticipated with respect to the Government's enjoyment of the Premises and express appurtenant rights.
- B. Broker. If GSA awarded this Lease using a contract real estate broker, Broker shall refer to GSA's broker.
- C. Building. Building(s) situated on the Property in which the Premises are located.
- D. Commission Credit. If GSA awarded this Lease using a Broker, and the Broker agreed to forego a percentage of its commission to which it is entitled in connection with the award of this Lease, the amount of this credit is referred to as the "Commission Credit."
- E. Common Area Factor. The "Common Area Factor" (CAF) is a conversion factor determined by the Building owner and applied by the owner to the ABOA SF to determine the RSF for the leased Space. The CAF is expressed as a percentage of the difference between the amount of rentable SF and ABOA SF, divided by the ABOA SF. For example 11,500 RSF and 10,000 ABOA SF will have a CAF of 15% [(11,500 RSF-10,000 ABOA SF)/10,000 ABOA SF]. For the purposes of this Lease, the CAF shall be determined in accordance with the applicable ANSI/BOMA standard for the type of space to which the CAF shall apply.
- F. Contract. "Contract" shall mean this Lease.
- G. Contractor. "Contractor" shall mean Lessor.
- H. Days. All references to "day" or "days" in this Lease shall mean calendar days, unless specified otherwise.
- I. FAR. All references to the FAR shall be understood to mean the Federal Acquisition Regulation, codified at 48 CFR Chapter 1.
- J. Firm Term/Non-Firm Term. The Firm Term is that part of the Lease term that is not subject to termination rights. The Non-Firm Term is that part of the Lease term following the end of the Firm Term.
- K. GSAR. All references to the GSAR shall be understood to mean the GSA supplement to the FAR, codified at 48 CFR Chapter 5.
- L. Lease Term Commencement Date. The date on which the lease term commences.
- M. Lease Award Date. The date the LCO executes the Lease and mails or otherwise furnishes written notification of the executed Lease to the successful Offeror (date on which the parties' obligations under the Lease begin).
- N. Premises. The Premises are defined as the total Office Area or other type of Space, together with all associated common areas, described in Section 1 of this Lease, and delineated by plan in the attached exhibit. Parking and other areas to which the Government has rights under this Lease are not included in the Premises.
- O. Property. Defined as the land and Buildings in which the Premises are located, including all Appurtenant Areas (e.g., parking areas) to which the Government is granted rights.
- P. Rentable Space or Rentable Square Feet (RSF). Rentable Space is the area for which a tenant is charged rent. It is determined by the Building owner and may vary by city or by building within the same city. The Rentable Space may include a share of Building support/common areas such as elevator lobbies, Building corridors, and floor service areas. Floor service areas typically include restrooms, janitor rooms, telephone closets, electrical closets, and mechanical rooms. The Rentable Space does not include vertical building penetrations and their enclosing walls, such as stairs, elevator shafts, and vertical ducts. Rentable Square Feet is calculated using the following formula for each type of Space (e.g., office, warehouse, etc.) included in the Premises: ABOA SF of Space x (1 + CAF) = RSF.
- Q. Space. The Space shall refer to that part of the Premises to which the Government has exclusive use, such as Office Area, or other type of Space. Parking areas to which the Government has rights under this Lease are not included in the Space.
- R. Office Area. For the purposes of this Lease, Space shall be measured in accordance with the standard (Z65.1-1996) provided by American National Standards Institute/Building Owners and Managers Association (ANSI/BOMA) for Office Area, which means "the area where a tenant normally houses personnel and/or furniture, for which a measurement is to be computed." References to ABOA mean ANSI/BOMA Office Area.
- S. Working Days. Working Days shall mean weekdays, excluding Saturdays and Sundays and Federal holidays.

Exhibit A

2.02 AUTHORIZED REPRESENTATIVES (OCT 2016)

Signatories to this Lease shall have full authority to bind their respective principals with regard to all matters relating to this Lease. No other persons shall be understood to have any authority to bind their respective principals, except to the extent that such authority may be explicitly delegated by notice to the other party, or to the extent that such authority is transferred by succession of interest. The Government shall have the right to substitute its Lease Contracting Officer (LCO) by notice, without an express delegation by the prior LCO.

2.03 ALTERATIONS REQUESTED BY THE GOVERNMENT (OCT 2018)

A. The Government may request the Lessor to provide alterations during the term of the Lease. Alterations will be ordered by issuance of a Lease Amendment, GSA Form 300, Order for Supplies or Services, or a tenant agency-approved form when specifically authorized to do so by the LCO. The General Services Administration Acquisition Manual ("GSAM") clause, 552.270-31, Prompt Payment, including its invoice requirements, shall apply to orders for alterations. All orders are subject to the terms and conditions of this Lease and may be placed by the LCO or a warranted contracting officer's representative (COR) in GSA or the tenant agency when specifically authorized to do so by the LCO, subject to the threshold limitation below.

B. Orders for alterations issued by an authorized COR are limited to no more than \$250,000 (LCOs are not subject to this threshold). This threshold will change according to future adjustments of the simplified acquisition threshold (see FAR 2.101). The LCO will provide the Lessor with a list of tenant agency officials authorized to place orders and will specify any limitations on the authority delegated to tenant agency officials. The tenant agency officials are not authorized to deal with the Lessor on any other matters.

C. Payments for alterations ordered by the tenant agency under the authorization described in sub-paragraph B will be made directly by the tenant agency placing the order.

2.04 WAIVER OF RESTORATION (OCT 2018)

Lessor shall have no right to require the Government to restore the Premises upon expiration or earlier termination (full or partial) of the Lease, and waives all claims against the Government for waste, damages, or restoration arising from or related to (a) the Government's normal and customary use of the Premises during the term of the Lease (including any extensions thereof), as well as (b) any initial or subsequent alteration to the Premises regardless of whether such alterations are performed by the Lessor or by the Government. At its sole option, the Government may abandon property in the Space following expiration or earlier termination (full or partial) of the Lease, in which case the property will become the property of the Lessor and the Government will be relieved of any liability in connection therewith.

2.05 ~~PAYMENT OF BROKER (JUL 2014)~~ INTENTIONALLY DELETED

2.06 CHANGE OF OWNERSHIP/NOVATION (OCT 2020)

A. If during the term of the Lease, title to the Property is transferred or the Lessor changes its legal name, the Lessor and its successor shall comply with the requirements of FAR Subpart 42.12. If title is transferred, the Lessor shall notify the Government within five days of the transfer of title.

B. The Government and the Lessor may execute a Change of Name Agreement if the Lessor is changing only its legal name, and the Government's and the Lessor's respective rights and obligations remain unaffected.

C. If title to the Property is transferred, the Government, the original Lessor (Transferor), and the new owner or assignee (Transferee) shall execute a Novation Agreement providing for the transfer of Transferor's rights and obligations under the Lease to the Transferee. When executed on behalf of the Government, a Novation Agreement will be made part of the Lease via Lease Amendment.

D. In addition to all documents required by FAR 42.1204, the LCO may request additional information (e.g., copy of the deed, bill of sale, certificate of merger, contract, court decree, articles of incorporation, operation agreement, partnership certificate of good standing, etc.) from the Transferor or Transferee to verify the parties' representations regarding the transfer, and to determine whether the transfer of the Lease is in the Government's interest.

E. If the LCO determines that recognizing the Transferee as the Lessor will not be in the Government's interest, the Transferor shall remain fully liable to the Government for the Transferee's performance of obligations under the Lease, notwithstanding the transfer. Under no condition shall the Government be obligated to release the Transferor of obligations prior to (a) the rent commencement date; and (b) any amounts due and owing to the Government under the Lease that have been paid in full or completely set off against the rental payments due under the Lease.

F. As a condition for being recognized as the Lessor and entitlement to receiving rent, the Transferee must register in the System for Award Management (SAM) for purposes of "All Awards" (See FAR 52.232-33), and complete all required representations and certifications within SAM. In addition, the Transferee must also complete a Foreign Ownership and Financing Representation.

G. If title to the Property is transferred, rent shall continue to be paid to the original Lessor, subject to the Government's rights as provided for in this Lease. The Government's obligation to pay rent to the Transferee shall commence on the effective date of the Lease Amendment incorporating the Novation Agreement. The Lease Amendment will not be issued until the Government has received all information reasonably required by the LCO, the Government has determined that recognizing the Transferee as the Lessor is in the Government's interest (which determination will be prompt and not unreasonably withheld), and the Transferee has met all conditions specified in sub-paragraph F. The original Lessor must maintain an active registration in SAM until the Novation process is complete.

2.07 REAL ESTATE TAX ADJUSTMENT (JUN 2012)

Exhibit A

A. Purpose: This paragraph provides for adjustment in the rent (tax adjustment) to account for increases or decreases in Real Estate Taxes for the Property after the establishment of the Real Estate Tax Base, as those terms are defined herein. Tax adjustments shall be calculated in accordance with this paragraph.

B. Definitions: The following definitions apply to the use of the terms within this paragraph:

Property is defined as the land and Buildings in which the Premises are located, including all Appurtenant Areas (e.g., parking areas to which the Government is granted rights).

Real Estate Taxes are those taxes that are levied upon the owners of real property by a Taxing Authority (as hereinafter defined) of a state or local Government on an ad valorem basis to raise general revenue for funding the provision of government services. The term excludes, without limitation, special assessments for specific purposes, assessments for business improvement districts, and/or community development assessments.

Taxing Authority is a state, commonwealth, territory, county, city, parish, or political subdivision thereof, authorized by law to levy, assess, and collect Real Estate Taxes.

Tax Year refers to the 12-month period adopted by a Taxing Authority as its fiscal year for assessing Real Estate Taxes on an annual basis.

Tax Abatement is an authorized reduction in the Lessor's liability for Real Estate Taxes below that determined by applying the generally applicable real estate tax rate to the Fully Assessed (as hereinafter defined) valuation of the Property.

Unadjusted Real Estate Taxes are the full amount of Real Estate Taxes that would be assessed for the Property for one full Tax Year without regard to the Lessor's entitlement to any Tax Abatements (except if such Tax Abatement came into effect after the date of award of the Lease), and not including any late charges, interest or penalties. If a Tax Abatement comes into effect after the date of award of the Lease, "unadjusted Real Estate Taxes" are the full amount of Real Estate Taxes assessed for the Property for one full Tax Year, less the amount of such Tax Abatement, and not including any late charges, interest, or penalties.

Real Estate Tax Base is the unadjusted Real Estate Taxes for the first full Tax Year following the commencement of the Lease term. If the Real Estate Taxes for that Tax Year are not based upon a Full Assessment of the Property, then the Real Estate Tax Base shall be the Unadjusted Real Estate Taxes for the Property for the first full Tax Year for which the Real Estate Taxes are based upon a Full Assessment. Such first full Tax Year may be hereinafter referred to as the Tax Base Year. Alternatively, the Real Estate Tax Base may be an amount negotiated by the parties that reflects an agreed upon base for a Fully Assessed value of the Property.

The Property is deemed to be Fully Assessed (and Real Estate Taxes are deemed to be based on a Full Assessment) only when a Taxing Authority has, for the purpose of determining the Lessor's liability for Real Estate Taxes, determined a value for the Property taking into account the value of all improvements contemplated for the Property pursuant to the Lease, and issued to the Lessor a tax bill or other notice of levy wherein the Real Estate Taxes for the full Tax Year are based upon such Full Assessment. At no time prior to the issuance of such a bill or notice shall the Property be deemed Fully Assessed.

Percentage of Occupancy refers to that portion of the Property exclusively occupied or used by the Government pursuant to the Lease. For Buildings, the Percentage of Occupancy is determined by calculating the ratio of the RSF occupied by the Government pursuant to the Lease to the total RSF in the Building or Buildings so occupied, and shall not take into account the Government's ancillary rights including, but not limited to, parking or roof space for antennas (unless facilities for such ancillary rights are separately assessed). This percentage shall be subject to adjustment to take into account increases or decreases for Space leased by the Government or for rentable space on the Property.

C. Adjustment for changes in Real Estate Taxes. After the Property is Fully Assessed, the Government shall pay its share of any increases and shall receive its share of any decreases in the Real Estate Taxes for the Property, such share of increases or decreases to be referred to herein as "tax adjustment." The amount of the tax adjustment shall be determined by multiplying the Government's Percentage of Occupancy by the difference between the current year Unadjusted Real Estate Taxes and the Real Estate Tax Base, less the portion of such difference not paid due to a Tax Abatement (except if a Tax Abatement comes into effect after the date of award of the Lease). If a Tax Abatement comes into effect after the date of award of the Lease, the amount of the tax adjustment shall be determined by multiplying the Government's Percentage of Occupancy by the difference between the current year Unadjusted Real Estate Taxes and the Real Estate Tax Base. The Government shall pay the tax adjustment in a single annual lump sum payment to the Lessor. In the event that this tax adjustment results in a credit owed to the Government, the Government may elect to receive payment in the form of a rental credit or lump sum payment.

If the Property contains more than one separately assessed parcel, then more than one tax adjustment shall be determined based upon the Percentage of Occupancy, Real Estate Tax Base, and Real Estate Taxes for each respective parcel.

After commencement of the Lease term, the Lessor shall provide to the LCO copies of all real estate tax bills for the Property, all documentation of Tax Abatements, credits, or refunds, if any, and all notices which may affect the assessed valuation of the Property, for the Tax Year prior to the commencement of the Lease Term, and all such documentation for every year following. Lessor acknowledges that the LCO shall rely on the completeness and accuracy of these submissions in order to establish the Real Estate Tax Base and to determine tax adjustments. The LCO may memorialize the establishment of the Real Estate Tax Base by issuing a unilateral administrative lease amendment indicating the base year, the amount of the Real Estate Tax Base, and the Government's Percentage of Occupancy.

The Real Estate Tax Base is subject to adjustment when increases or decreases to Real Estate Taxes in any Tax Year are attributable to (a) improvements or renovations to the Property not required by this Lease, or (b) changes in net operating income for the Property not derived from this Lease. If either condition results in a change to the Real Estate Taxes, the LCO may re-establish the Real Estate Tax Base as the Unadjusted Real Estate Taxes for the Tax Year the Property is reassessed under such condition, less the amount by which the Unadjusted Real Estate Taxes for the Tax Year prior to reassessment exceeds the prior Real Estate Tax Base.

Exhibit A

If this Lease includes any options to renew the term of the Lease, or be otherwise extended, the Real Estate Tax Base for determining tax adjustments during the renewal term or extension shall be the last Real Estate Tax Base established during the base term of the Lease.

If any Real Estate Taxes for the Property are retroactively reduced by a Taxing Authority during the term of the Lease, the Government shall be entitled to a proportional share of any tax refunds to which the Lessor is entitled, calculated in accordance with this Paragraph. Lessor acknowledges that it has an affirmative duty to disclose to the Government any decreases in the Real Estate Taxes paid for the Property during the term of the Lease. Lessor shall annually provide to the LCO all relevant tax records for determining whether a tax adjustment is due, irrespective of whether it seeks an adjustment in any Tax Year.

If the Lease terminates before the end of a Tax Year, or if rent has been suspended, payment for the real estate tax increase due because of this section for the Tax Year will be prorated based on the number of days that the Lease and the rent were in effect. Any credit due the Government after the expiration or earlier termination of the Lease shall be made by a lump sum payment to the Government or as a rental credit to any succeeding Lease, as determined in the LCO's sole discretion. Lessor shall remit any lump sum payment to the Government within 15 calendar days of payment or credit by the Taxing Authority to Lessor or Lessor's designee. If the credit due to the Government is not paid by the due date, interest shall accrue on the late payment at the rate established by the Secretary of the Treasury under Section 12 of the Contract Disputes Act of 1978, as amended (41 USC § 611), that is in effect on the day after the due date. The interest penalty shall accrue daily on the amount of the credit and shall be compounded in 30-day increments inclusive from the first day after the due date through the payment date. The Government shall have the right to pursue the outstanding balance of any tax credit using all such collection methods as are available to the United States to collect debts. Such collection rights shall survive the expiration of this Lease.

In order to obtain a tax adjustment, the Lessor shall furnish the LCO with copies of all paid tax receipts, or other similar evidence of payment acceptable to the LCO, and a proper invoice (as described in GSA Form 3517, General Clauses, 552.270-31, Prompt Payment) for the requested tax adjustment, including the calculation thereof. All such documents must be received by the LCO within 60 calendar days after the last date the real estate tax payment is due from the Lessor to the Taxing Authority without payment of penalty or interest. FAILURE TO SUBMIT THE PROPER INVOICE AND EVIDENCE OF PAYMENT WITHIN SUCH TIME FRAME SHALL CONSTITUTE A WAIVER OF THE LESSOR'S RIGHT TO RECEIVE A TAX ADJUSTMENT PURSUANT TO THIS PARAGRAPH FOR THE TAX YEAR AFFECTED.

Tax Appeals. If the Government occupies more than 50 percent of the Building by virtue of this and any other Government Lease(s), the Government may, upon reasonable notice, direct the Lessor to initiate a tax appeal, or the Government may elect to contest the assessed valuation on its own behalf or jointly on behalf of Government and the Lessor. If the Government elects to contest the assessed valuation on its own behalf or on behalf of the Government and the Lessor, the Lessor shall cooperate fully with this effort, including, without limitation, furnishing to the Government information necessary to contest the assessed valuation in accordance with the filing requirements of the Taxing Authority, executing documents, providing documentary and testimonial evidence, and verifying the accuracy and completeness of records. If the Lessor initiates an appeal at the direction of the Government, the Government shall have the right to approve the selection of counsel who shall represent the Lessor with regard to such appeal, which approval shall not be unreasonably withheld, conditioned or delayed, and the Lessor shall be entitled to a credit in the amount of its reasonable expenses in pursuing the appeal.

2.08 ADJUSTMENT FOR VACANT PREMISES (OCT 2017)

A. If the Government fails to occupy any portion of the leased Premises or vacates the Premises in whole or in part prior to expiration of the term of the Lease, the rental rate and the base for operating cost adjustments will be reduced using the figure specified in the "Rate for Adjustment for Vacant Leased Premises" paragraph of this Lease.

B. If no rate reduction has been established in this Lease, the rate will be reduced by that portion of the costs per ABOA SF of operating expenses not required to maintain the Space.

C. Said reduction shall occur after the Government gives 30 calendar days' prior notice to the Lessor and shall continue in effect until the Government occupies the vacant Premises or the Lease expires or is terminated.

2.09 OPERATING COSTS ADJUSTMENT (JUN 2012)

A. Beginning with the second year of the Lease and each year thereafter, the Government shall pay annual incremental adjusted rent for changes in costs for cleaning services, supplies, materials, maintenance, trash removal, landscaping, water, sewer charges, heating, electricity, and certain administrative expenses attributable to occupancy.

B. The amount of adjustment will be determined by multiplying the base rate by the annual percent of change in the Cost of Living Index. The percent change will be computed by comparing the index figure published for the month prior to the Lease Term Commencement Date with the index figure published for the month prior which begins each successive 12-month period. For example, a Lease which commences in June of 2005 would use the index published for May of 2005, and that figure would be compared with the index published for May of 2006, May of 2007, and so on, to determine the percent change. The Cost of Living Index will be measured by the Department of Labor revised Consumer Price Index for Urban Wage Earners and Clerical Workers (CPI-W), U.S. city average, all items, (1982 to 1984 = 100) published by the Bureau of Labor Statistics. Payment will be made with the monthly installment of fixed rent. Rental adjustments will be effective on the anniversary date of the Lease; however, payment of the adjusted rental rate will become due on the first workday of the second month following the publication of the Cost of Living Index for the month prior to the commencement of each 12-month period.

C. In the event of any decreases in the Cost of Living Index occurring during the term of the occupancy under the Lease, the rental amount will be reduced accordingly. The amount of such reductions will be determined in the same manner as increases in rent provided under this paragraph.

D. If the Government exercises an option to extend the Lease term at the same rate as that of the original term, the option price will be based on the adjustment during the original term. Annual adjustments will continue.

2.10 ADDITIONAL POST-AWARD FINANCIAL AND TECHNICAL DELIVERABLES (JUN 2012)

A. If the Lessor is a HUBZone small business concern (SBC) that did not waive the price evaluation preference, the Lessor shall provide a certification within 10 days after Lease award to the LCO (or representative designated by the LCO) that the Lessor was an eligible HUBZone SBC on the date of award. If it is determined within 20 days after award that a HUBZone SBC Offeror that has been awarded the Lease was not an eligible HUBZone SBC at the time of award, and the HUBZone SBC Lessor failed to provide the LCO with information regarding a change to its HUBZone eligibility prior to award, then the Lease shall be subject, at the LCO's discretion, to termination, and the Government will be relieved of all obligations to the Lessor in such an event and not be liable to the Lessor for any costs, claims or damages of any nature whatsoever.

B. Within **XX** days after Lease award, the Lessor shall provide to the LCO (or representative designated by the LCO) evidence of:

1. A firm commitment of funds in an amount sufficient to perform the work.
2. The names of at least two proposed construction contractors, as well as evidence of the contractors' experience, competency, and performance capabilities with construction similar in scope to that which is required herein.
3. The license or certification to practice in the state where the Building is located from the individual(s) and/or firm(s) providing architectural and engineering design services.

C. The Government shall have the right to withhold approval of design intent drawings (DIDs) until the conditions specified in sub-paragraphs A and B have been satisfied.

D. Within ten (10) calendar days after the LCO issues the Notice To Proceed (NTP) for TI construction, the Lessor shall provide to the LCO evidence of:

1. Award of a construction contract for TIs with a firm completion date. This date must be in accordance with the construction schedule for TIs as described in the "Schedule for Completion of Space" paragraph of this Lease.
2. Issuance of required permits for construction of the TIs.

2.11 ~~RELOCATION ASSISTANCE ACT (APR 2014)~~ INTENTIONALLY DELETED

SECTION 3 CONSTRUCTION STANDARDS AND SHELL COMPONENTS

3.01 ~~LABOR STANDARDS (OCT 2016)~~ INTENTIONALLY DELETED**3.02 WORK PERFORMANCE (JUN 2012)**

All work in performance of this Lease shall be done by skilled workers or mechanics and shall be acceptable to the LCO. The LCO may reject the Lessor's workers 1) if such are unlicensed, unskilled, or otherwise incompetent, or 2) if such have demonstrated a history of either untimely or otherwise unacceptable performance in connection with work carried out in conjunction with either this contract or other government or private contracts.

3.03 EXISTING FIT-OUT, SALVAGED, OR REUSED BUILDING MATERIAL (OCT 2019)

A. Items and materials existing in the Premises, or to be removed from the Premises during the demolition phase, are eligible for reuse in the construction phase of the project. The reuse of items and materials is preferable to recycling them; however, items considered for reuse shall be in refurbished condition and shall meet the quality standards set forth by the Government in this Lease. In the absence of definitive quality standards, the Lessor is responsible to confirm that the quality of the item(s) in question shall meet or exceed accepted industry or trade standards for first quality commercial grade applications.

B. Unless waived by the LCO, the Lessor shall submit a reuse plan for leases 10,000 RSF or greater. The Government will not pay for existing fixtures and other TIs accepted in place. However, the Government will reimburse the Lessor, as part of the TIA, the costs to repair or improve such fixtures or improvements identified on the reuse plan and approved by the LCO.

3.04 CONSTRUCTION WASTE MANAGEMENT (OCT 2019)

A. For leases 10,000 RSF or greater, recycling construction waste is mandatory for initial space alterations for TIs and subsequent alterations under the Lease.

B. **SUBMITTAL REQUIREMENT:** Prior to construction commencement, a proposed plan following industry standards to recycle construction waste. The construction waste management plan shall quantify material diversion goals and maximize the materials to be recycled and/or salvaged (at least 50 percent) from construction, demolition, and packaging debris. Where the small quantity of material, the extraordinarily complex nature of the waste disposal method, or prohibitive expense for recycling would represent a genuine hardship, the Government, upon written request of the Lessor and approval of the LCO, may permit alternative means of disposal.

C. The Lessor shall recycle the following items during both the demolition and construction phases of the project, subject to economic evaluation and feasibility: Ceiling grid and tile, light fixtures, including proper disposal of any transformers, ballasts, and fluorescent light bulbs, duct work and HVAC equipment, wiring and electrical equipment, aluminum and/or steel doors and frames, hardware, drywall, steel studs, carpet, carpet backing, and carpet padding, wood, insulation, cardboard packaging, pallets, windows and glazing materials, all miscellaneous metals (as in steel support frames for filing equipment), and all other finish and construction materials.

D. If any waste materials encountered during the demolition or construction phase are found to contain lead, asbestos, polychlorinated biphenyls (PCBs) (such as fluorescent lamp ballasts), or other harmful substances, they shall be handled and removed in accordance with Federal and state laws and requirements concerning hazardous waste.

E. In addition to providing "one time" removal and recycling of large scale demolition items such as carpeting or drywall, the Lessor shall provide continuous facilities for the recycling of incidental construction waste during the initial construction.

F. Construction materials recycling records shall be maintained by the Lessor and shall be accessible to the LCO. Records shall include materials recycled or land-filled, quantity, date, and identification of hazardous wastes.

3.05 WOOD PRODUCTS (OCT 2019)

A. Particle board, strawboard, and plywood materials used shall be free of formaldehyde or sufficiently aged prior to use such that indoor air levels in the finished leased space shall not exceed 0.016 parts per million (ppm) of formaldehyde.

B. All materials comprised of combustible substances, such as wood plywood and wood boards, shall be treated with fire retardant chemicals by a pressure impregnation process or other methods that treats the materials throughout as opposed to surface treatment.

C. For leases 10,000 RSF or greater, new installations of wood products shall not contain wood from endangered wood species, as listed by the Convention on International Trade in Endangered Species. The list of species can be found at [HTTP://WWW.WOOD-DATABASE.COM/WOOD-ARTICLES/RESTRICTED-AND-ENDANGERED-WOOD-SPECIES/](http://www.wood-database.com/wood-articles/restricted-and-endangered-wood-species/) or [HTTPS://WWW.FWS.GOV/INTERNATIONAL/PLANTS/CURRENT-CITES-LISTINGS-OF-TREE-SPECIES.HTML](https://www.fws.gov/international/plants/current-cites-listings-of-tree-species.html). In addition, the Lessor is encouraged to use independently certified forest products. For information on certification and certified wood products, refer to the Forest Stewardship Council United States ([HTTPS://US.FSC.ORG/EN-US](https://us.fsc.org/en-us)), or the Sustainable Forestry Initiative ([HTTP://WWW.SFIPROGRAM.ORG/](http://www.sfiprogram.org/)).

3.06 ADHESIVES AND SEALANTS (OCT 2019)

Exhibit A

A. All adhesives employed (including, but not limited to, adhesives for carpet, carpet tile, plastic laminate, wall coverings, adhesives for wood, or sealants) shall meet the requirements of the manufacturer of the products adhered or involved. The Lessor shall use adhesives and sealants with no heavy metals, and that do not result in indoor air levels above 0.016 parts per million (ppm) of formaldehyde. Adhesives and other materials used for the installation of carpets shall be limited to those having a flash point of 140 degrees F or higher.

B. For leases 10,000 RSF or greater, the Lessor is encouraged to use applicable environmentally preferable criteria that are recommended in the Green Procurement Compilation at [HTTPS://SFTOOL.GOV/GREENPROCUREMENT](https://sftool.gov/greenprocurement) and <https://sftool.gov/greenprocurement/green-products/8/miscellaneous/1238/adhesives/0>.

3.07 BUILDING SHELL REQUIREMENTS (OCT 2016)

A. The Building Shell shall be designed, constructed, and maintained in accordance with the standards set forth herein and completed prior to acceptance of Space. For pricing, fulfillment of all requirements not specifically designated as TIs, Building Specific Amortized Capital, Operating Costs, or other rent components as indicated shall be deemed included in the Shell Rent.

B. Base structure and Building enclosure components shall be complete. All common areas accessible by the Government, such as lobbies, fire egress corridors and stairwells, elevators, garages, and service areas, shall be complete. Restrooms shall be complete and operational. All newly installed Building shell components, including but not limited to, heating, ventilation, and air conditioning (HVAC), electrical, ceilings, sprinklers, etc., shall be furnished, installed, and coordinated with TIs. Circulation corridors are provided as part of the base Building only on multi-tenanted floors where the corridor is common to more than one tenant. On single tenant floors, only the fire egress corridor(s) necessary to meet code is provided as part of the shell.

C. The Building Shell rental rate shall also include, but is not limited to, costs included listed under Section II of GSA Form 1217, Lessor's Annual Cost Statement, including insurance, taxes, lease commission and management, in addition to profit, reserve costs and loan financing for the Building.

3.08 RESPONSIBILITY OF THE LESSOR AND LESSOR'S ARCHITECT/ENGINEER (JUN 2012)

A. The Lessor shall be responsible for the professional quality, technical accuracy, and the coordination of all designs, drawings, specifications, and other services furnished by the Lessor under this contract. The Lessor shall, without additional compensation, correct or revise any errors or deficiencies in its designs, drawings, specifications, or other services.

B. THE LESSOR REMAINS SOLELY RESPONSIBLE FOR DESIGNING, CONSTRUCTING, OPERATING, AND MAINTAINING THE LEASED PREMISES IN FULL ACCORDANCE WITH THE REQUIREMENTS OF THE LEASE. The Government retains the right to review and approve many aspects of the Lessor's design, including without limitation, review of the Lessor's design and construction drawings, shop drawings, product data, finish samples, and completed base building and TI construction. Such review and approval is intended to identify potential design flaws, to minimize costly misdirection of effort, and to assist the Lessor in its effort to monitor whether such design and construction comply with applicable laws and satisfy all Lease requirements.

C. Neither the Government's review, approval or acceptance of, nor payment through rent of the services required under this contract, shall be construed to operate as a waiver of any rights under this contract or of any cause of action arising out of the performance of this contract, and the Lessor shall be and remain liable to the Government in accordance with applicable law for all damages to the Government caused by the Lessor's negligent performance of any of the services required under this Lease.

D. Design and construction and performance information is contained throughout several of the documents which comprise this Lease. The Lessor shall provide to space planners, architects, engineers, construction contractors, etc., all information required whether it is found in this Lease, special requirements and attachments, price lists, or design intent drawings. Reliance upon one of these documents to the exclusion of any other may result in an incomplete understanding of the scope of the work to be performed and/or services to be provided.

3.09 QUALITY AND APPEARANCE OF BUILDING (JUN 2012)

The Building in which the Premises are located shall be designed, built and maintained in good condition and in accordance with the Lease requirements. If not new or recent construction, the Building shall have undergone by occupancy, modernization, or adaptive reuse for office space with modern conveniences. The Building shall be compatible with its surroundings. Overall, the Building shall project a professional and aesthetically pleasing appearance including an attractive front and entrance way.

3.10 VESTIBULES (OCT 2020)

A. Vestibules shall be provided at public entrances wherever entry to the Space is directly from the outside. In the event of negative air pressure conditions, provisions shall be made for equalizing air pressure. For measurement purposes, vestibules are considered building support space and not ABOA.

B. The Lessor shall provide permanent entryway systems (such as grilles or grates) to control dirt and particulates from entering the Building at all primary exterior entryways.

3.11 MEANS OF EGRESS (MAY 2015)

Exhibit A

- A. Prior to occupancy, the Premises and any parking garage areas shall meet or will be upgraded to meet, either the applicable egress requirements in the National Fire Protection Association, Life Safety Code (NFPA 101), or the International Code Council, International Building Code (IBC), each current as of the Lease Award Date, or use an alternative approach or method that achieves an equivalent level of safety deemed acceptable by the Government.
- B. The Space shall have unrestricted access to a minimum of two remote exits on each floor of Government occupancy.
- C. Interlocking or scissor stairs located on the floor(s) where Space is located shall only count as one exit stair.
- D. A fire escape located on the floor(s) where Space is located shall not be counted as an approved exit stair.
- E. Doors shall not be locked in the direction of egress unless equipped with special locking hardware in accordance with requirements of NFPA 101 or the IBC.

3.12 AUTOMATIC FIRE SPRINKLER SYSTEM (SEP 2013)

- A. Any portion of the Space located below-grade, including parking garage areas, and all areas in a Building referred to as "hazardous areas" (defined in National Fire Protection Association (NFPA) 101) that are located within the entire Building (including non-Government areas) shall be protected by an automatic fire sprinkler system or an equivalent level of safety.
- B. For Buildings in which any portion of the Space is on or above the sixth floor, then, at a minimum, the Building up to and including the highest floor of Government occupancy shall be protected by an automatic fire sprinkler system or an equivalent level of safety.
- C. For Buildings in which any portion of the Space is on or above the sixth floor, and lease of the Space will result, either individually or in combination with other Government Leases in the Building, in the Government leasing 35,000 or more ANSI/BOMA Office Area SF of Space in the Building, then the entire Building shall be protected throughout by an automatic fire sprinkler system or an equivalent level of safety.
- D. Automatic fire sprinkler system(s) shall be installed in accordance with the requirements of NFPA 13, Standard for the Installation of Sprinkler Systems that was in effect on the actual date of installation.
- E. Automatic fire sprinkler system(s) shall be maintained in accordance with the requirements of NFPA 25, Standard for the Inspection, Testing, and Maintenance of Water-based Fire Protection Systems (current as of the Lease Award Date).
- F. "Equivalent level of safety" means an alternative design or system (which may include automatic fire sprinkler systems), based upon fire protection engineering analysis, which achieves a level of safety equal to or greater than that provided by automatic fire sprinkler systems.

3.13 FIRE ALARM SYSTEM (SEP 2013)

- A. A Building-wide fire alarm system shall be installed in the entire Building in which any portion of the Space is located on the 3rd floor or higher.
- B. The fire alarm system shall be installed in accordance with the requirements of NFPA 72, National Fire Alarm and Signaling Code, that was in effect on the actual date of installation.
- C. The fire alarm system shall be maintained in accordance with the requirements of NFPA 72, National Fire Alarm and Signaling Code (current as of the Lease Award Date).
- D. The fire alarm system shall transmit all fire alarm signals to the local fire department via any of the following means: directly to the local fire department, to the (911) public communications center, to a central station, to a remote supervising station, or to a proprietary supervising station.
- E. If the Building's fire alarm control unit is over 25 years old as of the date of award of this Lease, Lessor shall install a new fire alarm system in accordance with the requirements of NFPA 72, National Fire Alarm and Signaling Code (current as of the Lease Award Date), prior to Government acceptance and occupancy of the Space.

3.14 ENERGY INDEPENDENCE AND SECURITY ACT (MAR 2016)

A. Energy-related Requirements:

1. The Energy Independence and Security Act (EISA) establishes the following requirements for Government Leases in Buildings that have not earned the ENERGY STAR® Label conferred by the Environmental Protection Agency (EPA) within one year prior to the due date for final proposal revisions ("most recent year").
2. If this Lease was awarded under any of EISA's Section 435 statutory exceptions, the Lessor shall either:
 - a. Earn the ENERGY STAR® Label prior to acceptance of the Space (or not later than one year after the Lease Award Date of a succeeding or superseding Lease); or
 - b. (i) Complete energy efficiency and conservation improvements if any, agreed to by Lessor in lieu of earning the ENERGY STAR® Label prior to acceptance of the Space (or not later than one year after the Lease Award Date of a succeeding or superseding Lease); and

Exhibit A

(ii) Obtain and publicly disclose the Building's current ENERGY STAR® score (using EPA's Portfolio Manager tool), unless the Lessor cannot access whole building utility consumption data, or there is no building category within Portfolio Manager to benchmark against, including spaces—

- I. That are located in States with privacy laws that provide that utilities shall not provide such aggregated information to multitenant building owners; and
- II. For which tenants do not provide energy consumption information to the commercial building owner in response to a request from the building owner. (A Federal agency that is a tenant of the space shall provide to the building owner, or authorize the owner to obtain from the utility, the energy consumption information of the space for the benchmarking and disclosure required by this subparagraph D).
- III. That cannot be benchmarked (scored) using EPA's Portfolio Manager tool because of excessive vacancy; in which case Lessor agrees to obtain the score and publicly disclose it within 120 days of the eligibility to obtain a score using the EPA Portfolio Manager tool.

Note: "public disclosure" means posting the Energy Star® score on state or local websites in those areas that have applicable disclosure mandates, and reporting the score to the Government via Portfolio Manager. In the absence of an applicable state or local disclosure mandate, Lessor shall either generate and display the Energy Star® score in a public space at the building location or post the score on Lessor's or Lessor's Parent/Affiliate website.

3. If this Lease was awarded to a Building to be built or to a Building predominantly vacant as of the due date for final proposal revisions and was unable to earn the ENERGY STAR® label for the most recent year (as defined above) due to insufficient occupancy, but was able to demonstrate sufficient evidence of capability to earn the ENERGY STAR® label, then Lessor must earn the ENERGY STAR® label within 18 months after occupancy by the Government.

4. The Lessor is encouraged to purchase at least 50 percent of the Government tenant's electricity from renewable sources.

B. Hydrology-related Requirements:

1. Per EISA Section 438, the sponsor of any development or redevelopment project involving a Federal facility with a footprint that exceeds 5,000 square feet shall use site planning, design, construction, and maintenance strategies for the property to maintain or restore, to the maximum extent technically feasible, the predevelopment hydrology of the Property with regard to the temperature, rate, volume, and duration of flow. If the Lessor proposes to satisfy the Government's space requirements through a development or redevelopment project, and the Government will be the sole or predominant tenant such that any other use of the Property will be functionally or quantitatively incidental to the Government's use, the Lessor is required to implement hydrology maintenance and restoration requirements as required by EISA Section 438.

a. For the purposes of applying EISA Section 438 in this Lease, "sponsor" shall mean "Lessor", and "exceeds 5,000 square feet" shall mean construction that disturbs 5,000 square feet or more of land area at the Property or on adjoining property to accommodate the Government's requirements, or at the Property for whatever reason. Information regarding implementation of the hydrology maintenance and restoration requirements can be found at: <http://www.epa.gov/greeningepa/technical-guidance-implementing-stormwater-runoff-requirements-federal-projects>

b. Lessor is required to implement these hydrology maintenance and restoration requirements to the maximum extent technically feasible, prior to acceptance of the Space, (or not later than one year after the Lease Award Date or Lease Term Commencement Date, whichever is later, of a succeeding or superseding Lease). Additionally, this Lease requires EISA Section 438 storm water compliance not later than one year from the date of any applicable disturbance (as defined in EISA Section 438) of more than 5,000 square feet of ground area if such disturbance occurs during the term of the Lease if the Government is the sole or predominant tenant. In the event the Lessor is required to comply with EISA Section 438, Lessor shall furnish the Government, prior to the filing for permits for the associated work, with a certification from Lessor's engineer that the design meets the hydrology maintenance and restoration requirements of EISA Section 438.

3.15 ELEVATORS (OCT 2020)

A. The Lessor shall provide suitable passenger elevator and, when required by the Government, freight elevator service to any of the Premises not having ground level access. Service shall be available during the normal hours of operation specified in the in this Lease. However, one passenger elevator and, when required by the Government, one freight elevator shall be available at all times for Government use. When a freight elevator is required by the Government, it shall be accessible to the loading areas. When possible, the Government shall be given 24-hour advance notice if the service is to be interrupted for more than 1-1/2 hours. Normal service interruption shall be scheduled outside of the Government's normal working hours. The Lessor shall also use best efforts to minimize the frequency and duration of unscheduled interruptions.

B. Code: Elevators shall conform to the requirements of the American Society of Mechanical Engineers ASME A17.1/CSA B44, Safety Code for Elevators and Escalators that were in effect based on the elevator installation date code year. Elevators shall be provided with Phase I emergency recall operation and Phase II emergency in-car operation in accordance with ASME A17.1/CSA B44. Fire alarm initiating devices (e.g., smoke detectors) used to initiate Phase I emergency recall operation shall be installed in accordance with the requirements of NFPA 72, National Fire Alarm and Signaling Code. The elevators shall be inspected and maintained in accordance with the current edition of the ASME A17.2, Inspector's Manual for Elevators. Except for the reference to ASME A17.1 in ABAAS, Section F105.2.2, all elevators must meet ABAAS requirements for accessibility in Sections 407, 408, and 409 of ABAAS.

C. Safety Systems: Elevators shall be equipped with telephones or other two-way emergency communication systems. The system used shall be marked and shall reach an emergency communication location staffed 24 hours per day, 7 days per week.

D. Speed: The passenger elevators shall have a capacity to transport in 5 minutes 15 percent of the normal population of all upper floors (based on 150 SF per person). Further, the dispatch interval between elevators during the up-peak demand period shall not exceed 35 seconds.

Exhibit A

E. Interior Finishes: Elevator cab walls shall be hardwood, marble, granite, or an equivalent pre-approved by the LCO. Elevator cab floors shall be marble, granite, terrazzo, or an equivalent pre-approved by the LCO.

3.16 BUILDING DIRECTORY (APR 2011)

A tamper-proof directory with lock shall be provided in the Building lobby listing the Government agency. It must be acceptable to the LCO.

3.17 DEMOLITION (JUN 2012)

The Lessor shall remove existing abandoned electric, telephone, and data cabling and devices, as well as any other improvements or fixtures in place to accommodate the Government's requirements. Any demolition of existing improvements that is necessary to satisfy the Government's layout shall be done at the Lessor's expense.

3.18 ACCESSIBILITY (FEB 2007)

The Building, leased Space, and areas serving the leased Space shall be accessible to persons with disabilities in accordance with the Architectural Barriers Act Accessibility Standard (ABAAS), Appendices C and D to 36 CFR Part 1191 (ABA Chapters 1 and 2, and Chapters 3 through 10). To the extent the standard referenced in the preceding sentence conflicts with local accessibility requirements, the more stringent shall apply.

3.19 CEILINGS (OCT 2019)

A complete acoustical ceiling system (which includes grid and lay-in tiles or other Building standard ceiling system as approved by the LCO) throughout the Space and Premises shall be required. The acoustical ceiling system shall be furnished, installed, and coordinated with TIs.

A. Ceilings shall be at a minimum 9 feet and 0 inches and no more than 12 feet and 0 inches measured from floor to the lowest obstruction. Areas with raised flooring shall maintain these ceiling-height limitations above the finished raised flooring. Bulkheads and hanging or surface mounted light fixtures which impede traffic ways shall be avoided. Ceilings shall be uniform in color and appearance throughout the Space, with no obvious damage to tiles or grid.

B. Prior to closing the ceiling, the Lessor shall coordinate with the Government for the installation of any items above the ceiling.

C. Should the ceiling be installed in the Space prior to construction of the TIs, then the Lessor shall be responsible for all costs in regard to the disassembly, storage during construction, and subsequent re-assembly of any of the ceiling components which may be required to complete the TIs. The Lessor shall also bear the risk for any damage to the ceiling or any components thereof during the construction of the TIs.

D. Ceilings shall be a flat plane in each room and shall be suspended and finished as follows unless an alternate equivalent is pre-approved by the LCO:

1. Restrooms. Plastered or spackled and taped gypsum board.
2. Offices and conference rooms. Mineral and acoustical tile or lay in panels with textured or patterned surface and tegular edges or an equivalent pre-approved by the LCO. For leases 10,000 RSF or greater, newly installed tiles or panels shall meet applicable, statutory environmentally preferable criteria related to biobased content as outlined under the Green Procurement Compilation at <https://sftool.gov/greenprocurement> and <https://sftool.gov/greenprocurement/green-products/3/building-finishes/1732/acoustical-ceiling-tiles/0?addon=False>.
3. Corridors and eating/galley areas. Plastered or spackled and taped gypsum board or mineral acoustical tile.

3.20 EXTERIOR AND COMMON AREA DOORS AND HARDWARE (SEP 2013)

A. Exterior Building doors and doors necessary to the lobbies, common areas, and core areas shall be required. This does not include suite entry or interior doors specific to TIs.

B. Exterior doors shall be weather tight and shall open outward. Hinges, pivots, and pins shall be installed in a manner which prevents removal when the door is closed and locked. These doors shall have a minimum clear opening of 32" clear wide x 80" high (per leaf). Doors shall be heavy duty, flush, (1) hollow steel construction, (2) solid core wood, or (3) insulated tempered glass. As a minimum requirement, hollow steel doors shall be fully insulated, flush, #16-gauge hollow steel. Solid-core wood doors and hollow steel doors shall be at least 1-3/4 inches thick. Door assemblies shall be of durable finish and shall have an aesthetically pleasing appearance acceptable to the LCO. The opening dimensions and operations shall conform to the governing building, fire safety, accessibility, and energy codes and/or requirements. Fire door assemblies shall be listed and labeled. Labels on fire door assemblies shall be maintained in a legible condition. Fire door assemblies and their accompanying hardware, including frames and closing devices shall be installed in accordance with the requirements of NFPA 80, Standard for Fire Doors and Other Opening Protectives.

C. Exterior doors and all common area doors shall have door handles or door pulls with heavyweight hinges. All doors shall have corresponding doorstops (wall or floor mounted) and silencers. All public use doors and restroom doors shall be equipped with kick plates. All doors shall have automatic door closers. All Building exterior doors shall have locking devices installed to reasonably deter unauthorized entry.

3.21 DOORS: IDENTIFICATION (APR 2011)

All signage required in common areas unrelated to tenant identification shall be provided and installed by the Lessor.

Exhibit A

3.22 WINDOWS (OCT 2020)

- A. Office Space shall have windows in each exterior bay unless waived by the LCO.
- B. All exterior window assemblies shall be weather resistant and water tight. Operable windows that open shall be equipped with secure latches. Off-street, ground-level windows and those accessible from adjacent roofs and other structures that can be opened must be fitted with a secure latch. Windows intended for use as a secondary means of egress must be openable from the egress side (e.g., inside) of the Building without the use of a key, tool, or special knowledge or effort for operation from the egress side.

3.23 PARTITIONS: GENERAL (OCT 2019)

- A. Partitions in public areas shall be marble, granite, hardwood, or drywall covered with durable wall covering or high performance coating, or equivalent pre-approved by the LCO.
- B. For leases 10,000 RSF or greater where the Government is a sole tenant of the Building, the Lessor is encouraged to use materials for newly installed gypsum board meeting applicable environmentally preferable criteria that are recommended in the Green Procurement Compilation at <HTTPS://SFTOOL.GOV/GREENPROCUREMENT> and <https://sftool.gov/greenprocurement/green-products/3/building-finishes/1735/wallboardgypsum-boarddrywall/0?addon=False>.

3.24 PARTITIONS: PERMANENT (OCT 2019)

- A. Permanent partitions shall extend from the structural floor slab to the structural ceiling slab. They shall be provided by the Lessor as part of shell rent as necessary to surround the Space, stairs, corridors, elevator shafts, restrooms, all columns, and janitor closets. They shall have a flame spread rating of 25 or less and a smoke development rating of 450 or less (ASTM E-84). Stairs, elevators, and other floor openings shall be enclosed by partitions and shall have the fire resistance required by the applicable building code, fire code and ordinances adopted by the jurisdiction in which the Building is located (such as the International Building Code, etc.) current as of the Lease Award Date.
- B. For leases 10,000 RSF or greater where the Government is a sole tenant of the Building, the Lessor is encouraged to use materials for newly installed gypsum board meeting the applicable environmentally preferable criteria that are recommended in the Green Procurement Compilation at <HTTPS://SFTOOL.GOV/GREENPROCUREMENT> and <https://sftool.gov/greenprocurement/green-products/3/building-finishes/1735/wallboardgypsum-boarddrywall/0?addon=False>.

3.25 INSULATION: THERMAL, ACOUSTIC, AND HVAC (OCT 2019)

- A. No insulation installed with this project shall be material manufactured using chlorofluorocarbons (CFCs), nor shall CFCs be used in the installation of the product.
- B. All insulation containing fibrous materials exposed to air flow shall be rated for that exposure or shall be encapsulated.
- C. Insulating properties for all materials shall meet or exceed applicable industry standards. Polystyrene products shall meet American Society for Testing and Materials (ASTM) C578 91.
- D. All insulation shall contain low emitting volatiles and not result in indoor air levels above 0.016 parts per million (ppm) of formaldehyde.
- E. The maximum flame spread and smoke developed index for insulation shall meet the requirements of the applicable local codes and ordinances (current as of the Lease Award Date) adopted by the jurisdiction in which the Building is located.
- F. For leases 10,000 RSF or greater, all insulation products shall meet applicable, statutory environmentally preferable criteria related to recovered material content as outlined in the Green Procurement Compilation at <HTTPS://SFTOOL.GOV/GREENPROCUREMENT> and <https://sftool.gov/greenprocurement/green-products/1/construction-materials/22/building-insulation/0>.

3.26 WALL FINISHES – SHELL (SEP 2015)

- A. All restrooms within the Building common areas of Government-occupied floors shall have 1) ceramic tile, recycled glass tile, or comparable wainscot from the finished floor to a minimum height of 4'-6" and 2) semigloss paint on remaining wall areas, or other finish approved by the Government.
- B. All elevator areas that access the Space and hallways accessing the Space shall be covered with wall coverings not less than 20 ounces per square yard, high performance paint, or an equivalent.

3.27 PAINTING – SHELL (OCT 2019)

- A. The Lessor shall bear the expense for all painting associated with the Building shell. These areas shall include all common areas. Exterior perimeter walls and interior core walls within the Space shall be spackled and prime painted. If any Building shell areas are already painted prior to TIs, then the Lessor shall repaint, at the Lessor's expense, as necessary during TIs.
- B. The costs for cyclical painting requirements as outlined in Section 6 shall be included in the shell rent.
- C. For leases 10,000 RSF or greater, primer shall meet applicable, statutory environmentally preferable criteria related to biobased and recovered material content as outlined in the Green Procurement Compilation at <HTTPS://SFTOOL.GOV/GREENPROCUREMENT> and <https://sftool.gov/greenprocurement/green-products/3/building-finishes/1338/paint/0?addon=False>.

Exhibit A

3.28 FLOORS AND FLOOR LOAD (OCT 2019)

A. All adjoining floor areas shall be of a common level not varying more than 1/4 inch over a 10-foot horizontal run in accordance with the American Concrete Institute standards, non-slip, and acceptable to the LCO.

B. Under-floor surfaces shall be smooth and level. Office areas shall have a minimum live load capacity of 50 pounds per ABOA SF plus 20 pounds per ABOA SF for moveable partitions. Storage areas shall have a minimum live load capacity of 100 pounds per ABOA SF, including moveable partitions. Lessor may be required to provide a report by a registered structural engineer showing the floor load capacity, at the Lessor's expense. Calculations and structural drawings may also be required.

3.29 FLOOR COVERING AND PERIMETERS – SHELL (SEP 2013)

A. Exposed interior floors in primary entrances and lobbies shall be marble, granite, or terrazzo. Exposed interior floors in secondary entrances, elevator lobbies, and primary interior corridors shall be high-grade carpet, marble, granite, or terrazzo. Resilient flooring shall be used in telecommunications rooms. Floor perimeters at partitions shall have wood, rubber, vinyl, marble, or carpet base.

B. Terrazzo, unglazed ceramic tile, recycled glass tile, and/or quarry tile shall be used in all restroom and service areas of Government-occupied floors.

C. Any alternate flooring must be pre-approved by the LCO.

D. The costs for cyclical carpet replacement requirements as outlined in Section 6 shall be included in the shell rent.

3.30 MECHANICAL, ELECTRICAL, PLUMBING: GENERAL (APR 2011)

The Lessor shall provide and operate all Building equipment and systems in accordance with applicable technical publications, manuals, and standard procedures. Mains, lines, and meters for utilities shall be provided by the Lessor. Exposed ducts, piping, and conduits are not permitted in office Space.

3.31 BUILDING SYSTEMS (APR 2011)

Whenever requested, the Lessor shall furnish to GSA as part of shell rent, a report by a registered professional engineer(s) showing that the Building and its systems as designed and constructed will satisfy the requirements of this Lease.

3.32 ELECTRICAL (OCT 2019)

A. The Lessor shall be responsible for meeting the applicable requirements of local codes and ordinances. When codes conflict, the more stringent standard shall apply. Main service facilities shall be enclosed. The enclosure may not be used for storage or other purposes and shall have door(s) fitted with an automatic deadlocking latch bolt with a minimum throw of 1/2 inch. Main distribution for standard office occupancy shall be provided at the Lessor's expense. The electrical distribution panels enclosed in the electrical room shall include: single-phase 120/240 volt or 3-phase 120/208 volt service for leased spaces under 10,000 RSF; 3-phase 120/208 volt service for leased spaces between 10,000 and 25,000 RSF; and 3-phase 277/480 volt and 3-phase 120/208 volt service for leased spaces over 25,000 RSF. In no event shall such power distribution (not including lighting and HVAC) for the Space fall below 4 watts per ABOA SF.

B. Main power distribution switchboards and distribution and lighting panel boards shall be circuit breaker type with copper buses that are properly rated to provide the calculated fault circuits. All power distribution panel boards shall be supplied with separate equipment ground buses. All power distribution equipment shall be required to handle the actual specified and projected loads and 10 percent spare load capacity. Distribution panels are required to accommodate circuit breakers for the actual calculated needs and 10 percent spare circuits that will be equivalent to the majority of other circuit breakers in the panel system. Fuses and circuit breakers shall be plainly marked or labeled to identify circuits or equipment supplied through them.

C. Convenience outlets shall be installed in accordance with NFPA Standard 70, National Electrical Code, or local code, whichever is more stringent. The Lessor shall provide duplex utility outlets in restrooms, corridors, and dispensing areas.

3.33 ~~ADDITIONAL ELECTRICAL CONTROLS (JUN 2012)~~ INTENTIONALLY DELETED

3.34 PLUMBING (JUN 2012)

The Lessor shall include the cost of plumbing in common areas. Hot and cold water risers and domestic waste and vent risers, installed and ready for connections that are required for TIs, shall be included in the shell rent.

3.35 DRINKING FOUNTAINS (OCT 2018)

On each floor of Government-occupied Space, the Lessor shall provide a minimum of two drinking fountains with chilled potable water within 200 feet of travel from any Government-occupied area on the floor. The fountains shall comply with Section F211 of the Architectural Barriers Act Accessibility Standard. Potable is defined as water meeting current EPA primary drinking water standards or more stringent, applicable state or local regulations. The Lessor shall serve as first responder to any occupant complaints about drinking water. The Lessor shall promptly investigate any such complaints and implement the necessary controls to address the complaints and maintain potable water conditions.

3.36 RESTROOMS (OCT 2020)

A. If this Lease is satisfied by new construction or by renovations that include the construction of restrooms, Lessor shall provide water closets, sinks and urinals on each floor that is partially or fully occupied by the government per the schedule below. The schedule is per floor and based on a density of one person for each 135 ABOA SF of office Space, allocated as 50% women and 50% men. If future renovations requiring restroom construction occur during the term of this Lease, the number of fixtures then must meet the schedule as part of the major alterations.

ESTIMATED NUMBER OF EACH GENDER PER FLOOR			(WOMEN'S) WATER CLOSETS	(WOMEN'S) SINKS	(MEN'S) WATER CLOSETS	(MEN'S) URINALS	(MEN'S) SINKS
1	to	8	2	1	1	1	1
9	to	24	3	2	2	1	1
25	to	36	3	2	2	1	2
37	to	56	5	3	3	2	2
57	to	75	6	4	4	2	2
76	to	96	6	5	4	2	3
97	to	119	7	5	5	2	3
120	to	134	9	5	6	3	4
Above 135			3/40	1/24	1/20	1/40	1/30

B. If no new construction of a restroom is occurring, at a minimum, separate restroom facilities for men and women shall be provided with sufficient fixtures (water closets, sinks and urinals), in accordance with local code or ordinances.

C. Each restroom shall have water closets enclosed with modern stall partitions and doors, urinals (in men's room), and hot (set in accordance with applicable building codes) and cold water. Water closets and urinals shall not be visible when the exterior door is open. These facilities shall be located on each floor occupied by the Government in the Building and shall be located so that employees will not be required to travel more than 200 feet on one floor to reach the restrooms.

D. Restrooms must meet ABAAS requirements as stated under this Lease.

E. Each main restroom shall contain the following:

1. A mirror and shelf above the lavatory.
2. A toilet paper dispenser in each water closet stall that will hold at least two rolls and allow easy, unrestricted dispensing.
3. A coat hook on the inside face of the door to each water closet stall and on several wall locations by the lavatories.
4. At least one modern paper towel dispenser, soap dispenser, and waste receptacle for every two lavatories.
5. A coin-operated sanitary napkin dispenser in women's restrooms with a waste receptacle in each water closet stall.
6. A disposable toilet seat cover dispenser.
7. A counter area of at least 2 feet, 0 inches in length, exclusive of the lavatories (however, it may be attached to the lavatories) with a mirror above and a ground-fault interrupter-type convenience outlet located adjacent to the counter area. The counter should be installed to minimize pooling or spilling of water at the front edge.
8. A floor drain.
9. Newly installed restroom partitions shall be made from recovered materials as listed in EPA's CPG.

3.37 PLUMBING FIXTURES: WATER CONSERVATION (OCT 2019)

For leases 10,000 RSF or greater, the specifications listed below apply:

1. New installations of plumbing fixtures,
 2. Replacement of existing plumbing fixtures, or
 3. Existing non-conforming fixtures where the Government occupies the full floor.
- A. Water closets must conform to EPA WaterSense or fixtures with equivalent flush volumes must be utilized.
- B. Urinals must conform to EPA WaterSense or fixtures with equivalent flush volumes must be utilized. Waterless urinals are acceptable.
- C. Faucets must conform to EPA WaterSense or fixtures with equivalent flow rates must be utilized.

Information on EPA WaterSense fixtures can be found at [HTTP://WWW.EPA.GOV/WATERSENSE/](http://www.epa.gov/watersense/).

3.38 JANITOR CLOSETS (SEP 2015)

Janitor closets shall meet all local codes and ordinances. When not addressed by local code, Lessor shall provide containment drains plumbed for appropriate disposal of liquid wastes in spaces where water and chemical concentrate mixing occurs for maintenance purposes. Disposal is not permitted in restrooms.

3.39 HEATING, VENTILATION, AND AIR CONDITIONING - SHELL (OCT 2020)

Exhibit A

- A. Central HVAC systems shall be installed and operational, including, as appropriate, main and branch lines, VAV boxes, dampers, flex ducts, and diffusers, for an open office layout, including all Building common areas. The Lessor shall provide conditioned air through medium pressure duct work at a rate of .75 cubic feet per minute per ABOA SF and systems shall be designed with sufficient systems capacity to meet all requirements in this Lease.
- B. Areas having excessive heat gain or heat loss, or affected by solar radiation at different times of the day, shall be independently controlled.
- C. Equipment Performance. Temperature control for office Spaces shall be provided by concealed central heating and air conditioning equipment. The equipment shall maintain Space temperature control over a range of internal load fluctuations of plus 0.5 W/SF to minus 1.5 W/SF from initial design requirements of the tenant.
- D. Ductwork Re-use and Cleaning. Any ductwork to be reused and/or to remain in place shall be cleaned, tested, and demonstrated to be clean in accordance with the standards set forth by NADCA. The cleaning, testing, and demonstration shall occur immediately prior to Government occupancy to avoid contamination from construction dust and other airborne particulates.
- E. During working hours in periods of heating and cooling, ventilation shall be provided in accordance with American National Standards Institute, American Society of Heating, Refrigeration and Air-Conditioning Engineers (ANSI/ASHRAE) Standard 62.1, Ventilation for Acceptable Indoor Air Quality that corresponds with how the HVAC system was designed to perform. At a minimum, Lessor must meet ASHRAE Standard 62.1-2004.
- F. Heating and air-conditioning air distribution systems (air handling units, VAV boxes, fan coil units, etc.) for the Space shall be equipped with particulate matter air filters that meet the Minimum Efficiency Reporting Value (MERV) specified in the ANSI/ASHRAE Standard 62.1 version referenced in sub-paragraph E above. Locations that do not meet the EPA National Ambient Air Quality Standards (NAAQS) for particulates (PM 10 or PM 2.5) must be equipped with additional filtration on outdoor air intakes as required in ANSI/ASHRAE Standard 62.1. NAAQS information can be found at <HTTPS://WWW.EPA.GOV/GREEN-BOOK>.
- G. Restrooms shall be properly exhausted, with a minimum of 10 air changes per hour.
- H. INTENTIONALLY DELETED

3.40 TELECOMMUNICATIONS: DISTRIBUTION AND EQUIPMENT (SEP 2015)

- A. Sufficient space shall be provided on the floor(s) where the Government occupies Space for the purposes of terminating telecommunications service into the Building. The Building's telecommunications closets located on all floors shall be vertically-stacked. Telecommunications switch rooms, wire closets, and related spaces shall be enclosed. The enclosure shall not be used for storage or other purposes and shall have door(s) fitted with an automatic door-closer and deadlocking latch bolt with a minimum throw of 1/2 inch. The telephone closets shall include a telephone backboard.
- B. Telecommunications switch rooms, wire closets, and related spaces shall meet applicable Telecommunications Industry Association (TIA) and Electronic Industries Alliance (EIA) standards. These standards include the following:
1. TIA/EIA-568, Commercial Building Telecommunications Cabling Standard,
 2. TIA/EIA 569, Commercial Building Standard for Telecommunications Pathways and Spaces,
 3. TIA/EIA-570, Residential and Light Commercial Telecommunications Wiring Standard, and
 4. TIA/EIA-607, Commercial Building Grounding and Bonding Requirements for Telecommunications Standard.
- C. Telecommunications switch rooms, wire closets, and related spaces shall meet applicable NFPA standards. Bonding and grounding shall be in accordance with NFPA Standard 70, National Electrical Code, and other applicable NFPA standards and/or local code requirements.

3.41 TELECOMMUNICATIONS: LOCAL EXCHANGE ACCESS (JUN 2012)

- A. The Government may elect to contract its own telecommunications (voice, data, video, Internet or other emerging technologies) service in the Space. The Government may contract with one or more parties to have INS wiring (or other transmission medium) and telecommunications equipment installed.
- B. The Lessor shall allow the Government's designated telecommunications providers access to utilize existing Building wiring to connect its services to the Government's Space. If the existing Building wiring is insufficient to handle the transmission requirements of the Government's designated telecommunications providers, the Lessor shall provide access from the point of entry into the Building to the Government's floor Space, subject to any inherent limitations in the pathway involved.
- C. The Lessor shall allow the Government's designated telecommunications providers to affix telecommunications antennas (high frequency, mobile, microwave, satellite, or other emerging technologies), subject to weight and wind load conditions, to roof, parapet, or Building envelope as required. Access from the antennas to the Premises shall be provided.
- D. The Lessor shall allow the Government's designated telecommunications providers to affix antennas and transmission devices throughout the Space and in appropriate common areas frequented by the Government's employees to allow the use of cellular telephones and communications devices necessary to conduct business.

3.42 LIGHTING: INTERIOR AND PARKING - SHELL (OCT 2020)

NOTE: FOR PRICING ESTIMATING PURPOSES, FIXTURES WILL BE INSTALLED AT THE AVERAGE RATIO OF 1 FIXTURE PER 80 ABOA SF.

Exhibit A

A. INTERIOR FIXTURES: High efficiency T-8, T-5, or LED light fixtures (and associated ballasts or drivers) shall be installed as either ceiling grid or pendant mounted for an open-office plan. Ceiling grid fixtures shall be either 2' wide by 4' long or 2' wide by 2' long. Lessor shall provide, as part of Shell Rent, a minimum overall lighting fixture efficiency of 85 percent. Lamps shall maintain a uniform color level throughout the lease term.

B. LIGHTING LEVELS: Fixtures shall have a minimum of two tubes and shall provide 50 foot-candles at desktop level (30" above finished floor) with a maximum uniformity ratio of 1.5:1. Lessor shall provide, as part of Shell Rent, 10 average foot-candles in all other Building areas within the Premises with a uniformity ratio of 4:1. Emergency egress lighting levels shall be provided in accordance with the local applicable building codes (but not less than 1 foot-candle) by either an onsite emergency generator or fixture mounted battery packs.

B. LIGHTING LEVELS WITH TASK LIGHTING: Fixtures shall have a minimum of two tubes and shall provide 30 foot-candles at desktop level (30" above finished floor) with a maximum uniformity ratio of 1.5:1 for XX percent of the total Space, and 50 foot-candles at desktop level (30" above finished floor) with a maximum uniformity ratio of 1.5:1 for XX percent of the Space. Lessor shall provide, as part of Shell Rent, 10 average foot-candles in all other Building areas within the Premises with a uniformity ratio of 4:1. Emergency egress lighting levels shall be provided in accordance with the local applicable building codes (but not less than 1 foot-candle) by either an onsite emergency generator or fixture mounted battery packs.

C. POWER DENSITY:

Existing Buildings: The maximum fixture power density shall not exceed 1.4 watts per ABOA SF.

New Construction: The maximum fixture power density shall not exceed 1.1 watts per ABOA SF.

D. DAYLIGHTING CONTROLS: If the Lease is more than 10,000 ABOA SF, the Lessor shall provide daylight dimming controls in atriums or within 15 feet of windows and skylights where daylight can contribute to energy savings. Daylight harvesting sensing and controls shall be either integral to the fixtures or ceiling mounted and shall maintain required lighting levels in work spaces.

E. OCCUPANCY/VACANCY SENSORS: The Lessor shall provide ceiling mount occupancy sensors, or vacancy sensors (preferred), or scheduling controls through the building automation system (BAS) throughout the Space in order to reduce the hours that the lights are on when a particular space is unoccupied. No more than 1,000 square feet shall be controlled by any one sensor. Occupancy sensors in enclosed rooms shall continue to operate after the BAS has shut down the building at the end of the workday.

F. BUILDING PERIMETER:

1. Exterior parking areas, vehicle driveways, pedestrian walks, and the Building perimeter lighting levels shall be designed per Illuminating Engineering Society (IES) standards. Provide 5 foot-candles for doorway areas, 3 foot-candles for transition areas and at least 1 foot-candle at the surface throughout the parking lot. Parking lot fixtures shall provide a maximum to minimum uniformity ratio of 15:1 and a maximum to average uniformity ratio of 4:1.

2. If the leased space is 100 percent occupied by Government tenants, all exterior parking lot fixtures shall be "Dark Sky" compliant with no property line trespass.

G. PARKING STRUCTURES: The minimum illuminance level for parking structures is 5 foot-candles as measured on the floor with a uniformity ratio of 10:1.

H. PARKING SENSORS: If the leased space is 100 percent occupied by Government tenants, exterior parking area and parking structure lighting shall be sensor or BAS controlled in order that it may be programmed to produce reduced lighting levels during non-use. This non-use time period will normally be from 11:00 pm to 6:00 am.

I. EXTERIOR POWER BACKUP: Exterior egress, walkway, parking lot, and parking structure lighting must have emergency power backup to provide for safe evacuation of the Building.

J. VIDEO SURVEILLANCE SYSTEM (VSS): Lighting shall be provided in such a manner to adequately support VSS operations, and not limit or preclude adequate fields of view.

3.43 ACOUSTICAL REQUIREMENTS (JUN 2012)

A. Reverberation Control. Private office and conference rooms using suspended acoustical ceilings shall have a noise reduction coefficient (NRC) of not less than 0.65 in accordance with ASTM C-423. Open office using suspended acoustical ceilings shall have an NRC of not less than 0.75. Private offices, conference rooms, and open offices using acoustical cloud or acoustical wall panels with a minimum of 70% coverage shall have an NRC of not less than 0.85.

B. Ambient Noise Control. Ambient noise from mechanical equipment shall not exceed noise criteria curve (NC) 35 in accordance with the ASHRAE Handbook of Fundamentals in offices and conference rooms; NC 40 in corridors, cafeterias, lobbies, and restrooms; NC 50 in other spaces.

C. Noise Isolation. Rooms separated from adjacent spaces by ceiling high partitions (not including doors) shall not be less than the following noise isolation class (NIC) standards when tested in accordance with ASTM E-336:

Conference rooms: NIC 40

Offices: NIC 35

Exhibit A

D. Testing. The LCO may require, at Lessor's expense, test reports by a qualified acoustical consultant showing that acoustical requirements have been met.

3.44 SECURITY FOR NEW CONSTRUCTION (OCT 2019) INTENTIONALLY DELETED

3.45 SEISMIC SAFETY FOR NEW CONSTRUCTION (OCT 2020) INTENTIONALLY DELETED

3.46 FIRE PROTECTION FOR NEW CONSTRUCTION (APR 2015) INTENTIONALLY DELETED

3.47 GREEN BUILDING RATING CERTIFICATION FOR NEW CONSTRUCTION (OCT 2016) INTENTIONALLY DELETED

3.48 GREEN BUILDING RATING CERTIFICATION FOR TENANT INTERIORS (OCT 2016)

A. The tenant Space must meet the requirements of LEED®-ID+C--Leadership in Energy and Environmental Design for Interior Design and Construction at the Certified level, at a minimum. The Lessor, at the Lessor's expense, shall obtain certification from the USGBC (for LEED®) within 9 months of occupancy. For requirements to achieve certification, Lessor must refer to latest version at the time of submittal of the LEED®-ID+C Reference Guide (at [HTTP://WWW.USGBC.ORG/](http://www.usgbc.org/)). At completion of all documentation and receipt of final certification, the Lessor must provide the Government two electronic copies on compact disks of all documentation submitted to the USGBC. Acceptable file format is Adobe PDF copied to disk from the LEED®-Online workspace. In addition, the Lessor will provide the Government viewing access to the LEED®-Online workspace as applicable during design and through the term of the Lease.

B. Prior to the end of the first 9 months of occupancy, if the Lessor fails to achieve LEED® certification, the Government may assist the Lessor in implementing a corrective action program to achieve LEED® certification and deduct its costs (including administrative costs) from the rent.

C. Any Building shell modifications necessary for the Space to meet the requirements of LEED®-ID+C certification, shall be noted and incorporated into the construction documents and shall be included as part of the Building shell costs. The Lessor must coordinate TI and shell requirements as necessary to meet the certification.

A. The tenant Space must meet the requirements of Green Globes® SI at the One Green Globes level, at a minimum. The Lessor, at the Lessor's expense, shall obtain certification from the GBI (for Green Globes®) within 9 months of occupancy. For requirements to achieve certification, Lessor must refer to latest version at the time of submittal of the Green Globes® SI Technical Reference Manual (at [HTTP://WWW.THEGBI.ORG/](http://www.thegbi.org/)). At completion of all documentation and receipt of final certification, the Lessor must provide the Government two electronic copies on compact disks of all documentation submitted to the GBI. Acceptable file format is Adobe PDF copied to disk from the Green Globes® online surveys. In addition, the Lessor will provide the Government viewing access to the Green Globes® online surveys as applicable during design and through the term of the Lease.

B. Prior to the end of the first 9 months of occupancy, if the Lessor fails to achieve Green Globes® certification, the Government may assist the Lessor in implementing a corrective action program to achieve Green Globes® certification and deduct its costs (including administrative costs) from the rent.

C. Any Building shell modifications necessary for the Space to meet the requirements of Green Globes® SI certification, shall be noted and incorporated into the construction documents and shall be included as part of the Building shell costs. The Lessor must coordinate TI and shell requirements as necessary to meet the certification.

3.49 INDOOR AIR QUALITY DURING CONSTRUCTION (OCT 2020)

A. The Lessor shall provide to the Government safety data sheets (SDS) or other appropriate documents upon request, but prior to installation or use for the following products, including but not limited to, adhesives, caulking, sealants, insulating materials, fireproofing or fire stopping materials, paints, carpets, floor and wall patching or leveling materials, lubricants, clear finishes for wood surfaces, janitorial cleaning products, and pest control products.

B. The LCO may eliminate from consideration products with significant quantities of toxic, flammable, corrosive, or carcinogenic material and products with potential for harmful chemical emissions. Materials used often or in large quantities will receive the greatest amount of review.

C. Where demolition or construction work occurs adjacent to occupied Space, the Lessor shall erect appropriate barriers (noise, dust, odor, etc.) and take necessary steps to minimize interference with the occupants. This includes maintaining acceptable temperature, humidity, and ventilation in the occupied areas during window removal, window replacement, or similar types of work.

D. HVAC during Construction: If air handlers are used during construction, the Lessor shall provide filtration media with a MERV of 8 at each return air grill, as determined by ANSI/ASHRAE Standard 52.2, Method of Testing General Ventilation Air Cleaning Devices for Removal Efficiency by Particle Size.

E. Flush-Out Procedure:

Exhibit A

1. HVAC flush-out shall commence after construction ends and the Building has been completely cleaned. All interior finishes, such as millwork, doors, paint, carpet, acoustic tiles, and movable furnishings (e.g., workstations, partitions), must be installed, and major VOC punch list items must be finished.

2. Prior to occupancy, Lessor shall install new filtration media and perform a building flush-out by supplying a total air volume of 14,000 cubic feet of outdoor air per square foot of gross floor area while maintaining an internal temperature of at least 60°F (15°C) and no higher than 80°F (27°C) and relative humidity no higher than 60%.

3. If the LCO determines that occupancy is required before flush-out can be completed, the Space may be occupied only after delivery of a minimum of 3,500 cubic feet of outdoor air per square foot of gross floor area while maintaining an internal temperature of at least 60°F (15°C) and no higher than 80°F (27°C) and relative humidity no higher than 60%. Once the Space is occupied, it must be ventilated at a minimum rate of 0.30 cubic foot per minute (cfm) per square foot of outdoor air or greater. During each day of the flush-out period, ventilation must begin at least three hours before occupancy and continue during occupancy. These conditions must be maintained until a total of 14,000 cubic feet per square foot of outdoor air (4 270 liters of outdoor air per square meter) has been delivered to the space.

3.50 SYSTEMS COMMISSIONING (APR 2011)

The Lessor shall incorporate commissioning requirements to verify that the installation and performance of energy consuming systems meet the Government's project requirements. The commissioning shall cover only work associated with TIs or alterations or at a minimum: heating, ventilating, air conditioning and refrigeration (HVAC&R) systems and associated controls, lighting controls, and domestic hot water systems.

3.51 DUE DILIGENCE AND NATIONAL ENVIRONMENTAL POLICY ACT REQUIREMENTS – LEASE (SEP 2014)

A. Environmental Due Diligence

Lessor is responsible for performing all necessary "response" actions (as that term is defined at 42 U.S.C. § 9601(25) of the Comprehensive Environmental Response, Compensation and Liability Act (CERCLA)) with regard to all "recognized environmental conditions," as that term is defined in ASTM Standard E1527-13, as such standard may be revised from time to time. This obligation extends to any contamination of the Property where such contamination is not attributable to the Government. Lessor must provide the Government with a summary report demonstrating completion of all required response actions prior to Substantial Completion. Any remediation performed by or on behalf of Lessor must be undertaken in strict compliance with all applicable federal, state and local laws and regulations.

B. National Environmental Policy Act

The National Environmental Policy Act regulations provide for analyzing proposed major federal actions to determine if there are ways to mitigate the impact of the proposed actions to avoid, minimize, rectify, reduce, or compensate for environmental impacts associated with such actions. Where the Government has determined that any or all of these mitigation measures should be or must be adopted to lessen the impact of these proposed actions, Lessor must incorporate all mitigation measures identified and adopted by the Government in the design and construction drawings and specifications. All costs and expenses for development of design alternatives, mitigation measures and review submittals for work to be performed under the Lease are the sole responsibility of Lessor.

3.52 NATIONAL HISTORIC PRESERVATION ACT REQUIREMENTS - LEASE (SEP 2014)

A. Where a Memorandum of Agreement or other pre-award agreement concluding the Section 106 consultation includes mitigation, design review or other continuing responsibilities of the Government, Lessor must allow the Government access to the Property to carry out compliance activities. Compliance may require excavation for artifact recovery, recordation and interpretation. For Tenant Improvements and other tenant-driven alterations within an existing historic building, new construction or exterior alterations that could affect historic properties, compliance also may require on-going design review. In these instances, Lessor will be required to retain, at its sole cost and expense, the services of a preservation architect who meets or exceeds the *Secretary of the Interior's Professional Qualifications Standards for Historic Architecture*, as amended and annotated and previously published in the Code of Federal Regulations, 36 C.F.R. part 61, and the *GSA Qualifications Standards for Preservation Architects*. These standards are available at: [HTTP://WWW.GSA.GOV/HISTORICPRESERVATION](http://www.gsa.gov/historicpreservation)>Project Management Tools> Qualification Requirements for Preservation Architects. The preservation architect will be responsible for developing preservation design solutions and project documentation required for review by the Government, the State Historic Preservation Officer (SHPO), the Tribal Historic Preservation Officer (THPO), if applicable, and other consulting parties in accordance with Section 106. For Tenant Improvements and other tenant-driven alterations within an existing historic building, the preservation architect must develop context-sensitive design options consistent with the *Secretary of the Interior's Standards for the Treatment of Historic Properties*. Where new construction or exterior alterations, or both, are located within a historic district, may be visible from historic properties or may affect archeological resources, compliance may require tailoring the design of the improvements to be compatible with the surrounding area. Design review may require multiple revised submissions, depending on the complexity of the project and potential for adverse effects to historic properties. GSA is responsible for corresponding with the SHPO, the THPO, if applicable, and any other consulting party.

B. Compliance requirements under Section 106 apply to all historic property alterations and new construction, regardless of the magnitude, complexity or cost of the proposed scope of work.

C. The costs for development of design alternatives and review submittals for work required under the Lease are the sole responsibility of Lessor. In addition, building shell costs relating to such design alternatives are the sole responsibility of Lessor and must be included in the shell rent. Such costs may be offset by federal, state or local preservation tax benefits. Lessor is encouraged to seek independent financial and legal advice concerning the availability of these tax benefits.

3.53 DESIGN EXCELLENCE—LEASE (OCT 2016) INTENTIONALLY DELETED

SECTION 4 DESIGN, CONSTRUCTION, AND POST AWARD ACTIVITIES

4.01 SCHEDULE FOR COMPLETION OF SPACE (OCT 2020)

Design and construction activities for the Space shall commence upon Lease award. The Lessor shall schedule the following activities to achieve timely completion of the work required by this Lease:

A. Lessor-Provided Design Intent Drawings (DIDs): The Lessor must submit to GSA, as part of the shell cost, complete DIDs conforming to the requirements of this Lease and other Government-supplied information related to the tenant agency's interior build-out requirements not later than **XX** Working Days following the Lease Award Date, provided that the Government supplies such information and direction as reasonably required for Lessor to timely complete DIDs. The Government (GSA and the tenant agency) shall attend two meetings at the Lessor's request for the purpose of providing information and direction in the development of DIDs. These meetings may be held either in person or virtually, at the discretion of the Government. The Lessor should anticipate at least two submissions of DIDs before receiving approval. At the sole discretion of the Government, the Lessor may be required to submit a budget proposal based on the TIs and associated work as shown on the DIDs. This budget proposal shall be completed, as part of the shell cost, within **XX** Working Days of the Government's request.

B. DIDs. For the purposes of this Lease, DIDs are defined as layout line drawings of the leased Space, reflecting all Lease requirements, showing partitions and doors; schematic demolition; voice, data, and electrical outlet locations; finishes; generic furniture layout, and any additional details necessary to communicate the design intent to the lessor's architect for the purpose of preparing the construction documents (CDs). A full DID set must include the following elements:

Level 1 (included in Shell rent):

1. Cover Sheet;
2. Demolition Plan (if applicable);
3. Construction (Partition) Plan;
4. Power/Communication (Electrical) Plan;
5. Furniture Plan; and
6. Finish Plan.

Level 2 DIDs (reimbursable):

After Lease Award, the Government may request the Lessor to submit a separate price proposal to provide Level 2 DIDs in addition to the Level 1 DIDs which are already priced as part of the shell rent. If requested, Level 2 DIDs must include the following Level 2 elements:

1. Reflected Ceiling Plan;
2. Interior Elevations;
3. Interior Sections;
4. Partition Type/ Section Plan; and
5. Door/Hardware Schedule

C. Government review and approval of Lessor-provided DIDs: The Government must notify the Lessor of DID approval not later than **XX** Working Days following submission of DIDs conforming to the requirements of this Lease as supplied by the Government. Should the DIDs not conform to these requirements, the Government must notify the Lessor of such non-conformances within the same period; however, the Lessor shall be responsible for any delay to approval of DIDs occasioned by such non-conformance. The Government's review and approval of the DIDs is limited to conformance to the specific requirements of the Lease as they apply to the Space.

D. The Lessor's preparation and submission of construction documents (CDs): The Lessor as part of the TI must complete CDs conforming to the approved DIDs not later than **30** Working Days following the approval of DIDs. If during the preparation of CDs the Lessor becomes aware that any material requirement indicated in the approved DIDs cannot be reasonably achieved, the Lessor shall promptly notify GSA, and shall not proceed with completion of CDs until direction is received from the LCO. The LCO shall provide direction within **15** Working Days of such notice, but the Government shall not be responsible for delays to completion of CDs occasioned by such circumstances. For the purpose of this paragraph, a "material requirement" shall mean any requirement necessary for the Government's intended use of the Space as provided for in, or reasonably inferable from, the Lease and the approved DIDs (e.g., number of workstations and required adjacencies).

E. Government review of CDs: The Government shall have **30** Working Days to review CDs prior to issuing a Notice to Proceed (NTP). At any time during this period of review, the Government shall have the right to require the Lessor to modify the CDs to enforce conformance to Lease requirements and the approved DIDs.

F. INTENTIONALLY DELETED

Exhibit A

G. INTENTIONALLY DELETED

H. INTENTIONALLY DELETED

I. Construction of TIs and completion of other required construction work: The Lessor shall complete all work required to prepare the Premises as required in this Lease ready for use not later than ~~XX~~ Working days following issuance of NTP.

4.02 CONSTRUCTION DOCUMENTS (SEP 2012)

The Lessor's CDs shall include all mechanical, electrical, plumbing, fire protection, life safety, lighting, structural, security, and architectural improvements scheduled for inclusion into the Space. CDs shall be annotated with all applicable specifications. CDs shall also clearly identify TIs already in place and the work to be done by the Lessor or others. Notwithstanding the Government's review of the CDs, the Lessor is solely responsible and liable for their technical accuracy and compliance with all applicable Lease requirements.

4.03 ~~TENANT IMPROVEMENTS PRICE PROPOSAL (OCT 2020)~~ INTENTIONALLY DELETED

4.04 ~~BUILDING SPECIFIC AMORTIZED CAPITAL (BSAC) PRICE PROPOSAL (SEP 2015)~~ INTENTIONALLY DELETED

4.05 GREEN LEASE SUBMITTALS (OCT 2019)

The Lessor shall submit to the LCO:

- A. Product data sheets for floor coverings, paints and wall coverings, ceiling materials, all adhesives, wood products, suite and interior doors, subdividing partitions, wall base, door hardware finishes, window coverings, millwork substrate and millwork finishes, lighting and lighting controls, and insulation to be used within the leased Space. This information must be submitted NO LATER THAN the submission of the DIDs, if applicable.
- B. SDS or other appropriate documents upon request for products listed in the Lease. All SDS shall comply with Occupational Safety and Health Administration (OSHA) requirements for the Globally Harmonized System of Classification and Labeling of Chemicals (GHS). The Lessor and its agents shall comply with all recommended measures in the SDS to protect the health and safety of personnel.
- C. For leases 10,000 RSF or greater, a re-use plan, if required in accordance with the "Existing Fit-out, Salvaged, or Re-used Building Material" paragraph in the Lease.
- D. If the Lessor is unable to comply with the environmentally preferable requirements stated throughout the Lease, he/she must submit a waiver request for each material within the TI pricing submittal. The waiver request shall be based on the following exceptions:
 - 1. Product cannot be acquired competitively within a reasonable performance schedule.
 - 2. Product cannot be acquired that meets reasonable performance requirements.
 - 3. Product cannot be acquired at a reasonable price.
 - 4. An exception is provided by statute.

The price shall be deemed unreasonable when the total life cycle costs are significantly higher for the sustainable product versus the non-sustainable product. Life cycle costs are determined by combining the initial costs of a product with any additional costs or revenues generated from that product during its entire life.

- E. Radon test results as may be required by the "Radon in Air" and "Radon in Water" paragraphs in the Lease.
- F. Construction waste management plan: For leases 10,000 RSF or greater, prior to construction commencement, a proposed plan following industry standards to recycle construction waste. The construction waste management plan shall quantify material diversion goals and maximize the materials to be recycled and/or salvaged (at least 50 percent) from construction, demolition, and packaging debris. Where the small quantity of material, the extraordinarily complex nature of the waste disposal method, or prohibitive expense for recycling would represent a genuine hardship, the Government, upon written request of the Lessor and approval of the LCO, may permit alternative means of disposal.
- G. Building recycling service plan: A Building recycling service plan with floor plans annotating recycling area(s) as part of DIDs, if applicable, to be reflected on the CD submission.
- H. A signed statement from the Lessor for the leased Space explaining how all HVAC systems serving the leased Space will achieve the desired ventilation of the Space during the flush-out period called for in the Lease.
- I. A written commissioning plan submitted to the LCO prior to the completion of DIDs, if applicable, that includes:
 - 1. A schedule of systems commissioning (revised as needed during all construction phases of the project, with such revisions provided to the LCO immediately); and
 - 2. A description of how commissioning requirements will be met and confirmed.

Exhibit A

- J. At completion of LEED®, documentation and receipt of final certification, along with two electronic copies of all supporting documentation for certification on compact disk.
- J. At completion of Green Globes® documentation and receipt of final certification, along with two electronic copies of all supporting documentation for certification on compact disk.
- K. If renewable source power is purchased, documentation within 9 months of occupancy.

4.06 CONSTRUCTION SCHEDULE AND INITIAL CONSTRUCTION MEETING (OCT 2020)

The Lessor shall furnish a detailed construction schedule (such as Critical Path Method) to the Government within **10** Working Days of issuance of the NTP. Such schedule shall also indicate the dates available for Government contractors to install telephone/data lines or equipment, if needed. Within **10** Working Days of NTP, the Lessor shall initiate a construction meeting. This meeting may be held in person or virtually, at the discretion of the Government. The Lessor will have contractor representatives including its architects, engineers, general contractor and sub-contractor representatives in attendance. The Lessor shall keep meeting minutes of discussion topics and attendance.

4.07 PROGRESS REPORTS (OCT 2020)

After start of construction, the Lessor shall submit to the LCO written progress reports at intervals of **5** Working Days. Each report shall include information as to the percentage of the work completed by phase and trade; a statement as to expected completion and occupancy dates; changes introduced into the work; and general remarks on such items as material shortages, strikes, weather, etc, that may affect timely completion. In addition, at the Government's discretion, the Lessor shall conduct meetings every two weeks to brief Government personnel and/or contractors regarding the progress of design and construction of the Space. These meetings may be held in person or virtually, at the discretion of the Government. The Lessor shall be responsible for taking and distributing minutes of these meetings.

4.08 CONSTRUCTION INSPECTIONS (SEP 2015)

- A. The LCO or the LCO's designated technical representative may periodically inspect construction work to review compliance with Lease requirements and approved DIDs, if applicable.
- B. Periodic reviews, witnessing of tests, and inspections by the Government shall not constitute approval of the Lessor's apparent progress toward meeting the Government's objectives but are intended to discover any information which the LCO may be able to call to the Lessor's attention to prevent costly misdirection of effort. The Lessor shall remain responsible for designing, constructing, operating, and maintaining the Building in full accordance with the requirements of the Lease.

4.09 ACCESS BY THE GOVERNMENT PRIOR TO ACCEPTANCE (SEP 2013)

The Government shall have the right to access any space within the Building during construction for the purposes of performing inspections or installing Government furnished equipment. The Government shall coordinate the activity of Government contractors with the Lessor to minimize conflicts with and disruption to other contractors on site. Access shall not be unreasonably denied to authorized Government officials including, but not limited to, Government contractors, subcontractors, or consultants acting on behalf of the Government on this project.

4.10 ACCEPTANCE OF SPACE AND CERTIFICATE OF OCCUPANCY (SEP 2015)

- A. Ten (10) Working Days prior to the completion of the Space, the Lessor shall issue written notice to the Government to schedule the inspection of the Space for acceptance. The Government shall accept the Space only if the construction of Building shell and TIs conforming to this Lease and the approved DIDs, if applicable, is substantially complete, a Certificate of Occupancy (C of O) has been issued as set forth below, and the Building improvements necessary for acceptance as described in the paragraph "Building Improvements" are completed.
- B. The Space shall be considered substantially complete only if the Space may be used for its intended purpose, and completion of remaining work will not interfere unreasonably with the Government's enjoyment of the Space. Acceptance shall be final and binding upon the Government with respect to conformance of the completed TIs to the approved DIDs, with the exception of items identified on a punch list generated as a result of the inspection, concealed conditions, latent defects, or fraud, but shall not relieve the Lessor of any other Lease requirements.
- C. The Lessor shall provide a valid C of O, issued by the local jurisdiction, for the intended use of the Government. If the local jurisdiction does not issue C of O's or if the C of O is not available, the Lessor may satisfy this condition by providing a report prepared by a licensed fire protection engineer that indicates the Space and Building are compliant with all applicable local codes and ordinances and all fire protection and life safety-related requirements of this Lease.
- D. The Government will not be required to accept space prior to the schedule outlined in this Lease.

4.11 LEASE TERM COMMENCEMENT DATE AND RENT RECONCILIATION (JUN 2012)

At acceptance, the Space shall be measured in accordance with the standards set forth in this Lease to determine the total ABOA SF in the Space. The rent for the Space will be adjusted based upon the measured ABOA square footage as outlined under the Payment clause of the General Clauses. At acceptance, the Lease term shall commence. The Lease Term Commencement Date, final measurement of the Premises, reconciliation of the annual rent, and amount of Commission Credit, if any, shall be memorialized by Lease Amendment.

4.12 AS-BUILT DRAWINGS (OCT 2019)

Not later than **10** days after the acceptance of the Space, the Lessor, at Lessor's expense, shall furnish to the Government a complete set of Computer Aided Design (CAD) files of as-built floor plans showing the Space under Lease, as well as corridors, stairways, and core areas. As-built drawings shall

Exhibit A

include those for Civil, Architectural, Mechanical, Electrical, and Plumbing features, including, but not limited to, those for IT, Communications, Security, and Fire Protection. The plans shall have been generated by a CAD program which is compatible with the latest release of AutoCAD. The required file extension is ".DWG." Clean and purged files shall be submitted in a digital format. They shall be labeled with Building name, address, list of drawing(s), date of the drawing(s), and Lessor's architect and architect's phone number. The Lessor's operator shall demonstrate the submission on GSA equipment, if requested by the LCO.

4.13 LIQUIDATED DAMAGES (JUN 2012)

In case of failure on the part of the Lessor to complete the work within the time fixed in the Lease, the Lessor shall pay the Government as fixed and agreed liquidated damages \$~~XX~~ for each and every calendar day that the delivery is delayed beyond the date specified for delivery of all the Space ready for occupancy by the Government. This remedy is not exclusive and is in addition to any other remedies which may be available under this Lease or at law. This liquidated sum is not meant as a penalty, but as an approximation of actual damages that would be suffered by the Government because of the Lessor's delay.

4.14 SEISMIC RETROFIT (SEP 2013)

The following requirements apply to Leases requiring seismic retrofit:

- A. The Lessor shall provide a final construction schedule, all final design and construction documents for the seismic retrofit, including structural calculations, drawings, and specifications to the Government for review and approval prior to the start of construction. When required by local building code, a geotechnical report shall be made available to the Government.
- B. The Lessor's registered civil or structural engineer shall perform special inspections to meet the requirements of Chapter 17 of the International Building Code (IBC).
- C. For Leases requiring seismic retrofit, the Space will not be considered substantially complete until a Seismic Form E - Certificate Of Seismic Compliance - Retrofitted Building, certifying that the Building meets the Basic Safety Objective of ASCE/SEI 41, executed by a registered civil or structural engineer, has been delivered to the LCO.

4.15 ~~LESSOR'S PROJECT MANAGEMENT RESPONSIBILITIES (OCT 2020)~~ INTENTIONALLY DELETED

SECTION 5 TENANT IMPROVEMENT COMPONENTS

5.01 TENANT IMPROVEMENT REQUIREMENTS (OCT 2016)

The TIs shall be designed, constructed, and maintained in accordance with the standards set forth in this Lease. For pricing, only those requirements designated within this Section 5, or designated as TIs within the attached agency requirements and Security Requirements, shall be deemed to be TI costs.

5.02 ~~TENANT IMPROVEMENT SPECIFICATIONS (SEP 2015)~~ INTENTIONALLY DELETED**5.03 FINISH SELECTIONS (SEP 2015)**

The Lessor must consult with the Government prior to developing a minimum of three (3) finish options to include coordinated samples of finishes for all interior elements such as paint, wall coverings, base coving, carpet, window treatments, laminates, and flooring. All samples provided must comply with specifications set forth elsewhere in this Lease. All required finish option samples must be provided at no additional cost to the Government within 10 Working Days after initial submission of DIDs, if applicable. GSA must deliver necessary finish selections to the Lessor within 10 Working Days after receipt of samples. The finish options must be approved by GSA prior to installation. The Lessor may not make any substitutions after the finish option is selected.

5.04 WINDOW COVERINGS (JUN 2012)

A. Window Blinds. All exterior windows shall be equipped with window blinds in new or like new condition, which shall be provided as part of the TIs. The blinds may be aluminum or plastic vertical blinds, horizontal blinds with aluminum slats of one-inch width or less, solar fabric roller shades, or an equivalent product pre-approved by the Government. The window blinds shall have non-corroding mechanisms and synthetic tapes. Color selection will be made by the Government.

B. Draperies:

1. If draperies are required, they shall be part of the TIs and the following minimum specifications shall apply:

a. Fabrics shall be lined with either white or off-white plain lining fabric suited to the drapery fabric weight. Draperies shall be floor, apron, or sill length, as specified by the Government, and shall be wide enough to cover window and trim. Draperies shall be hung with drapery hooks on well-anchored heavy duty traverse rods. Traverse rods shall draw from the center, right, or left side.

b. Construction. Any draperies to be newly installed shall be made as follows:

- i. Fullness of 100 percent, including overlap, side hems, and necessary returns;
- ii. Double headings of 4 inches turned over a 4-inch permanently finished stiffener;
- iii. Doubled side hems of 1-1/2 inches; 4-inch doubled and blind stitched bottom hems;
- iv. Three-fold pinch pleats;
- v. Safety stitched intermediate seams;
- vi. Matched patterns;
- vii. Tacked corners; and,
- viii. No raw edges or exposed seams.

c. Use of existing draperies must be approved by the Government.

5.05 DOORS: SUITE ENTRY (OCT 2019)

A. Suite entry doors shall be provided as part of the TIs and shall have a minimum clear opening of 32" wide x 84" high (per leaf). Doors shall meet the requirements of being a flush, solid core, 1-3/4-inch thick, wood door with a natural wood veneer face or an equivalent pre-approved by the Government. Hollow core wood doors are not acceptable. They shall be operable by a single effort; and shall meet the requirement of NFPA 101, Life Safety Code or the International Building Code (current as of the Lease Award Date). Doors shall be installed in a metal frame assembly which is primed and finished with a low VOC semi gloss oil-based paint finish that does not result in indoor air quality levels above 0.016 parts per million (ppm) of formaldehyde.

B. For leases 10,000 RSF or greater, the paint finish must meet applicable, statutory environmentally preferable criteria related to biobased and recovered material content as outlined in the Green Procurement Compilation at [HTTPS://SFTOOL.GOV/GREENPROCUREMENT](https://SFTOOL.GOV/GREENPROCUREMENT).and <https://sftool.gov/greenprocurement/green-products/3/building-finishes/1338/paint/0?addon=False>.

5.06 DOORS: INTERIOR (OCT 2019)

A. Doors within the Space shall be provided as part of the TIs and shall have a minimum clear opening of 32" wide x 80" high. Doors shall be flush, solid core, wood with a natural wood veneer face or an equivalent door pre-approved by the LCO. Hollow core wood doors are not acceptable. They shall be operable with a single effort, and shall meet the requirements of NFPA 101, Life Safety Code or the International Building Code (current as of the Lease Award Date). Doors shall be installed in a metal frame assembly which is primed and finished with a low VOC semi-gloss oil-based paint and which does not result in indoor air quality levels above 0.016 parts per million (ppm) of formaldehyde.

Exhibit A

B. For leases 10,000 RSF or greater, the paint finish must meet applicable, statutory environmentally preferable criteria related to biobased and recovered material content as outlined in the Green Procurement Compilation at [HTTPS://SFTOOL.GOV/GREENPROCUREMENT](https://SFTOOL.GOV/GREENPROCUREMENT).and <https://sftool.gov/greenprocurement/green-products/3/building-finishes/1338/paint/0?addon=False>.

5.07 DOORS: HARDWARE (SEP 2013)

Doors shall have door handles or door pulls with heavyweight hinges. The Lessor is encouraged to avoid the use of chrome-plated hardware. All doors shall have corresponding doorstops (wall- or floor-mounted) and silencers. All door entrances leading into the Space from public corridors and exterior doors shall have automatic door closers. Doors designated by the Government shall be equipped with 5-pin, tumbler cylinder locks and strike plates. All locks shall be master keyed. Furnish at least two master keys for each lock to the Government. Any exterior entrance shall have a high security lock, with appropriate key control procedures, as determined by Government specifications. Hinge pins and hasps shall be secured against unauthorized removal by using spot welds or pinned mounting bolts. The exterior side of the door shall have a lock guard or astragal to prevent tampering of the latch hardware. Doors used for egress only shall not have any operable exterior hardware. All security-locking arrangements on doors used for egress shall comply with requirements of NFPA 101 or the International Building Code current as of the Lease Award Date.

5.08 DOORS: IDENTIFICATION (JUN 2012)

Door identification shall be installed in approved locations adjacent to office entrances as part of the TIs. The form of door identification shall be approved by the Government.

5.09 PARTITIONS: SUBDIVIDING (OCT 2020)

A. Office subdividing partitions shall comply with applicable building codes and local requirements and ordinances and shall be provided as part of the TIs. Partitioning shall extend from the finished floor to the finished ceiling and shall be designed to provide a minimum sound transmission class (STC) of 37. Partitioning shall be installed by the Lessor at locations to be determined by the Government as identified in the DIDs, if applicable. They shall have a flame spread rating of 25 or less and a smoke development rating of 450 or less (ASTM E-84).

B. HVAC shall be rebalanced and lighting repositioned, as appropriate, after installation of partitions.

C. If installed in accordance with the "Automatic Fire Sprinkler System" and "Fire Alarm System" paragraphs, sprinklers and fire alarm notification appliances shall be repositioned as appropriate after installation of partitions to maintain the level of fire protection and life safety.

D. Partitioning requirements may be satisfied with existing partitions if they meet the Government's standards and layout requirements.

E. For leases 10,000 RSF or greater where the Government is a sole tenant of the Building, the Lessor is encouraged to use materials for newly installed gypsum board meeting applicable environmentally preferable criteria that are recommended in the Green Procurement Compilation at [HTTPS://SFTOOL.GOV/GREENPROCUREMENT](https://SFTOOL.GOV/GREENPROCUREMENT) and <https://sftool.gov/greenprocurement/green-products/3/building-finishes/1735/wallboardgypsum-boarddrywall/0?addon=False>.

5.10 WALL FINISHES (OCT 2019)

If the Government chooses to install a wall covering, the following specifications shall apply:

A. Commercial grade, weighing not less than 13 ounces per square yard.

B. For leases 10,000 RSF or greater, wall covering shall be vinyl-free, chlorine-free, plasticizer-free, with recycled or bio-based content. If the Government chooses to install a high-performance paint coating, it shall comply with the VOC limits of the Green Seal Standard GS-11.

5.11 PAINTING – TI (OCT 2019)

A. Prior to acceptance, all surfaces within the Space which are designated by GSA for painting shall be newly finished in colors and type of paint acceptable to the Government.

B. For leases 10,000 RSF or greater, the Lessor shall provide interior paints, primers, coatings, stains, and sealers that meet applicable, statutory, environmentally preferable criteria for biobased and recovered material content as outlined under the Green Procurement Compilation at [HTTPS://SFTOOL.GOV/GREENPROCUREMENT](https://SFTOOL.GOV/GREENPROCUREMENT) and <https://sftool.gov/greenprocurement/green-products/3/building-finishes/1338/paint/0?addon=False>. The Lessor shall use reprocessed latex paint in accordance with EPA's CPG (Comprehensive Procurement Guidelines) on all painted surfaces where feasible.

5.12 FLOOR COVERINGS AND PERIMETERS (OCT 2019)

A. Broadloom carpet or carpet tiles shall meet the requirements set forth in the specifications below. Floor perimeters at partitions shall have wood, rubber, vinyl, or carpet base. Floor covering shall be installed in accordance with manufacturing instructions to lay smoothly and evenly.

B. The use of existing carpet may be approved by the Government; however, existing carpet shall be repaired, stretched, and cleaned before occupancy and shall meet the static buildup requirement as stated in the specifications below.

C. Any alternate flooring shall be pre-approved by the Government.

D. SPECIFICATIONS FOR CARPET TO BE NEWLY INSTALLED OR REPLACED

Exhibit A

1. Product sustainability and environmental requirements. For leases 10,000 RSF or greater, floor covering and perimeter products must meet applicable, statutory, environmentally preferable criteria related to biobased and recovered material content as outlined under the Green Procurement Compilation at WWW.SFTOOL.GOV/GREENPROCUREMENT and [HTTPS://SFTOOL.GOV/GREENPROCUREMENT/GREEN-PRODUCTS/3/BUILDING-FINISHES/23/CARPET/0?ADDON=FALSE](https://SFTOOL.GOV/GREENPROCUREMENT/GREEN-PRODUCTS/3/BUILDING-FINISHES/23/CARPET/0?ADDON=FALSE), [HTTPS://SFTOOL.GOV/GREENPROCUREMENT/GREEN-PRODUCTS/3/BUILDING-FINISHES/1307/FLOOR-COVERINGS-NON-CARPET/0?ADDON=FALSE](https://SFTOOL.GOV/GREENPROCUREMENT/GREEN-PRODUCTS/3/BUILDING-FINISHES/1307/FLOOR-COVERINGS-NON-CARPET/0?ADDON=FALSE), and <https://sftool.gov/greenprocurement/green-products/3/building-finishes/97/floor-tiles-heavy-dutycommercial/0?addon=False>.

2. Face fiber content. Face yarn must be 100 percent nylon fiber. Loop Pile shall be 100 percent Bulk Continuous Filament (BCF); cut and loop shall be 100 percent BCF for the loop portion and may be BCF or staple for the cut portion; cut pile carpet shall be staple or BCF.

3. Performance requirements for broadloom and modular tile:

- a. Static: Less than or equal to 3.5 kV when tested by AATCC Test Method 134 (Step Test Option).
- b. Flammability: Meets CPSC-FF-1-70, DOC-FF-1-70 Methenamine Tablet Test criteria.
- c. Flooring Radiant Panel Test: Meets NFPA 253 Class I or II depending upon occupancy and fire code when tested under ASTM E-648 for glue down installation.
- d. Smoke Density: NBS Smoke Chamber - Less than 450 Flaming Mode when tested under ASTM E-662.

NOTE: Testing must be performed in a NVLAP accredited laboratory.

4. Texture Appearance Retention Rating (TARR). Carpet must meet TARR rating of at least 3.0 TARR for moderate traffic areas such as private offices, and heavy traffic areas such as training space, conference rooms, courtrooms, etc., and at least 3.5 TARR for severe traffic areas, including open office space, cafeteria, corridors and lobbies. The carpet must be evaluated using ASTM D-5252 Hexapod Drum Test as per the commercial carpet test procedure and the TARR classification determined using ASTM D-7330.

5. Carpet reclamation. Reclamation of existing carpet to be determined with potential vendor. When carpet is replaced, submit certification documentation from the reclamation facility to the LCO.

6. Warranty. Submit a copy of the manufacturer's standard warranty to the LCO within the first 60 days of Government occupancy. The Government is to be a beneficiary of the terms of this warranty.

5.13 HEATING AND AIR CONDITIONING (JUN 2012)

Zone Control. Provide individual thermostat control for office Space with control areas not to exceed 1,500 ABOA SF. Interior spaces must be separately zoned. Specialty occupancies (conference rooms, kitchens, etc.) must have active controls capable of sensing Space use and modulating HVAC system in response to Space demand. Areas that routinely have extended hours of operation shall be environmentally controlled through dedicated heating and air conditioning equipment. Special purpose areas (such as photocopy centers, large conference rooms, computer rooms, etc.) with an internal cooling load in excess of 5 tons shall be independently controlled. Provide concealed package air conditioning equipment to meet localized spot cooling of tenant special equipment. Portable space heaters are prohibited.

5.14 ELECTRICAL: DISTRIBUTION (SEP 2015)

A. All electrical, telephone, and data outlets within the Space shall be installed by the Lessor in accordance with the DIDs, if applicable. All electrical outlets shall be installed in accordance with NFPA Standard 70.

B. All outlets within the Space shall be marked and coded for ease of wire tracing; outlets shall be circuited separately from lighting. All floor outlets shall be flush with the plane of the finished floor. Outlet cover colors shall be coordinated with partition finish selections.

C. The Lessor shall in all cases safely conceal outlets and associated wiring (for electricity, voice, and data) to the workstation(s) in partitions, ceiling plenums, in recessed floor ducts, under raised flooring, or by use of a method acceptable to the Government.

5.15 TELECOMMUNICATIONS: DISTRIBUTION AND EQUIPMENT (JUN 2012)

Telecommunications floor or wall outlets shall be provided as part of the TIs. At a minimum, each outlet shall house one 4-pair wire jack for voice and one 4-pair wire jack for data. The Lessor shall ensure that all outlets and associated wiring, copper, coaxial cable, optical fiber, or other transmission medium used to transmit telecommunications (voice, data, video, Internet, or other emerging technologies) service to the workstation shall be safely concealed under raised floors, in floor ducts, walls, columns, or molding. All outlets/junction boxes shall be provided with rings and pull strings to facilitate the installation of cable. Some transmission medium may require special conduit, inner duct, or shielding as specified by the Government.

5.16 TELECOMMUNICATIONS: LOCAL EXCHANGE ACCESS (AUG 2008)

Provide sealed conduit to house the agency telecommunications system when required.

5.17 DATA DISTRIBUTION (OCT 2020)

The Lessor shall purchase and install data cable as part of the tenant improvements. The Lessor shall safely conceal data outlets and the associated wiring used to transmit data to workstations in floor ducts, walls, columns, or below access flooring. When cable consists of multiple runs, the Lessor shall provide ladder type or other acceptable cable trays to prevent cable coming into contact with suspended ceilings or sprinkler piping. Cable trays shall form a loop around the perimeter of the Space such that they are within a 30-foot horizontal distance of any single drop. If the Government chooses to purchase and install data cabling, then the Lessor shall provide, as part of the tenant improvements, outlets with rings and pull strings to facilitate the installation of the data cable.

5.18 ELECTRICAL, TELEPHONE, DATA FOR SYSTEMS FURNITURE (OCT 2020)

A. The Lessor shall provide as part of the TIs separate data, telephone, and electric junction boxes for the base feed connections to Government provided modular or systems furniture, when such feeds are supplied via wall outlets or floor penetrations. When overhead feeds are used, junction boxes shall be installed for electrical connections. Raceways shall be provided throughout the furniture panels to distribute the electrical, telephone, and data cable. The Lessor shall provide all electrical service wiring and connections to the furniture at designated junction points. Each electrical junction shall contain an 8-wire feed consisting of 3 general purpose 120-V circuits with 1 neutral and 1 ground wire, and a 120-V isolated ground circuit with 1 neutral and 1 isolated ground wire. A 20-ampere circuit shall have no more than 8 general purpose receptacles or 4 isolated ground "computer" receptacles.

B. The Lessor shall purchase and install data and telecommunications cable. Said cable shall be installed and connected to systems furniture by the Lessor/contractor with the assistance and/or advice of the Government or computer vendor. The Lessor shall provide wall mounted data and telephone junction boxes. When cable consists of multiple runs, the Lessor shall provide ladder-type or other acceptable cable trays to prevent Government provided cable coming into contact with suspended ceilings or sprinkler piping. Cable trays shall form a loop around the perimeter of the Space such that they are within a 30-foot horizontal distance of any single drop. Said cable trays shall provide access to both telecommunications data closets and telephone closets. If the Government chooses to purchase and install data and telecommunications cabling, then the Lessor shall provide, as part of the TIs, outlets with rings and pull strings to facilitate the installation of the data cable.

C. The Lessor shall furnish and install suitably sized junction boxes near the "feeding points" of the furniture panels. All "feeding points" shall be shown on Government approved design intent drawings. The Lessor shall temporarily cap off the wiring in the junction boxes until the furniture is installed. The Lessor shall make all connections in the power panel and shall keep the circuit breakers off. The Lessor shall identify each circuit with the breaker number and shall identify the computer hardware to be connected to it. The Lessor shall identify each breaker at the panel and identify the devices that it serves.

D. The Lessor's electrical contractor must connect power poles or base feeds in the junction boxes to the furniture electrical system and test all pre-wired receptacles in the systems furniture. Other Government contractors will be installing the data cable in the furniture panels for the terminal and printer locations, installing the connectors on the terminal/printer ends of the cable, and continuity testing each cable. Work shall be coordinated and performed in conjunction with the furniture, telephone, and data cable installers. Much of this work may occur over a weekend on a schedule that requires flexibility and on-call visits. The Lessor must coordinate the application of Certification of Occupancy with furniture installation.

5.19 LIGHTING: INTERIOR AND PARKING – TI (SEP 2015)

A. **FIXTURES:** Once the design intent drawings are approved, the Lessor shall design and provide interior lighting to comply with requirements under the paragraph, "Lighting: Interior and Parking – Shell." Any additional lighting fixtures and/or components required beyond what would have been provided for an open office plan (shell) are part of the TIs.

B. **PENDANT STYLE FIXTURES:** If pendant style lighting fixtures are used, the increase between the number of fixtures required in the Building shell and the Space layout is part of the TIs.

C. **MIXED FIXTURES:** DIDs, if applicable, may require a mixed use of recessed or pendant style fixtures in the Space.

D. **BUILDING PERIMETER:** There may be additional requirements for lighting in exterior parking areas, vehicle driveways, pedestrian walkways, and Building perimeter in the Security Requirements attached to this Lease.

5.20 AUTOMATIC FIRE SPRINKLER SYSTEM - TI (OCT 2016)

Where sprinklers are required in the Space, sprinkler mains and distribution piping in a "protection" layout (open plan) with heads turned down with an escutcheon or trim plate shall be provided as part of Shell rent. Any additional sprinkler fixtures and/or components required in the Space beyond what would have been provided for an open office plan (shell) are part of the TIs.

SECTION 6 UTILITIES, SERVICES, AND OBLIGATIONS DURING THE LEASE TERM

6.01 PROVISION OF SERVICES, ACCESS, AND NORMAL HOURS (JUN 2012)

A. The Government's normal hours of operations are established as **06:00** AM to **06:00** PM, Monday through Friday, with the exception of Federal holidays. Services, maintenance, and utilities shall be provided during these hours. The Government shall have access to the Premises and its Appurtenant Areas at all times without additional payment, including the use, during other than normal hours, of necessary services and utilities such as elevators, restrooms, lights, and electric power. Cleaning shall be performed during normal hours.

B. The Lessor and the Lessor's representatives, employees and contractors shall demonstrate a cooperative, positive, welcoming, respectful, professional and business-like demeanor and shall present a neat, clean, job-appropriate (professional) appearance.

6.02 UTILITIES (APR 2011)

The Lessor is responsible for providing all utilities necessary for base Building and tenant operations as part of the rental consideration.

VERSION 2:

6.03 UTILITIES SEPARATE FROM RENTAL/BUILDING OPERATING PLAN (OCT 2020) INTENTIONALLY DELETED

6.04 UTILITY CONSUMPTION REPORTING (OCT 2016)

Upon the effective date of the Lease, only for leases over 10,000 RSF, the Lessor shall provide regular quarterly reports for the amount of utilities (including water) consumed at the Building broken down by utility type per month for the duration of the Lease. Lessors shall report this utility consumption data within 45 calendar days of the end of each calendar quarter in the Environmental Protection Agency (EPA) Portfolio Manager online tool [HTTPS://WWW.ENERGYSTAR.GOV/](https://www.energystar.gov/). Data reported includes, but is not limited to, the number of actual units consumed, by utility type per month, and associated start and end date(s) for that consumption.

(Refer to the following link for reporting guidance: www.gsa.gov/ucf)

6.05 HEATING AND AIR CONDITIONING (OCT 2020)

A. In all office areas, temperatures shall conform to local commercial equivalent temperature levels and operating practices in order to maximize tenant satisfaction. These temperatures shall be maintained throughout the leased Premises and service areas, regardless of outside temperatures, during the hours of operation specified in the Lease. The Lessor shall perform any necessary systems start-up required to meet the commercially equivalent temperature levels prior to the first hour of each day's operation. At all times, humidity shall be maintained below 60% relative humidity.

B. During non working hours, heating temperatures shall be set no higher than 55° Fahrenheit, and air conditioning shall not be provided except as necessary to return Space temperatures to a suitable level for the beginning of working hours. Thermostats shall be secured from manual operation by key or locked cage. A key shall be provided to the Government's designated representative.

C. Thermal comfort. During all working hours, Lessor shall comply with ANSI/ASHRAE Standard 55, Thermal Environmental Conditions for Human Occupancy that corresponds with how the Building's HVAC system was designed to perform. At a minimum, Lessor must meet ASHRAE Standard 55-2004.

D. Warehouse or garage areas require heating and ventilation only. Cooling of this Space is not required. Temperature of warehouse or garage areas shall be maintained at a minimum of 50° Fahrenheit.

E. The Lessor shall conduct HVAC system balancing after any HVAC system alterations during the term of the Lease and shall make a reasonable attempt to schedule major construction outside of office hours.

F. Normal HVAC systems' maintenance shall not disrupt tenant operations.

G. **100** ABOA SF of the Premises shall receive cooling at all times (24 hrs a day, 365 days a year) for purposes of cooling the designated server room. The BTU output of this room is established as **8,500** BTU per hour. The temperature of this room shall be maintained at **67-71** degrees F, with humidity control not to exceed 60% relative humidity, regardless of outside temperature or seasonal changes.

H. In addition to the server room requirements stated above, the following areas shall receive HVAC at all times:

- 1. _____
- 2. _____

I. The 24 hour, 365 days a year HVAC service(s) stated above shall be provided by the Lessor as part of the operating rent established under the Lease.

6.06 OVERTIME HVAC USAGE (OCT 2020)

Exhibit A

- A. If there is to be a charge for heating or cooling outside of the Building's normal hours, such services shall be provided at the hourly rates set forth elsewhere in the Lease. Overtime usage services may be ordered by the Government's authorized representative only.
- B. When the cost of service is \$10,000 or less, the service may be ordered orally. An invoice shall be submitted to the official placing the order for certification and payment. Orders for services costing more than \$10,000 shall be placed using GSA Form 300, Order for Supplies or Services, or other approved service requisition procurement document. An invoice conforming to the requirements of this Lease shall be submitted to the official placing the order for certification and payment.
- C. Failure to submit a proper invoice within 120 days of providing overtime utilities shall constitute a waiver of the Lessor's right to receive any payment for such overtime utilities pursuant to this Lease.

6.07 JANITORIAL SERVICES (JUL 2020)

The Lessor shall maintain the Premises and all areas of the Property to which the Government has routine access in a clean condition and shall provide supplies and equipment for the term of the Lease. The following schedule describes the level of services intended. Performance will be based on the LCO's evaluation of results, not the frequency or method of performance.

- A. Daily. Empty trash receptacles. Sweep entrances, lobbies, and corridors. Spot sweep floors, and spot vacuum carpets. Clean drinking fountains. Sweep and damp mop or scrub restrooms. Clean all restroom fixtures, and replenish restroom supplies. Dispose of all trash and garbage generated in or about the Building. Wash inside and out or steam clean cans used for collection of food remnants from snack bars and vending machines. Dust horizontal surfaces that are readily available and visibly require dusting. Spray buff resilient floors in main corridors, entrances, and lobbies. Clean elevators and escalators. Remove carpet stains. Police sidewalks, parking areas, and driveways. Sweep loading dock areas and platforms. Clean glass entry doors to the Space.
- B. Three times a week. Sweep or vacuum stairs.
- C. Weekly. Damp mop and spray buff all resilient floors in restrooms and health units. Sweep sidewalks, parking areas, and driveways (weather permitting).
- D. Every two weeks. Spray buff resilient floors in secondary corridors, entrance, and lobbies. Damp mop and spray buff hard and resilient floors in office Space.
- E. Monthly. Thoroughly dust furniture. Completely sweep and/or vacuum carpets. Sweep storage Space. Spot clean all wall surfaces within 70 inches of the floor.
- F. Every two months. Damp wipe restroom wastepaper receptacles, stall partitions, doors, window sills, and frames. Shampoo entrance and elevator carpets.
- G. Three times a year. Dust wall surfaces within 70 inches of the floor, vertical surfaces and under surfaces. Clean metal and marble surfaces in lobbies. Wet mop or scrub garages.
- H. Twice a year. Wash all interior and exterior windows and other glass surfaces. Strip and apply four coats of finish to resilient floors in restrooms. Strip and refinish main corridors and other heavy traffic areas.
- I. Annually. Wash all venetian blinds, and dust 6 months from washing. Vacuum or dust all surfaces in the Building more than 70 inches from the floor, including light fixtures. Vacuum all draperies in place. Strip and refinish floors in offices and secondary lobbies and corridors. Shampoo carpets in corridors and lobbies. Clean balconies, ledges, courts, areaways, and flat roofs.
- J. Every two years. Shampoo carpets in all offices and other non-public areas.
- K. Every five years. Dry clean or wash (as appropriate) all draperies.
- L. As required. Properly maintain plants and lawns. Provide initial supply, installation, and replacement of light bulbs, tubes, ballasts, and starters. Provide and empty exterior ash cans and clean area of any discarded cigarette butts.
- M. Pest control. Control pests as appropriate, using Integrated Pest Management techniques, as specified in the GSA Environmental Management Integrated Pest Management Technique Guide (E402-1001).
- N. Routine Cleaning and Disinfecting Requirements for the Premises.

The Lessor shall wipe down daily all solid, high contact surfaces in Building common areas (defined here as those areas used or accessed by the Government's employees and visitors), and within the leased Space, using a disinfectant from the EPA-registered list of products identified as effective against Novel Coronavirus SARS-CoV-2 ([HTTPS://WWW.EPA.GOV/PESTICIDE-REGISTRATION/LIST-N-DISINFECTANTS-USE-AGAINST-SARS-COV-2](https://www.epa.gov/pesticide-registration/list-n-disinfectants-use-against-sars-cov-2)), or other products containing the same active ingredient(s) at the same or greater concentration than those on the list. Cleaning staff shall use products in accordance with directions provided by the manufacturer. Cleaning staff shall wear disposable gloves (e.g., latex, nitrile, etc.), facemasks, and any additional personal protective equipment (PPE) as recommended by the cleaning and disinfectant product manufacturers. Disinfection application and products should be chosen so as to not damage interior finishes or furnishings.

Examples of solid, high contact surfaces in Building common and high traffic areas include, but are not limited to, handrails, door knobs, key card scan pads, light switches, countertops, table tops, water faucets and handles, elevator buttons, sinks, toilets and control handles, restroom stall handles, toilet

Exhibit A

paper and other paper dispensers, door handles and push plates, water cooler and drinking fountain controls. It does not include agency owned equipment such as desks, telephones, computers, keyboards, docking stations, computer power supplies, and computer mouse, personal fans and heaters, desk lighting, etc. Disinfected surfaces should be allowed to air dry.

The Government reserves the right to issue notice to unilaterally cancel this routine cleaning and disinfecting at any time during the Lease term and, in such a case, the rental rate will be reduced by the amount specified for "Routine Cleaning and Disinfecting Services" under lease clause "Rent and Other Consideration." This reduction shall occur after the Government gives 30 calendar days notice to the Lessor and shall continue in effect until the Lease expires or is terminated.

6.08 SELECTION OF CLEANING PRODUCTS (OCT 2019)

For leases 10,000 RSF or greater where the Government is a sole occupant of the Building, the Lessor shall use cleaning products (including general purpose cleaners, floor cleaners, hand soap, etc.) that meet applicable, statutory, environmentally preferable criteria related to biobased and recovered material content as outlined under the Green Procurement Compilation at [HTTPS://SFTOOL.GREENPORCUREMENT](https://sftool.greenprocurement.gov) and <https://sftool.gov/greenprocurement/green-products/5/cleaning-products/0>.

6.09 SELECTION OF PAPER PRODUCTS (OCT 2019)

For leases 10,000 RSF or greater where the Government is a sole occupant of the Building, the Lessor shall select paper and paper products (e.g., restroom tissue and paper towels) that meet applicable, statutory, environmentally preferable criteria related to recovered material content as outlined under the Green Procurement Compilation at [HTTPS://SFTOOL.GREENPORCUREMENT](https://sftool.greenprocurement.gov) and <https://sftool.gov/greenprocurement/green-products/5/cleaning-products/0>

6.10 SNOW REMOVAL (OCT 2020)

Lessor shall provide snow removal services for the Government on all days for which this Lease has designated normal hours. Lessor shall clear parking lots if the accumulation of snow exceeds two inches. Lessor shall clear sidewalks, walkways and other entrances before accumulation exceeds 1.5 inches. The snow removal shall take place no later than 5:00 AM, without exception. Should accumulation continue throughout the day, the Lessor shall provide such additional snow removal services to prevent accumulation greater than the maximums specified in this paragraph. In addition to snow removal, the Lessor shall keep walkways, sidewalks and parking lots free of ice during the normal hours. The Lessor shall remove excess buildup of sand and/or ice melt to minimize slipping hazards. If the Building entrance(s) has a northern exposure, then Lessor shall take additional measures (e.g., more frequent snow removal or application of ice-melting agents, warning signs, etc.) to protect the safety of pedestrians.

6.11 MAINTENANCE AND TESTING OF SYSTEMS (SEP 2013)

A. The Lessor is responsible for the total maintenance and repair of the leased Premises. Such maintenance and repairs include the site and private access roads. All equipment and systems shall be maintained to provide reliable, energy efficient service without unusual interruption, disturbing noises, exposure to fire or safety hazards, uncomfortable drafts, excessive air velocities, or unusual emissions of dirt. The Lessor's maintenance responsibility includes initial supply and replacement of all supplies, materials, and equipment necessary for such maintenance. Maintenance, testing, and inspection of appropriate equipment and systems shall be done in accordance with current applicable codes, and inspection certificates shall be displayed as appropriate. Copies of all records in this regard shall be forwarded to the Government's designated representative.

B. At the Lessor's expense, the Government reserves the right to require documentation of proper operations, inspection, testing, and maintenance of fire protection systems, such as, but not limited to, fire alarm, fire sprinkler, standpipes, fire pump, emergency lighting, illuminated exit signs, emergency generator, prior to occupancy to ensure proper operation. These tests shall be witnessed by the Government's designated representative.

6.12 MAINTENANCE OF PROVIDED FINISHES (OCT 2016)

A. Paint, wall coverings. Lessor shall maintain all wall coverings and high performance paint coatings in "like new" condition for the life of the Lease. All painted surfaces shall be repainted at the Lessor's expense, including the moving and returning of furnishings, any time during the occupancy by the Government if the paint is peeling or permanently stained, except where damaged due to the negligence of the Government. All work shall be done after normal working hours as defined elsewhere in this Lease. In addition to the foregoing requirement,

1. Lessor shall repaint common areas at least every three years.
2. Lessor shall perform cyclical repainting of the Space every 5 years of occupancy. This cost, including the moving and returning of furnishings, as well as disassembly and reassembly of systems furniture per manufacturer's warranty, shall be at the Lessor's expense.

B. Carpet and flooring.

1. Except when damaged by the Government, the Lessor shall repair or replace flooring at any time during the Lease term when:
 - a. Backing or underlayment is exposed;
 - b. There are noticeable variations in surface color or texture;
 - c. It has curls, upturned edges, or other noticeable variations in texture;
 - d. Tiles are loose; or,
 - e. Tears or tripping hazards are present.
2. Notwithstanding the foregoing, as part of the rental consideration, the Lessor shall replace all carpet and base coving in the Space every 5 years, with a product which meets the requirements in the "Floor Coverings and Perimeters" paragraph in this Lease.

Exhibit A

3. Repair or replacement shall include the moving and returning of furnishings, including disassembly and reassembly of systems furniture per manufacturer's warranty, if necessary. Work shall be performed after the normal hours established elsewhere in this Lease.

6.13 ASBESTOS ABATEMENT (APR 2011)

If asbestos abatement work is to be performed in the Space after occupancy, the Lessor shall submit to the Government the occupant safety plan and a description of the methods of abatement and re-occupancy clearance, in accordance with OSHA, EPA, DOT, state, and local regulations and guidance, at least 4 weeks prior to the abatement work.

6.14 ONSITE LESSOR MANAGEMENT (APR 2011)

The Lessor shall provide an onsite Building superintendent or a locally designated representative available to promptly respond to deficiencies, and immediately address all emergency situations.

6.15 IDENTITY VERIFICATION OF PERSONNEL (OCT 2020)

A. The Government reserves the right to verify identities of personnel with routine and/or unaccompanied access to the Government's Space, including both pre and post occupancy periods. The Lessor shall comply with the agency personal identity verification procedures below that implement [Homeland Security Presidential Directive-12](#) (HSPD-12), Office of Management and Budget (OMB) guidance [M-05-24](#) and [M-19-17](#), and Federal Information Processing Standards Publication (FIPS PUB) Number 201, as amended. These policies require the Government to conduct background investigations and make HSPD-12 compliant suitability determinations for all persons with routine or unaccompanied access to Government leased Space. By definition, this includes at a minimum each employee of the Lessor, as well as employees of the Lessor's contractors or subcontractors who will provide building operating services requiring routine access to the Government's leased Space for a period greater than 6 months. The Government may also require this information for the Lessor's employees, contractors, or subcontractors who will be engaged to perform alterations or emergency repairs in the Government's Space.

B. Application Process: The background investigation will be done using the Government's prescribed process. The Lessor must provide information on each of their contractor/personnel meeting the above criteria to the Government, whereupon each identified contractor/personnel will be notified with instructions for completing the identity verification application within a given time frame. The application process will include completing supplemental information forms that must be inputted into the identity verification system in order for the application to be considered complete. Additionally, the Lessor must ensure prompt completion of the fingerprint process for their contractor/personnel. Email notifications will be sent with instructions on the steps to be taken to schedule an appointment for fingerprinting at an approved regional location along with instructions on how to complete the background investigation application.

C. The Lessor must ensure the Lease Contracting Officer (or the Lease Contracting Officer's designated representative) has all of the requested documentation timely to ensure the completion of the investigation.

D. Based on the information furnished, the Government will conduct background investigations. The Lease Contracting Officer will advise the Lessor in writing if a person fails the investigation, and, effective immediately, that person will no longer be allowed to work or be assigned to work in the Government's Space.

E. Throughout the life of the Lease, the Lessor shall provide the same data for any new employees, contractors, or subcontractors who will be assigned to the Government's Space in accordance with the above criteria. In the event the Lessor's contractor or subcontractor is subsequently replaced, the new contractor or subcontractor is not required to have persons re-apply who were cleared through this process while associated with the former contractor or subcontractor in accordance with GSA policy. The Lessor shall require each cleared person to re-apply and obtain a new clearance in accordance with GSA policy.

F. The Lessor is accountable for not allowing contractors to start work without the successful completion of the appropriate background investigation as required by GSA policy.

G. Access Card Retrieval/Return: Upon an Entry on Duty notification, the Government will issue a Personal Identity Verification (PIV) credential that is sometimes referred to as a GSA Access card. Lessors are responsible for all PIV credential issued to their contractors/personnel pursuant to this Lease. Lessors are specifically responsible for ensuring that all GSA PIV access cards are returned to the Lease Contracting Officer or their designee whenever their employees or a contractor no longer require access to the Space (such as When no longer needed for contract performance, upon completion of the Contractor employee's employment, and upon contract completion or termination). Additionally, the Lessor must notify the Lease Contracting Officer or their designee whenever a GSA PIV Access card is lost or stolen in which event the Lessor may be responsible for reimbursing the Government for replacement credentials at the current cost per PIV HSPD12 credential. Unreturned PIV Access cards will be considered as lost or stolen cards.

H. The Government reserves the right to conduct additional background checks on Lessor personnel and contractors with routine access to Government leased Space throughout the term of the Lease to determine who may have access to the Premises.

I. The Lease Contracting Officer may delay final payment under a contract if the Contractor fails to comply with these requirements.

J. The Lessor shall insert this paragraph in all subcontracts when the subcontractor is required to have physical access to a federally controlled facility or access to a federal information system.

6.16 SCHEDULE OF PERIODIC SERVICES (OCT 2020)

Exhibit A

Upon acceptance of the Space, the Lessor shall provide the LCO with a detailed written schedule of all periodic services and maintenance to be performed other than daily, weekly, or monthly.

6.17 LANDSCAPING (OCT 2019)

A. For leases 10,000 RSF or greater where the Government is the sole occupant of the building, the Lessor shall use landscaping products that meet applicable, statutory, environmentally preferable criteria related to recycled content as outlined under the Green Procurement Compilation at <HTTPS://SFTOOL/GREENPROCUREMENT> AND <HTTPS://SFTOOL.GOV/GREENPROCUREMENT/GREEN-PRODUCTS/6/LANDSCAPING-PRODUCTS/0>.

B. Landscape management practices shall prevent pollution by:

1. Employing practices which avoid or minimize the need for herbicides, fertilizers and pesticides; and
2. Composting/recycling all yard waste.

C. INTENTIONALLY DELETED

6.18 LANDSCAPE MAINTENANCE (APR 2011)

Landscape maintenance shall be performed during the growing season at not less than a weekly cycle and shall consist of watering, weeding, mowing, and policing the area to keep it free of debris. Pruning and fertilization shall be done on an as-needed basis. In addition, dead, dying, or damaged plants shall be replaced.

6.19 RECYCLING (JUN 2012)

A. For Leases greater than 10,000 rentable SF, with a Lease term greater than six months, the Lessor shall establish a recycling program for (at a minimum) paper, corrugated cardboard, glass, plastics, and metals where local markets for recovered materials exist.

B. Where state or local law, code, or ordinance requires recycling programs for the Premises, Lessor shall comply with such state and/or local law, code, or ordinance.

C. When implementing any recycling program, the Lessor shall provide an easily accessible, appropriately sized area (2 SF per 1,000 SF of Building gross floor area) that serves the Space for the collection and storage of materials for recycling. Telecom rooms are not acceptable as recycling space. During the Lease term, the Lessor agrees, upon request, to provide the Government with additional information concerning recycling programs maintained in the Building and in the Space.

6.20 RANDOLPH-SHEPPARD COMPLIANCE (SEP 2013)

During the term of the Lease, the Lessor may not establish vending facilities within the leased Space that will compete with any Randolph-Sheppard vending facilities.

6.21 SAFEGUARDING AND DISSEMINATION OF CONTROLLED UNCLASSIFIED INFORMATION (CUI) BUILDING INFORMATION (FEB 2020)

This clause applies to all recipients of CUI building information (which falls within the CUI Physical Security category), including offerors, bidders, awardees, contractors, subcontractors, lessors, suppliers and manufacturers.

Marking CUI. Contractors must submit any contractor-generated documents that contain building information to GSA for review and identification of any CUI building information that may be included. In addition, any documents GSA identifies as containing CUI building information must be marked in accordance with the Order and the Marking Controlled Unclassified Information Handbook (the current version may be found at <https://www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf>) before the original or any copies are disseminated to any other parties. If CUI content is identified, the CO may direct the contractor, as specified elsewhere in this contract, to imprint or affix CUI document markings (CUI) to the original documents and all copies, before any dissemination, or authorized GSA employees may mark the documents.

1. Authorized recipients.

- a. Building information designated as CUI must be protected with access strictly controlled and limited to those individuals having a Lawful Government Purpose to access such information, as defined in 32 C.F.R. § 2002.4(bb). Those with such a Lawful Government Purpose may include Federal, state and local government entities, and non-governmental entities engaged in the conduct of business on behalf of or with GSA. Non-governmental entities may include architects, engineers, consultants, contractors, subcontractors, suppliers, utilities, and others submitting an offer or bid to GSA, or performing work under a GSA contract or subcontract. Recipient contractors must be registered as "active" in the System for Award Management (SAM) database at www.sam.gov, and have a Lawful Government Purpose to access such information. If a subcontractor is not registered in the SAM database and has a Lawful Government Purpose to possess CUI building information in furtherance of the contract, the subcontractor must provide to the contractor its DUNS number or its tax ID number and a copy of its business license. The contractor must keep this information related to the subcontractor for the duration of the contract and subcontract.
- b. All GSA personnel and contractors must be provided CUI building information when needed for the performance of official Federal, state, and local government functions, such as for code compliance reviews and the issuance of building permits. Public safety entities such as fire and utility departments may have a Lawful Government Purpose to access CUI building information on a case-by-case basis. This clause must not prevent or encumber the necessary dissemination of CUI building information to public safety entities.

Exhibit A

2. Dissemination of CUI building information:
 - a. By electronic transmission. Electronic transmission of CUI information outside of the GSA network must use session encryption (or alternatively, file encryption) consistent with National Institute of Standards and Technology (NIST) SP 800-171. Encryption must be through an approved NIST algorithm with a valid certification, such as Advanced Encryption Standard or Triple Data Encryption Standard, in accordance with Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules, as required by GSA policy.
 - b. By nonelectronic form or on portable electronic data storage devices. Portable electronic data storage devices include CDs, DVDs, and USB drives. Nonelectronic forms of CUI building information include paper documents, photographs, and film, among other formats.
 - i. By mail. Contractors must only use methods of shipping that provide services for monitoring receipt such as track and confirm, proof of delivery, signature confirmation, or return receipt.
 - ii. In person. Contractors must provide CUI building information only to authorized recipients with a Lawful Government Purpose to access such information. Further information on authorized recipients is found in section 1 of this clause.
3. Record keeping. Contractors must maintain a list of all entities to which CUI is disseminated, in accordance with sections 2 and 3 of this clause. This list must include, at a minimum:
 - 1) The name of the state, Federal, or local government entity, utility, or firm to which CUI has been disseminated;
 - 2) The name of the individual at the entity or firm who is responsible for protecting the CUI building information, with access strictly controlled and limited to those individuals having a Lawful Government Purpose to access such information;
 - 3) Contact information for the named individual; and
 - 4) A description of the CUI building information provided.

Once "as built" drawings are submitted, the contractor must collect all lists maintained in accordance with this clause, including those maintained by any subcontractors and suppliers, and submit them to the CO. For Federal buildings, final payment may be withheld until the lists are received.

4. Safeguarding CUI documents. CUI building information (both electronic and paper formats) must be stored within controlled environments that prevent unauthorized access. GSA contractors and subcontractors must not take CUI building information outside of GSA or their own facilities or network, except as necessary for the performance of that contract. Access to the information must be limited to those with a Lawful Government Purpose for access.
5. Destroying CUI building information. When no longer needed, CUI building information must either be returned to the CO or destroyed in accordance with guidelines in NIST Special Publication 800-88, Guidelines for Media Sanitization.
6. Notice of disposal. The contractor must notify the CO that all CUI building information has been returned or destroyed by the contractor and its subcontractors or suppliers in accordance with paragraphs 4 and 5 of this clause, with the exception of the contractor's record copy. This notice must be submitted to the CO at the completion of the contract to receive final payment. For leases, this notice must be submitted to the CO at the completion of the lease term.
7. CUI security incidents. All improper disclosures or receipt of CUI building information must be immediately reported to the CO and the GSA Incident Response Team Center at gsa-ir@gsa.gov. If the contract provides for progress payments, the CO may withhold approval of progress payments until the contractor provides a corrective action plan explaining how the contractor will prevent future improper disclosures of CUI building information. Progress payments may also be withheld for failure to comply with any provision in this clause until the contractor provides a corrective action plan explaining how the contractor will rectify any noncompliance and comply with the clause in the future.
8. Subcontracts. The contractor and subcontractors must insert the substance of this clause in all subcontracts.

6.22 INDOOR AIR QUALITY (OCT 2019)

A. The Lessor shall control airborne contaminants at the source and/or operate the Space in such a manner that indoor air quality action limits identified in the PBS Desk Guide for Indoor Air Quality Management (Companion to GSA Order PBS 1000.8), OSHA regulatory limits, and generally accepted consensus standards are not exceeded. .

B. The Lessor shall avoid the use of products containing toxic, hazardous, carcinogenic, flammable, or corrosive ingredients as determined from the product label or manufacturer's safety data sheet. The Lessor shall use available odor-free or low odor products when applying paints, glues, lubricants, and similar wet products. When such equivalent products are not available, lessor shall use the alternate products outside normal working hours. Except in an emergency, the Lessor shall provide at least 72 hours advance notice to the Government before applying chemicals or products with noticeable odors in occupied Spaces and shall adequately ventilate those Spaces during and after application.

C. The Lessor shall serve as first responder to any occupant complaints about indoor air quality (IAQ). The Lessor shall promptly investigate such complaints and implement the necessary controls to address each complaint. Investigations shall include testing as needed, to ascertain the source and severity of the complaint.

D. The Government reserves the right to conduct independent IAQ assessments and detailed studies in Space that it occupies, as well as in space serving the Space (e.g., common use areas, mechanical rooms, HVAC systems, etc.). The Lessor shall assist the Government in its assessments and detailed studies by:

1. Making available information on Building operations and Lessor activities;
2. Providing access to Space for assessment and testing, if required; and

Exhibit A

3. Implementing corrective measures required by the LCO. The Lessor shall take corrective action to correct any tests or measurements that do not meet GSA policy action limits in the PBS Desk Guide for Indoor Air Quality Management (Companion to GSA Order PBS 1000.8), OSHA regulatory limits, and generally accepted consensus standards.

E. The Lessor shall provide to the Government safety data sheets (SDS) upon request for the following products prior to their use during the term of the Lease: adhesives, caulking, sealants, insulating materials, fireproofing or firestopping materials, paints, carpets, floor and wall patching or leveling materials, lubricants, clear finish for wood surfaces, janitorial cleaning products, pesticides, rodenticides, and herbicides. The Government reserves the right to review such products used by the Lessor within the Space, common building areas, ventilation systems and zones serving the Space, and the area above suspended ceilings and engineering space in the same ventilation zone as the Space.

F. The Lessor shall use high efficiency (HEPA) filtration vacuums for cleaning and minimum MERV 10 rated ventilation system filtration whenever feasible.

G. The Lessor is encouraged to comply with best practices outlined in Appendix D- Indoor Air Quality in GSA Leased Facilities (Best Practices) within the PBS Desk Guide for Indoor Air Quality Management (Companion to GSA Order PBS 1000.8).

6.23 RADON IN AIR (OCT 2016)

If Space planned for occupancy by the Government is on the second floor above grade or lower, the Lessor shall, prior to occupancy, test the leased Space for 2 days to 3 days using charcoal canisters. The Lessor is responsible to provide Space in which radon levels in air are below the GSA action levels of 4 pCi/L for childcare and 25 pCi/L for all other space. After the initial testing, a follow-up test for a minimum of 90 days using alpha track detectors shall be completed. For further information on radon, go to: [HTTPS://WWW.EPA.GOV/RADON](https://www.epa.gov/radon).

A. The radon concentration in the air of the Space shall be less than 4 pCi/L for childcare and 25 pCi/L for all other space, herein called "GSA action levels."

B. Initial Testing:

1. The Lessor shall:

a. Test for radon that portion of Space planned for occupancy by the Government in ground contact or closest to the ground up to and including the second floor above grade (Space on the third or higher floor above grade need not be measured);
b. Report the results to the LCO upon award; and
c. Promptly carry out a corrective action program for any radon concentration which equals or exceeds the GSA action levels.

2. Testing sequence. The Lessor shall measure radon by the standard test in sub-paragraph D.1, completing the test not later than 150 days after award, unless the LCO decides that there is not enough time to complete the test before Government occupancy, in which case the Lessor shall perform the short test in sub-paragraph D.2.

3. If the Space offered for Lease to the Government is in a Building under construction or proposed for construction, the Lessor, if possible, shall perform the standard test during buildout before Government occupancy of the Space. If the LCO decides that it is not possible to complete the standard test before occupancy, the Lessor shall complete the short test before occupancy and the standard test not later than 150 days after occupancy.

C. Corrective Action Program:

1. Program Initiation and Procedures.

a. If either the Government or the Lessor detects radon at or above the GSA action levels at any time before Government occupancy, the Lessor shall carry out a corrective action program which reduces the concentration to below the GSA action levels before Government occupancy.

b. If either the Government or the Lessor detects a radon concentration at or above the GSA action levels at any time after Government occupancy, the Lessor shall promptly carry out a corrective action program which reduces the concentration to below the GSA action levels.

c. If either the Government or the Lessor detects a radon concentration at or above the GSA action levels at any time after Government occupancy, the Lessor shall promptly restrict the use of the affected area and shall provide comparable temporary space for the tenants, as agreed to by the Government, until the Lessor carries out a prompt corrective action program which reduces the concentration to below the GSA action levels and certifies the Space for re-occupancy.

d. The Lessor shall provide the Government with prior written notice of any proposed corrective action or tenant relocation. The Lessor shall promptly revise the corrective action program upon any change in Building condition or operation which would affect the program or increase the radon concentration to or above the GSA action levels.

2. The Lessor shall perform the standard test in sub-paragraph D.1 to assess the effectiveness of a corrective action program. The Lessor may also perform the short test in sub-paragraph D.2 to determine whether the Space may be occupied but shall begin the standard test concurrently with the short test.

3. All measures to accommodate delay of occupancy, corrective action, tenant relocation, tenant re-occupancy, or follow-up measurement, shall be provided by the Lessor at no additional cost to the Government.

4. If the Lessor fails to exercise due diligence, or is otherwise unable to reduce the radon concentration promptly to below the GSA action levels, the Government may implement a corrective action program and deduct its costs from the rent.

D. Testing Procedures:

1. Standard Test. Place alpha track detectors throughout the required area for 91 or more days so that each covers no more than 2,000 ABOA SF. Use only devices listed in the EPA Radon Measurement Proficiency Program (RMP) application device checklists. Use a laboratory rated proficient in the EPA RMP to analyze the devices. Submit the results and supporting data (sample location, device type, duration, radon measurements, laboratory proficiency certification number, and the signature of a responsible laboratory official) within 30 days after the measurement.

Exhibit A

2. Short Test. Place alpha track detectors for at least 14 days, or charcoal canisters for 2 days to 3 days, throughout the required area so that each covers no more than 2,000 ABOA SF, starting not later than 7 days after award. Use only devices listed in the EPA RMP application device checklists. Use a laboratory rated proficient in the EPA RMP to analyze the devices. Submit the results and supporting data within 30 days after the measurement. In addition, complete the standard test not later than 150 days after Government occupancy.

6.24 RADON IN WATER (JUN 2012)

A. If the water source is not from a public utility, the Lessor shall demonstrate that water provided to the Premises is in compliance with EPA requirements and shall submit certification to the LCO prior to the Government occupying the Space.

B. If the EPA action level is reached or exceeded, the Lessor shall institute appropriate abatement methods which reduce the radon levels to below this action.

6.25 HAZARDOUS MATERIALS (SEP 2013)

A. The leased Space shall be free of hazardous materials, hazardous substances, and hazardous wastes, as defined by and according to applicable Federal, state, and local environmental regulations. Should there be reason to suspect otherwise, the Government reserves the right, at Lessor's expense, to require documentation or testing to confirm that the Space is free of all hazardous materials.

B. Lessor shall, to the extent of its knowledge, notify Government of the introduction of any hazardous materials onto the Property by Lessor or others, including but not limited to, co-tenants occupying Space in the Building.

6.26 MOLD (OCT 2020)

A. Actionable mold is either visible mold or airborne mold of types and concentrations in excess of that found in the local outdoor air or non-problematic control areas elsewhere in the same building, whichever is lower. The Lessor shall safely remediate all actionable mold in accordance with sub-paragraph C below.

B. The Lessor shall provide Space to the Government that is free from ongoing water leaks or moisture infiltration. The Space and ventilation zones serving the Space shall also be free of actionable mold.

C. Within 72 hours following a flood, plumbing leak or heavy rain whereby the Government Space or air zones serving the Space may have become moisture damaged, the Lessor shall repair any leakage sources and remediate the moisture damage. Whenever moisture damage or infiltration persists such that: mold is visible, mold odors are present, or occupants register complaints about mold, the Lessor shall employ an industrial hygienist or environmental consultant experienced in mold assessment to inspect and evaluate the Space and air zones serving the Space for visible and/or actionable mold presence; inspection shall take place no later than 15 calendar days following identification of a potential mold issue as described above. The Lessor shall promptly furnish these inspection results to the Government. After all leaks have been identified and corrected, the Lessor shall safely remediate all visible moldy and/or water damaged materials identified by the consultant using a qualified remediation contractor following the methods identified in "Mold Remediation in Schools and Commercial Buildings" (EPA 402-K-01-001, September 2008) and all applicable state laws pertaining to mold remediation practices. Remediation shall also remove actionable mold levels. Remediation shall be completed within a time frame acceptable to the Lease Contracting Officer which shall be no later than 90 calendar days following confirmation of the presence of actionable mold.

D. The presence of actionable mold in the Premises may be treated as a Casualty, as determined by the Government, in accordance with the Fire and Other Casualty clause contained in the General Clauses of this Lease. In addition to the provisions of the Fire and Other Casualty clause of this Lease, should a portion of the Premises be determined by the Government to be un-tenantable due to an act of negligence by the Lessor or his agents, the Lessor shall provide reasonably acceptable alternative Space at the Lessor's expense, including the cost of moving, and any required alterations.

6.27 OCCUPANT EMERGENCY PLANS (OCT 2020)

The Lessor is required to cooperate, participate and comply with the development and implementation of the Government's Occupant Emergency Plan (OEP) and a supplemental Shelter-in Place (SIP) Plan. Periodically, the Government may request that the Lessor assist in reviewing and revising its OEP and SIP. The Plan, among other things, will include evacuation procedures and an annual emergency evacuation drill, emergency shutdown of air intake procedures, and emergency notification procedures for the Lessor's Building engineer or manager, Building security, local emergency personnel, and Government agency personnel.

SECTION 7 ADDITIONAL TERMS AND CONDITIONS

7.01 SECURITY REQUIREMENTS (OCT 2016)

The Lessor agrees to the requirements of Federal Security Level **2** attached to this Lease.

7.02 MODIFIED LEASE PARAGRAPHS (OCT 2016)

The following paragraphs have been modified in this Lease:

7.03 ADDENDUM TO GSA FORM 3517B, GENERAL CLAUSES, NO FEDERALLY ELECTED OFFICIALS TO BENEFIT (OCT 2018)

The following clause is added to GSA Form 3517B, General Clauses:

No Federally Elected Officials to Benefit

- A. No person holding a Federally-elected office may directly or indirectly, regardless of whether such person took office before or after execution of the Lease, participate in or benefit from the Lease or any part thereof.
- B. The foregoing prohibition shall not apply if the Lease is entered into with a publicly-held corporation or publicly-held entity for the general benefit of such corporation or entity.
- C. Any violation of this clause shall render the Lease void, and the Government shall have no obligation to the Lessor in consequence thereof following the date the Lease is deemed void.
- D. In the event the Lease is voided pursuant to this clause, the Lessor shall be and remain liable to the Government for any and all costs associated with relocating and housing Government occupants from the leased premises to replacement premises. Such costs shall include, but not be limited to:
 - 1. moving and other physical relocation costs,
 - 2. furniture, fixtures and equipment costs related to occupancy of replacement premises,
 - 3. replication of tenant build-out costs at replacement premises,
 - 4. excess rental costs at replacement premises for the remainder of the firm term of the terminated Lease, and
 - 5. all other direct and consequential damages and costs associated with the Government relocating occupants from the leased premises to replacement premises, whether Federally-owned or leased.
- E. Nothing in this clause shall be deemed or interpreted to waive, modify, alter or limit any provision of existing law, including 41 U.S.C. § 6306 and 18 U.S.C. §§ 431-433.
- F. Lessor's obligation to be and remain liable for the costs and damages specified in this clause shall survive any voiding of the Lease pursuant to this clause or any provision of existing law.

PROGRAM FOR DESIGN

664-L10 SD ADMIN LEASE (FINAL)

MINOR REPLACEMENT LEASE - HT 7/31/2020 - PENDING AWARD
SAN DIEGO

Projected Year: 2020 Midpoint Year: 2021

VISN: 22 State: CA Station ID: 664
Station: San Diego
Installation: San Diego HCS

Project Created: 31 Jul 2019 04:12PM ET by Eric Rocha
Space Plan Last Edited: 14 Aug 2020 02:28PM ET by Eric Rocha

Contents List Created: 31 Jul 2019 05:25PM ET by Eric Rocha
Contents List Last Edited: 14 Aug 2020 02:28PM ET by Eric Rocha

Report Generated: 14 Aug 2020 02:29PM

Program For Design (14 Aug 2020 02:29PM)

664-L10 SD ADMIN LEASE (FINAL)
 MINOR REPLACEMENT LEASE - HT 7/31/2020 - PENDING AWARD
 SAN DIEGO

Department: 1 - HEALTH ADMINISTRATION SERVICE (246)

Functional Area: 1 - HIM - ADMIN MANAGEMENT

Qty	Room Code	Room Name	Unit Area	Net Area	Const Phase	Const Type
1	OFA07	Workstation, Program Specialist	42	42	1	0
1	OFA09	Office, Health Information Management Section (HIMS) Chief	100	100	1	0
1	OFA07	Workstation, Administrative Assistance	42	42	1	0

FA Totals: Room Qty: 3 Net Area: 184 Gross Area: 239

Department: 1 - HEALTH ADMINISTRATION SERVICE (246)

Functional Area: 2 - HIM - CODER

Qty	Room Code	Room Name	Unit Area	Net Area	Const Phase	Const Type
1	OFA07	Workstation, Coding Unit - Coder	42	42	1	0
1	OFA07	xVacant - Workstation, Coding Unit - Coder	42	42	1	0
1	OFA07	xVacant - Workstation, Coding Unit - Coder	42	42	1	0
1	OFA09	xVacant - Office, Coding Supervisor	100	100	1	0

FA Totals: Room Qty: 4 Net Area: 226 Gross Area: 294

Program For Design (14 Aug 2020 02:29PM)

664-L10 SD ADMIN LEASE (FINAL)
 MINOR REPLACEMENT LEASE - HT 7/31/2020 - PENDING AWARD
 SAN DIEGO

Department: 1 - HEALTH ADMINISTRATION SERVICE (246)

Functional Area: 3 - HIM - FILE CLERK / RECORD MGR.

Qty	Room Code	Room Name	Unit Area	Net Area	Const Phase	Const Type
1	OFA07	Workstation, Lead File Clerk	42	42	1	0
1	OFA07	Workstation, File Clerk	42	42	1	0
1	OFA07	Workstation, File Clerk	42	42	1	0
1	OFA07	Workstation, File Clerk	42	42	1	0
1	OFA07	Workstation, File Clerk	42	42	1	0
1	OFA07	Workstation, File Clerk	42	42	1	0
1	OFA07	Workstation, File Clerk	42	42	1	0
1	OFA07	Workstation, File Clerk	42	42	1	0
1	OFA07	Workstation, File Clerk	42	42	1	0
1	OFA07	Workstation, File Clerk	42	42	1	0
1	OFA07	Workstation, File Clerk	42	42	1	0
1	OFA07	Workstation, Program Specialist	42	42	1	0
1	OFA07	Workstation, Program Specialist	42	42	1	0
1	OFA09	Office, Records Manager / Scanning Supervisor	100	100	1	0

FA Totals: Room Qty: 14 Net Area: 646 Gross Area: 840

Program For Design (14 Aug 2020 02:29PM)

664-L10 SD ADMIN LEASE (FINAL)
 MINOR REPLACEMENT LEASE - HT 7/31/2020 - PENDING AWARD
 SAN DIEGO

Department: 1 - HEALTH ADMINISTRATION SERVICE (246)

Functional Area: 4 - HIM - MRT HIT & CDIS

Qty	Room Code	Room Name	Unit Area	Net Area	Const Phase	Const Type
1	OFA07	Workstation, MRT HIT (Medical Records Technician Health/ Information Technician	42	42	1	0
1	OFA07	Workstation, MRT HIT (Medical Records Technician Health/ Information Technician	42	42	1	0
1	OFA07	Workstation, MRT HIT (Medical Records Technician Health/ Information Technician	42	42	1	0
1	OFA07	Workstation, MRT HIT (Medical Records Technician Health/ Information Technician	42	42	1	0
1	OFA09	Office, Assistant Chief, HIM	100	100	1	0
1	OFA07	Workstation, Contract & OP CDIS	42	42	1	0
1	OFA07	Workstation, Contract & OP CDIS	42	42	1	0

FA Totals: Room Qty: 7 Net Area: 352 Gross Area: 458

Program For Design (14 Aug 2020 02:29PM)

664-L10 SD ADMIN LEASE (FINAL)
 MINOR REPLACEMENT LEASE - HT 7/31/2020 - PENDING AWARD
 SAN DIEGO

Department: 1 - HEALTH ADMINISTRATION SERVICE (246)

Functional Area: 5 - HIM - ROI (RELEASE OF INFORMATION)

Qty	Room Code	Room Name	Unit Area	Net Area	Const Phase	Const Type
1	OFA07	Workstation, ROI Legal	42	42	1	0
1	OFA07	Workstation, ROI	42	42	1	0
1	OFA07	Workstation, ROI	42	42	1	0
1	OFA07	Workstation, ROI	42	42	1	0
1	OFA07	Workstation, ROI	42	42	1	0
1	OFA09	Office, ROI Supervisor	100	100	1	0

FA Totals: Room Qty: 6 Net Area: 310 Gross Area: 403

Department: 1 - HEALTH ADMINISTRATION SERVICE (246)

Functional Area: 6 - HAS - ADMIN - OFFICE OF THE CHIEF (HAS)

Qty	Room Code	Room Name	Unit Area	Net Area	Const Phase	Const Type
1	OFA07	Workstation, HAS - Program Application Specialist	42	42	1	0
1	OFA07	Workstation, HAS - Program Specialist (ADPAC)	42	42	1	0

FA Totals: Room Qty: 2 Net Area: 84 Gross Area: 109

Program For Design (14 Aug 2020 02:29PM)

664-L10 SD ADMIN LEASE (FINAL)
 MINOR REPLACEMENT LEASE - HT 7/31/2020 - PENDING AWARD
 SAN DIEGO

Department: 1 - HEALTH ADMINISTRATION SERVICE (246)

Functional Area: 7 - HAS - BENEFICIARY TRAVEL SECTION

Qty	Room Code	Room Name	Unit Area	Net Area	Const Phase	Const Type
1	OFA09	Office, Supervisor - Ben Travel	100	100	1	0
1	OFA07	Workstation - Ben Travel	42	42	1	0
1	OFA07	Workstation - Ben Travel	42	42	1	0
1	OFA07	Workstation - Ben Travel	42	42	1	0
1	OFA07	Workstation - Ben Travel	42	42	1	0
1	OFA07	Workstation - Ben Travel	42	42	1	0
1	OFA07	Workstation - Ben Travel	42	42	1	0
1	OFA07	Workstation - Ben Travel	42	42	1	0
1	OFA07	Workstation - Ben Travel	42	42	1	0
1	OFA07	Workstation - Ben Travel	42	42	1	0

FA Totals: Room Qty: 9 Net Area: 436 Gross Area: 567

Program For Design (14 Aug 2020 02:29PM)

664-L10 SD ADMIN LEASE (FINAL)
 MINOR REPLACEMENT LEASE - HT 7/31/2020 - PENDING AWARD
 SAN DIEGO

Department: 1 - HEALTH ADMINISTRATION SERVICE (246)

Functional Area: 8 - HIM - SUPPORT/COMMON SPACE

Qty	Room Code	Room Name	Unit Area	Net Area	Const Phase	Const Type
1	CFR03	Conference Room, 20 people	500	500	1	0
1	FILE1	File / Staging Room	300	300	1	0
1	FILE1	File Room - File Cabinets/Laterals	150	150	1	0
1	MRWK1	Document Scanning Station	100	100	1	0
1	FILE1	File Room - File Cabinets/Laterals	150	150	1	0
1	MRWK1	Document Scanning Station	100	100	1	0

FA Totals: Room Qty: 6 Net Area: 1,300 Gross Area: 1,690

Program For Design (14 Aug 2020 02:29PM)

664-L10 SD ADMIN LEASE (FINAL)
 MINOR REPLACEMENT LEASE - HT 7/31/2020 - PENDING AWARD
 SAN DIEGO

Department: 1 - HEALTH ADMINISTRATION SERVICE (246)

Functional Area: 9 - HAS/HIM - OTHER

Qty	Room Code	Room Name	Unit Area	Net Area	Const Phase	Const Type
1	OFA07	Workstation - Ben Travel	42	42	1	0
1	OFA07	Workstation - Ben Travel	42	42	1	0
1	OFA07	Workstation - Ben Travel	42	42	1	0
1	OFA07	Workstation - Ben Travel	42	42	1	0
1	OFA07	Workstation - Ben Travel	42	42	1	0
1	OFA07	Workstation - Ben Travel	42	42	1	0
1	OFA07	Workstation - Ben Travel	42	42	1	0
1	OFA07	Workstation - Ben Travel	42	42	1	0
1	OFA07	Workstation - Ben Travel	42	42	1	0
1	OFA07	Workstation - Ben Travel	42	42	1	0
1	OFA07	Workstation - Ben Travel	42	42	1	0

FA Totals: **Room Qty:** 10 **Net Area:** 420 **Gross Area:** 546
Dept Totals: **Room Qty:** 61 **Net Area:** 3,958 **Gross Area:** 5,145

Program For Design (14 Aug 2020 02:29PM)

664-L10 SD ADMIN LEASE (FINAL)
 MINOR REPLACEMENT LEASE - HT 7/31/2020 - PENDING AWARD
 SAN DIEGO

Department: 2 - NURSING SERVICE ADMINISTRATION (254)

Functional Area: 1 - STAFF AND ADMINISTRATIVE AREA

Qty	Room Code	Room Name	Unit Area	Net Area	Const Phase	Const Type
1	OFA02	Office, Administrative Shared (2 Person)	150	150	1	0
1	OFA02	Office, Administrative Shared (2 Person)	150	150	1	0

FA Totals: Room Qty: 2 Net Area: 300 Gross Area: 390

Dept Totals: Room Qty: 2 Net Area: 300 Gross Area: 390

Program For Design (14 Aug 2020 02:29PM)

664-L10 SD ADMIN LEASE (FINAL)
 MINOR REPLACEMENT LEASE - HT 7/31/2020 - PENDING AWARD
 SAN DIEGO

Department: 3 - PROSTHETIC AND SENSORY AIDS SERVICE (308)

Functional Area: 1 - STAFF AND ADMINISTRATIVE AREA

Qty	Room Code	Room Name	Unit Area	Net Area	Const Phase	Const Type
1	OFA09	Office, Supervisory Prosthetic Representative	100	100	1	0
1	OFA07	Workstation, Program Specialist	42	42	1	0
1	OFA07	Workstation, Prosthetic Clerk	42	42	1	0
1	OFA07	Workstation, Purchasing Agent	42	42	1	0
1	OFA07	Workstation, Purchasing Agent	42	42	1	0
1	OFA07	Workstation, Purchasing Agent	42	42	1	0
1	OFA07	Workstation, Purchasing Agent	42	42	1	0
1	OFA07	Workstation, Purchasing Agent	42	42	1	0
1	OFA07	Workstation, Purchasing Agent	42	42	1	0
1	OFA07	Workstation, Purchasing Agent	42	42	1	0
1	OFA07	Workstation, Purchasing Agent	42	42	1	0
1	OFA07	Workstation, Tele-Work Staff	42	42	1	0
1	OFA07	Workstation, Tele-Work Staff	42	42	1	0

FA Totals: Room Qty: 13 Net Area: 604 Gross Area: 755

Dept Totals: Room Qty: 13 Net Area: 604 Gross Area: 755

Program For Design (14 Aug 2020 02:29PM)

664-L10 SD ADMIN LEASE (FINAL)
 MINOR REPLACEMENT LEASE - HT 7/31/2020 - PENDING AWARD
 SAN DIEGO

Department: 4 - WCPAC (TENANT)

Functional Area: 1 - STAFF ADMIN AREA

Qty	Room Code	Room Name	Unit Area	Net Area	Const Phase	Const Type
1	WRTM1	Team Room - UR Nurse	240	240	1	0
1	OFA02	Office, Supervisor & Trainee, Shared (2 Person)	100	100	1	0

FA Totals: Room Qty: 2 Net Area: 340 Gross Area: 442

Dept Totals: Room Qty: 2 Net Area: 340 Gross Area: 442

Program For Design (14 Aug 2020 02:29PM)

664-L10 SD ADMIN LEASE (FINAL)
 MINOR REPLACEMENT LEASE - HT 7/31/2020 - PENDING AWARD
 SAN DIEGO

Department: 5 - SUPPORT (SHARED)/OIT/SECURITY

Functional Area: 1 - SUPPORT/COMMON SPACE

Qty	Room Code	Room Name	Unit Area	Net Area	Const Phase	Const Type
1	SSLG1	Staff Lounge, 16 people (Copy Content from LGST5)	400	400	1	0
1	RPR03	Alcove, Copier/ Printer - RICOH	30	30	1	0
1	RPR03	Alcove, Copier/ Printer - RICOH	30	30	1	0
1	RPR03	Alcove, Copier/ Printer - RICOH	30	30	1	0
1	RPR03	Alcove, Copier/ Printer - RICOH	30	30	1	0
1	RPR03	Alcove, Copier/ Printer - Smaller Printers	30	30	1	0
1	RPR03	Alcove, Copier/ Printer - Smaller Printers	30	30	1	0
1	TNPF1	Toilet, Non-Patient, Multi-User, Female	205	205	1	0
1	TNPF1	Toilet, Non-Patient, Multi-User, Female	205	205	1	0
1	TNPM1	Toilet, Non-Patient, Multi-User, Male	205	205	1	0
1	TNPM1	Toilet, Non-Patient, Multi-User, Male	205	205	1	0
1	CFR02	Conference Room, 10 people	400	400	1	0

FA Totals: Room Qty: 12 Net Area: 1,800 Gross Area: 2,340

Program For Design (14 Aug 2020 02:29PM)

664-L10 SD ADMIN LEASE (FINAL)
 MINOR REPLACEMENT LEASE - HT 7/31/2020 - PENDING AWARD
 SAN DIEGO

Department: 5 - SUPPORT (SHARED)/OIT/SECURITY

Functional Area: 2 - TELECOMMUNICATIONS SUPPORT AREA

Qty	Room Code	Room Name	Unit Area	Net Area	Const Phase	Const Type
1	TETR1	Telecommunications Room (TR) (Refer to VA's TIL for latest JSNs assigned to this room)	120	120	1	0
1	TETR1	Telecommunications Room (TR) (Refer to VA's TIL for latest JSNs assigned to this room)	120	120	1	0

FA Totals: Room Qty: 2 Net Area: 240 Gross Area: 312

Department: 5 - SUPPORT (SHARED)/OIT/SECURITY

Functional Area: 3 - SECURITY

Qty	Room Code	Room Name	Unit Area	Net Area	Const Phase	Const Type
1	CSME1	Alcove, Enclosed - Security Equipment	28	28	1	0

FA Totals: Room Qty: 1 Net Area: 28 Gross Area: 36

Dept Totals: Room Qty: 15 Net Area: 2,068 Gross Area: 2,688

Program For Design (14 Aug 2020 02:29PM)

664-L10 SD ADMIN LEASE (FINAL)
 MINOR REPLACEMENT LEASE - HT 7/31/2020 - PENDING AWARD
 SAN DIEGO

Department: 6 - FRMS - PAYROLL (234)

Functional Area: 1 - STAFF AND ADMINISTRATIVE AREA

Qty	Room Code	Room Name	Unit Area	Net Area	Const Phase	Const Type
1	OFA09	Office, 1-person - Other	100	100	1	0
1	OFA07	Workstation - Other	42	42	1	0
1	OFA07	Workstation - Other	42	42	1	0
1	OFA07	Workstation - Other	42	42	1	0
1	OFA07	Workstation - Other	42	42	1	0
1	OFA07	Workstation - Other	42	42	1	0
1	OFA07	Workstation - Other	42	42	1	0
1	OFA07	Workstation - Other	42	42	1	0
1	OFA07	Workstation - Other	42	42	1	0
1	OFA07	Workstation - Other	42	42	1	0

FA Totals: Room Qty: 9 Net Area: 436 Gross Area: 567

Department: 6 - FRMS - PAYROLL (234)

Functional Area: 2 - SUPPORT AREA

Qty	Room Code	Room Name	Unit Area	Net Area	Const Phase	Const Type
1	FILE1	File/Storage Room	115	115	1	0

FA Totals: Room Qty: 1 Net Area: 115 Gross Area: 150

Dept Totals: Room Qty: 10 Net Area: 551 Gross Area: 716

Bldg Totals: Room Qty: 103 Net Area: 7,821 Sum of Dept Gross Area: 10,137 Gross Area: 13,178

Program For Design (14 Aug 2020 02:29PM)

664-L10 SD ADMIN LEASE (FINAL)
 MINOR REPLACEMENT LEASE - HT 7/31/2020 - PENDING AWARD
 SAN DIEGO

Department Area Summary (NSF/GSF)

Department	Total NSF	Total GSF
1 - HEALTH ADMINISTRATION SERVICE (246)(NTG Factor: 1.30)	3,958	5,145
2 - NURSING SERVICE ADMINISTRATION (254)(NTG Factor: 1.30)	300	390
3 - PROSTHETIC AND SENSORY AIDS SERVICE (308)(NTG Factor: 1.25)	604	755
4 - WCPAC (TENANT) (NTG Factor: 1.30)	340	442
5 - SUPPORT (SHARED)/OIT/SECURITY (NTG Factor: 1.30)	2,068	2,688
6 - FRMS - PAYROLL (234)(NTG Factor: 1.30)	551	716
Totals:	7,821	10,137

Program For Design (14 Aug 2020 02:29PM)

664-L10 SD ADMIN LEASE (FINAL)
MINOR REPLACEMENT LEASE - HT 7/31/2020 - PENDING AWARD
SAN DIEGO

Building Area Summary And Net to Gross Factor Breakdown

Current Building Factor applied to this Project: 1.30

	Building GSF
Current	13,178

STANDARDS ALERT

FEBRUARY 25, 2020
003C2B-SA-017

Office of Information and Technology Infrastructure Standards for Telecommunications Spaces

NEW STANDARD(S): The following standards are added to the Technical Information Library (TIL):

- [Office of Information and Technology \(OIT\) Infrastructure Standards for Telecommunications Spaces v2.2 \(10 Apr 2019\) \(OIT “eye” “ess”, OIT IS\)](#)
- [Office of Information and Technology \(OIT\) Design Guide Templates for Critical Telecommunications Spaces in Clinical and Non-clinical Environments v1.0 \(27 Dec 2018\) \(room templates”, OIT RT\)](#)

These documents are referred to collectively herein as the OIT Standards.

The OIT Standards are accessed via links on the [Design Guides \(PG-18-12\)](#) web page, below the Office of Information & Technology heading, with text referring to this Standards Alert.

IMPLEMENTATION: The OIT Standards:

- Must be utilized, and implemented to the maximum extent practicable, on new and existing projects during planning, design, and construction of all VA facilities;
- Become the primary standard for the technical content therein, and define best practices to enable the VA Enterprise Architecture for information technology; and
- Do not strictly supersede other TIL standards, due to differences in scope and the presence of conflicting criteria which require full consideration by the design team to resolve on a project-specific basis.

Project teams must:

- Proactively notify and engage OIT’s Enterprise Data Center Infrastructure Collaboration Team (EDICT) using the contact information provided in the OIT IS;

- Where conflicts arise between the OIT Standards and other TIL standards, or for other technical conflicts/issues:
 - Document the conflict/issue;
 - Consult with EDICT and other project stakeholders to achieve best-value project-specific solutions;
 - Document deliberation and solution;
 - Maintain documentation in the project file; and
 - Provide copies of documentation to EDICT and the TIL feedback mailbox (til@va.gov) to facilitate lessons learned and standards evolution.

For editorial issues which do not have a technical effect, email the TIL feedback mailbox at the address above.

Known conflicts/issues which require careful coordination and evaluation include, but are not limited to:

- Room names, minimum floor area, height, layout and finishes;
- HVAC configuration; and
- Cable type.

Further details on these and other issues are provided in Attachment 1.

PURPOSE: To improve facility planning, design, and construction project team awareness of and access to the OIT Standards. This will improve project planning, will eliminate or minimize re-design and associated cost and delay in latter project stages, and will ensure VA IT infrastructure is well-positioned to leverage advancements in information technology.

CONTACT: Bryan Unger, (202) 632-4690, bryan.unger@va.gov

ATTACHMENTS: The following provide more detailed information on specific technical issues; background on development of the OIT Standards and telecommunications standards on the TIL, and future plans; policy excerpts establishing OIT authority to develop the OIT Standards, and other related VA organizational authorities and responsibilities; and a list of references.

[Attachment 1 — Known Standards Conflicts and Other Issues](#)

[Attachment 2 — Background Information](#)

[Attachment 3 — Policy Excerpts](#)

[Attachment 4 — References](#)



Attachment 1

KNOWN TECHNICAL CONFLICTS AND OTHER ISSUES: This attachment provides more detail on select known conflicts between the OIT Standards and the major telecommunications program guides on the TIL, referred collectively herein as the TIL Telecom Standards:

- PG 18-9 Space Planning Criteria – Chapter 232 – Office of Information and Technology (OIT), October 2016
- PG 18-12 Design Guide – Office of Information and Technology (OIT), February 2011
- PG 18-10 Design Manual – Telecommunications and Special Telecommunications Systems, February 2016

In addition to the telecom standards above, there may be conflicting requirements with other TIL standards, such as PG 18-10 HVAC and Electrical Design Manuals, PG 18-1 Master Construction Specifications, etc.

Standards excerpts provided herein serve the purposes of narrative and reader convenience only, and do not supersede the actual standard text.

Conflicts/Issues

Scope of Application	A1-2
Room Names and Room Codes	A1-3
Room Minimum Floor Area of Main Computer Room and Telecommunications Room	A1-10
Room Height	A1-12
Room Layout – Separation of OIT and Veterans Health Administration (VHA) Medical Center Facilities Management Services (FMS) Equipment and Space	A1-12
Room Layout – Equipment Allowances and Clearances – General – MCRs and TRs	A1-14
Room Layout – Equipment Allowances and Clearances - Rack Rows Terminating Against A Wall	A1-15
Room Finishes – Raised Access Floor and Slab Depressions	A1-16
Room Finishes – Ceiling	A1-16
Room Occupancy – Shallow Rooms	A1-17
HVAC Configuration	A1-18
Minimum Category Cable Rating	A1-18
Reliability and Redundancy	A1-19
Manufacturer-Specific Equipment	A1-19



Scope of Application

The scope of application refers to the facilities and project types to which standards documents, or specific criteria therein, are applied.

In general, in accordance with [Design Alert 148](#), TIL standards apply “In all phases of Planning, Design, and Construction, for all VA projects.” The Design Alert provides further detail on conditions for variances, and individual standards documents address other specific applications.

Regarding the TIL Telecom Standards, the scope of application is developed marginally further than the Design Alert:

- PG 18-9’s scope is limited to specific medical facility types only, but this is a legacy limitation, and in practice it is applied at all VA facilities where it addresses programmed space. It is silent on facility age (new, existing) and project type (new, major renovation, minor renovation, etc.).
- PG 18-12’s scope is limited to “assisting medical staff and contracting officers” and “OIT areas and spaces in VA...medical facilities”, but this is a legacy limitation, and in practice is referenced for guidance at all VA facilities where it addressed programmed space. For both new construction and renovation of existing Telephone Equipment Rooms, the standard specifically requires use of Main Computer Room standards.
- PG 18-10 provides guidance for existing facilities and systems scattered throughout. There are too many individual items to list here.

As defined in the OIT IS, the scope of application of the OIT Standards is similar to the TIL standards, and includes limited allowances for existing facilities scattered throughout:

- p.1, 1.2 Scope — The Standards shall be applied to all aspects of IT support infrastructure at all VA facilities. “All aspects” includes, but is not limited to: planning, design, construction, sustainment (operations, maintenance, repair), restoration, modernization, and administration. “All VA facilities” includes but is not limited to VA Central Office (VACO) facilities and all field facilities managed by VA Administrations (Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), and the National Cemetery Administration (NCA)).
- p.2, 1.3 Administration — Existing IT support infrastructure that doesn’t conform to The Standards shall be brought into compliance during routine tech refresh, lifecycle replacement, upgrades, new installations, or renovations of existing space.
- p.2, 1.3 Administration — Facility managers should take every opportunity to bring telecommunications spaces into compliance with The Standards through incremental changes between scheduled sustainment activities.
- p.24, 3.1.2.2 Data Center Layout — All data center design for new data centers, expansion, or significant modification of existing data centers will be approved through



OIT Solution Delivery Data Center and Cloud Engineering
(VAITSEDatacenterEngineering2@va.gov).

- p.26, 3.1.2.2 Data Center Layout, Implementation Guidance — These standards apply to new data center and telecommunications space construction as well as expansion, modification, and operation of existing facilities.

Room Names and Room Codes

The TIL provides a Space and Equipment Planning System (SEPS) to assist facility planning. SEPS is a VA database and software tool for facility space and equipment planning which implements and is used in conjunction with narrative and graphical criteria found in PG 18-9 and PG 18-12. SEPS' master database is keyed to a standardized and coordinated list of Room Names and Room Codes to which design criteria are associated in SEPS and the Program Guides.

PG 18-9 and -12 group OIT rooms/spaces into six Functional Areas:

- Reception
- Computer
- Computer Support
- Telecommunications Support
- Staff and Administrative
- Staff Lounge, Lockers, and Toilets

Of these, the OIT Standards address only three: Computer, Computer Support, and Telecommunications Support. The tables on the following pages compare room/space designations from the OIT Standards to TIL room names and room codes. The tables also include select TIL rooms or other areas which are not addressed by the OIT Standards.

Project teams should establish project-specific designations for telecommunications spaces which avoid confusing facility staff and support design decisions. It may be necessary to have multiple designations for a room: planning/design room name/code, OIT IS data center classification, operational designation familiar to staff and is coordinated with existing facility signage conventions, building code designation, and an OIT datacenter program and inventory identifiers. This should be done on the project drawings, design narratives, calculations, and building information models.

Within the functional areas addressed by the OIT Standards, criteria for the following rooms are not provided:

- HVAC and Electrical Equipment Room, Computer Area
- Telephone Equipment
- Network Operations



- Storage, Active Data
- Storage, Temporary Data
- Storage, IT Equipment
- Receiving / Breakdown
- Workroom, Equipment Configuration / Repair
- Antenna Headend Equipment
- Telephone Operators
- Toilet, Staff
- Lounge, Telephone Operators

Project teams must solicit and document stakeholder feedback and consensus on space programs.



OIT STANDARDS TO TIL STANDARDS SPACE/ROOM COMPARISON TABLES

OIT Standards Room Designation	TIL/SEPS Room Name	TIL/SEPS Room Code
Computer Room	Main Computer Room	NA

Comments: The OIT IS also uses Computer Room in a generic sense to refer to any room that has computer equipment. Therefore, in practice, “Computer Room” is not formally an OIT IS room designation. Facilities should maintain existing Main Computer Room designation. This may need to be re-evaluated should a Backup Computer Room be eliminated from the facility (see next row), in which case the modifier “Main” for the remaining room is unnecessary.

PG 18-12 OIT Design Guide p.1-8, definition item W defines the term “Information Technology Equipment Room” as “Used in 2003 and later editions of NFPA 75 in lieu of the term “computer room”. This is considered an abstraction for design and code application. Facilities are not required to use “Information Technology Equipment Room” as a room name.

The TIL Standards also treat this space as consisting of several different zones or areas which are assigned design criteria individually. Refer to PG 18-9 and PG 18-12 for more information.

OIT Standards Room Designation	TIL/SEPS Room Name	TIL/SEPS Room Code
Equipment Room	Main Computer Room	NA

Comments: Equipment Room is not a formal room name. It is an ANSI/TIA designation for a level of the structured cabling system hierarchy.

OIT Standards Room Designation	TIL/SEPS Room Name	TIL/SEPS Room Code
Health Care Facility Equipment Room	NA	NA

Comments: This is not a formal room name. It is a room floor area/layout category in the OIT RT.



OIT Standards Room Designation	TIL/SEPS Room Name	TIL/SEPS Room Code
NA	Backup Computer Room	ITBU1

Comments: OIT Standards envision one computer room per facility, in accordance with Office of Management and Budget memoranda and Federal data center consolidation and optimization initiatives, and so do not provide standards for backup computer rooms.

OIT Standards Room Designation	TIL/SEPS Room Name	TIL/SEPS Room Code
NA	VoIP Active Equipment Digital Telephone (PBX) Equipment OIT (IT) Active Equipment OIT (IT) Passive Distribution Equipment FMS Active Equipment FMS Passive Distribution Equipment	TEIP1 TEDP1 ITAE1 ITPE1 FMAE1 FMPE1

Comments: These are not room names. They are areas within a Main Computer Room (MCR). Floor areas for these spaces are calculated separately for planning purposes, and combined to arrive at the area of the MCR. In contrast, the OIT Standards sizes the Main Computer Room as a whole, following the design assumption that all equipment will be collocated in the same rack row, or otherwise intermixed by rack or in rack as necessary to maximize efficient utilization of IT equipment, physical space, energy, etc.

OIT Standards Room Designation	TIL/SEPS Room Name	TIL/SEPS Room Code
Telecommunications Room (TR)	Telecommunications Room (TR)	TETR1
Health Care Facility Telecommunications Room	NA	NA

Comments: This is not a formal room name. It is a room floor area/layout category in the OIT RT.



OIT Standards Room Designation	TIL/SEPS Room Name	TIL/SEPS Room Code
Entrance Room (ER)	Demarcation Room (aka Demarc)	TEDR1
Health Care Entrance Room	NA	NA

Comments: This is not a formal room name. It is a room floor area/layout category in the OIT RT.

OIT Standards Room Designation	TIL/SEPS Room Name	TIL/SEPS Room Code
Shallow Room	NA	NA

Comments: Shallow Room is not a formal room name or other designation. Refer to the section “Room Occupancy – Shallow Rooms” for additional information.

OIT Standards Room Designation	TIL/SEPS Room Name	TIL/SEPS Room Code
Closet	NA	NA

Comments: In the TIL standards, it is indicated that the term “Telecommunications Room” replaces legacy terms “Signal Closet” and “Telecommunications Closet”. In general, “Closet” is not a formal room name. OIT Standards similarly deprecate this term.

OIT Standards Room Designation	TIL/SEPS Room Name	TIL/SEPS Room Code
Enterprise Test/Development Data Centers	NA	NA

Comments: This is not a formal room name, nor is it a formal data center category to which ANSI/TIA 942 Ratings and other design criteria are assigned. Instead, it is used to distinguish a facility, room, area, or equipment that is not currently used as “production” equipment for daily operations and is being prepared and/or evaluated for that purpose.



OIT Standards Room Designation	TIL/SEPS Room Name	TIL/SEPS Room Code
Small Server Room	NA	NA

Comments: Small server room is not a formal room name. It is a generic label for rooms with one-to-few racks of IT equipment which would be assigned to the Network Support Center data center category.

OIT Standards Room Designation	TIL/SEPS Room Name	TIL/SEPS Room Code
Distributor Room/ Enclosure Access Provider Space Service Provider Space	NA	NA

Comments: These are not formal room names. They are functional descriptions of select ASHRAE Class B spaces.

OIT Standards Room Designation	TIL/SEPS Room Name	TIL/SEPS Room Code
Main Distribution Area (MDA) Horizontal Distribution Area (HDA) Equipment Distribution Area (EDA)	NA	NA

Comments: These are not formal room names. These designate locations within a facility, room, or space where distribution equipment is installed, such as a rack footprint or units within a rack.

OIT Standards Room Designation	TIL/SEPS Room Name	TIL/SEPS Room Code
Data Center	NA	NA

Comments: Data Center is an abstract functional designation assigned to a room or stand-alone facility for use in OIT data center program management activities. Spaces designated as data centers are assigned to one of the four data center types listed below and designed in accordance with the associated criteria. Although PG 18-12 does associate the term data center with the Main Computer Room only, the OIT Standards apply the designation to Main Computer Rooms, Telecommunications Rooms, and other telecommunications spaces.



OIT Standards Room Designation	TIL/SEPS Room Name	TIL/SEPS Room Code
Core Data Center (CDC) Mission Support Center (MSC) Campus Support Center (CSC) Network Support Center (NSC)	NA	NA

Comments: These are not room or space designations, so there are no equivalent designations on the TIL. These are classifications assigned to telecommunications spaces (computer rooms or telecommunications rooms) to which are associated various technical specification for redundancy, environment, etc. Project teams should assign one of these designations to each telecommunications space as required by the OIT IS.

OIT Standards Room Designation	TIL/SEPS Room Name	TIL/SEPS Room Code
Extra Small Data Center Small Data Center Medium Data Center Large Data Center Extra Large Data Center	NA	NA

Comments: These are not room names, so there are no equivalent designations on the TIL. These are select room floor area/layout categories used in the OIT RT.

OIT Standards Room Designation	TIL/SEPS Room Name	TIL/SEPS Room Code
Standardized Data Center Identification	NA	NA

Comments: OIT IS 3.2.3 and 3.2.4 require assignment of standardized designations (FACILITYNAME, CITYTYPE, DCOI#, VA#) for use in the context of VA-wide data center program management and reporting to OMB on evolving federal data center initiatives, and program management of other IT spaces. In the context of projects, these designations are not room names used by facility personnel; they are an abstraction.



Room Minimum Floor Area of Main Computer Room and Telecommunications Room

The minimum floor area of the Main Computer Room and the Telecommunications Room in PG 18-12 OIT Design Guide are “sized on the quantity of floor-mounted cabinets, racks, and trunk and backbone lines in and out required to support the number of anticipated subscriber ports and lines. The number of anticipated ports and lines has been related to the total net area of the building based on OIT field experience. The quantity of cabinets and racks allocated will support the IT equipment needed for the anticipated number of lines and ports, plus both a 50-percent expected expansion and space for anticipated systems redundancy.” (PG 18-12 p.2-3). These relationships were derived from field surveys during the development PG 18-12 and the associated PG 18-9 and PG 18-5. For specifics, refer to the excerpts at the end of this section.

OIT Standards for minimum floor area of telecommunications spaces are communicated in the OIT RT. For Main Computer Rooms (i.e. data centers), several room templates representing a wide range of floor areas are derived from assumed equipment/capacity needs and application of OIT IS layout requirements. Similarly, several layouts for Telecommunications Rooms (TRs) and Entrance Rooms (ER) (i.e. Demarcs) are also provided. Minimum floor areas for these spaces also consider guidance in telecommunications industry standards (TIA, BISC). The OIT Standards do not explicitly reserve space for wall mounted equipment, although some is shown on the room templates.

The differing basis for the TIL and OIT standards can result in different minimum floor area requirements for telecommunications spaces.

TIL Standards, OIT IS, and industry standard requirements for telecommunications room area, while differing in expression, are essentially equivalent. Strict adherence to OIT RT space requirements may be unconservative in some cases due to the absence of a reserved clearance for wall mounted equipment, and due to deferral to recommendations in industry standards.

Project teams must ensure spaces are programmed and executed with sufficient floor area to accommodate project-specific and anticipated future capacity and equipment, all specified clearances, door swings, wall mounted equipment, conduit penetrations, and all other potential consumers of floor area.

Key TIL standards excerpts:

- PG 18-9 OIT Space Planning Criteria, p.12, 5.D.4
 - Provide one room with:
 - Minimum square footage is 20 net square feet (NSF) (1.9 net square meters (NSM)) if the total NSF of this facility is between 250 and 999.
 - Provide an additional 180 NSF if the total [NSF] of this facility is between 1,000 and 6,749 NSF;
 - Provide two rooms at 200 NSF if the total NSF of this facility is between 6,750 and 12,499 NSF;



- Requires additional rooms at 200 NSF with increasing facility NSF.
- PG 18-12 OIT Design Guide, p.4-84, Telecommunications Room Floor Plan — Implements the PG 18-9 narrative:
 - Room dimensions between inside faces of perimeter walls are 18'-2" by 11'-0" resulting in a room area of 200 NSF (18.6 net square meters (NSM)), stated in the top right-hand corner of the graphic.
 - An asterisk (*) next to those numerical statements refers to a note at the bottom of the graphic which states "Minimum room size is 20 NSF for facility sizes below 1000 NSF. Room shown is for facility sizes 1000 NSF and larger."
 - Further, there is a note with several qualifications at the very bottom, one of which states "The design team is responsible to perform the calculations that determine the quantities as well as the location of each component for every project."

Key OIT Standards excerpts:

- OIT IS
 - OIT IS has no explicit minimum net square footage requirements, relying instead on the cited EIA/TIA standard and other constraints such as minimum aisle clearances, airflow management, and rack layout guidance (hot aisle / cold aisle), etc.
 - OIT IS 3.1.2 states "...TRs...shall be designed and operated in accordance with EIA/TIA-942 Ratings for each data center classification, except as detailed specification are provided in this and other VA data center facilities standards."
- OIT RT
 - Sheet 5 – Detail 1 – Telecommunication Room Notes – Floor Space Requirements:
 - Minimum of 80 sq. ft. for a 1-rack TR.
 - Add an additional 20 sq. ft. per additional rack.
 - Minimum of 170 sq. ft. for a health care facility TR.

Key industry standards excerpts:

- EIA/TIA-942 4.1 states "Estimate...space...of the data center at full capacity [and] anticipated [expected] future...trends over the lifetime of the data center."
- EIA/TIA 942-6.4.2.2 states "The room shall be sized to meet the known requirements of specific equipment including proper clearances; this information can be obtained from the equipment provider(s). Sizing should include projected future as well as present requirements. See Annex D regarding data center space considerations."



- ANSI/BICSI 004 and 007 contain the following best practices for telecommunications rooms:
 - TR shall be designed in accordance with the requirements of the standards being followed (e.g. NFPA 99, ANSI/TIA-1197-A...)
 - The minimum floor dimensions of a TR shall meet the requirements of the AHJ (e.g. NFPA 99). Where AHJ requirements are not present, the minimum floor dimensions shall be 4 m x 4.5 m (12 ft x 14 ft) [18 m² or 168 ft²].
 - If the TR is to support additional systems (e.g. building automation, nurse call, security, CATV, paging, intercom, or clinical systems) the TRs physical size shall provide adequate space for these additional systems. This may require additional physical space.
 - A growth factor of 50% of the systems and services being supported by the TR should be considered when determining the final physical size of the TR.
 - Some facilities do not allow placing medical or building systems in the TR. Where this restriction applies, medical and building systems shall be placed within a dedicated space adjacent to the TR.
 - Room sizing shall take into consideration the wall mounting area required of each system.
 - Working space in front and behind racks, cabinets, and equipment shall be at least 0.9 m (3 ft).
 - Where systems, applications, and other requirements are not defined, TRs should be at least 4 m x 4.9 m (12 ft x 16 ft) [19.6 m² or 192 ft²].

Room Height

There are several standards in both the OIT Standards and TIL standards which directly or indirectly affect minimum heights of computer and telecommunications rooms, or related parameters (e.g. ceiling height, minimum raised floor height, bottom of lights, cable tray clearances, equipment heights, presence/absence of ceilings, etc.), are specified.

Project teams should maximize room height within the context of other project constraints (existing vs new, construction cost, etc.) while being mindful that a goal of OIT Standards is to maximize HVAC efficiency by maximizing vertical temperature differential and the height of heat collection.

Room Layout – Separation of OIT and Veterans Health Administration (VHA) Medical Center Facilities Management Services (FMS) Equipment and Space

In the TIL standards, for both the Main Computer Room (MCR) and Telecommunications Rooms (TR), OIT and FMS equipment are contained within a unified space, but there are requirements for separation of OIT and FMS equipment and for controlling access to FMS equipment.



In the MCR, TIL standards require separate OIT and FMS entrances, and a fixed, full-height, non-airflow-restricting interior fence between FMS and OIT equipment to control access to FMS equipment by OIT personnel, and vice versa. It is unclear if the MCR interior fence is intended to separate OIT and FMS overhead cabling and cable support.

TRs do not require separate entrances, and equipment separation and interior fence are optional. Equipment separation is required only if lockable rack and cabinet enclosures are not used. If equipment is separated and the fence is provided, FMS access must be through OIT space, and the fence is limited in height to eight feet allowing overhead cable tray to pass.

In contrast to the TIL standards, the OIT Standards do not require equipment separation, anticipating collocation in rack rows or individual racks, and convergence of OIT and FMS systems on common equipment as technological advances enable virtualization and performance required to accommodate life-safety and clinical applications.

For each FMS information technology and telecommunications system affected by a project, project teams should evaluate and document the technological, regulatory, and operational feasibility of implementing the converged approach envisioned by the OIT Standards. The starting point for planning and design must be consolidated and continuous space, not physically separated space. Written justification and OIT approval is required for maintaining or constructing physically separated space.

Relevant excerpts from PG 18-9 and PG 18-12 OIT standards:

- PG 18-9 and PG 18-12 facilitate planning of space for OIT and FMS areas separately;
- PG 18-9 §2, pp. 3 & 4, and PG 18-12 Definitions, pp. 1-7 & 8, list systems allocated to FMS and OIT areas;
- PG 18-12 p.2-18 requires the Main Computer Room (MCR) to have “separate entrances to the FMS and OIT areas”, and the MCR is required to be “functionally divided into OIT space and FMS space by a non-removable fence which extends from the floor slab to the structure above. The fence should not restrict airflow.”;
- PG 18-12 p.2-21 requires Telecommunications Rooms to have separate conduit paths feeding the OIT and FMS equipment: “OIT conduits shall enter the OIT side of the TR, and FMS conduits shall enter the FMS side of the TR”.
- PG 18-12 p.2-22 requires Telecommunications Rooms “be functionally divided into OIT space and FMS space. An optional barrier with keyed gates (sliding or hinged) may be provided. The barrier may be removable.”
- PG 18-12 p.4-32 OIT Passive Distribution Equipment Area Floor Plan (a component of the MCR), illustrates the fence with a note stating “Wire Mesh Partition from top of access floor to underside of suspended ceiling, Master Construction Specification (MCS) 10 22 13”. This is repeated on the floor plan for the adjacent FMS Passive Distribution Equipment area.



- PG 18-12 pp.4-20 & 44 floor plans show the separate entrances for OIT and FMS equipment areas of the MCR.
- PG 18-12 pp.4-84 through 87 illustrate the TR fence requirement, and a note describing the fence on p.4-88 states “Optional Wire Mesh partition to 96”H with lockable, sliding, wire mesh gates (36”W x 93”H) at each opening. Provide separate OIT and FMS equipment if lockable enclosures are not used at racks or cabinets.”

Room Layout – Equipment Allowances and Clearances – General – MCRs and TRs

There are several different equipment clearance parameters, which in some cases vary between the TIL standards and the OIT Standards.

Parameter	TIL Standards	OIT Standards
End of Row - MCR	To perimeter wall: 4’-0” min 5’-0” max (PG 18-12 p.4-2) Expressed as a range to accommodate 12” conduit entry (floor penetration) clearance while maintaining the minimum 4’-0” clearance.	To perimeter wall - 3’-0” To HVAC and power distribution equipment – 4’-0” min (6’-0” recommended) (OIT IS p.25, 3.1.2.2 Data Center Layout Standard, Table 12, ID 3 – Equipment Rows, Clearance)
Provided at Both Ends of Rows	See Discussion in Next Section	See Discussion in Next Section
Wall-Mounted Equipment Allowance – MCR – FMS Equipment Areas	12” (PG 18-12 p.2-23)	None
Conduit Entry (Floor Penetration) Allowance at Perimeter Wall – MCR – OIT Passive Distribution Equipment	12” (PG 18-12 p.4-32)	None
Wall-Mounted Equipment Allowance - TR	12” (PG 18-12 p.2-22)	None
Clearance at Front and Rear of Racks – TR – To Wall-Mounted Equipment Allowance	3’-0”	None



Parameter	TIL Standards	OIT Standards
Minimum Aisle Width – MCR – Cabinets (Clearance from front and rear)	4'-0"	In cold aisles - 4'-0" min In hot aisles - 3'-0" min (4'-0" recommended) (OIT IS p.24, 3.1.2.2 Data Center Layout Standard, Table 12, ID 1 – Aisles, Width)
Minimum Aisle Width – MCR – Racks (Clearance from front and rear)	3'-0"	See MCR Cabinets Above
Alignment with 24" Grid (Access Floor Tile Layout, or Floor Markings)	Access floor panel size "shall be 24 inches by 24 inches" (PG 18-12 p.2-11) There are no specific requirements or guidance to align equipment with the tile grid.	Yes – Front face of equipment (OIT IS p.24, 3.1.2.2 Data Center Layout Standard, Table 12, ID 1 – Aisles, Orientation; pp.68-71, 3.2.1 Data Center Position Identification)

Room Layout – Equipment Allowances and Clearances - Rack Rows Terminating Against A Wall

In the TIL standards, PG 18-12 p.2-19 states "Rows of cabinets and racks are pushed to one wall of the MCR. There will not be circulation space around both ends of a row." This is illustrated in PG 18-12 Floor Plans for each area of the MCR. PG 18-12 p.4-2 Figure 4.1 End Clearance Plan also has a note which states "[End clearance] required on at least one end of each row of cabinets, or racks." This implementation of the requirement differs from the original written text in that it doesn't prohibit clearance at both ends of the rack row.

In contrast, the OIT Standards clearly prohibit rows terminating into a wall, in effect requiring clearance at both ends.^{1,2} The rationale for this is to:

- Facilitate rack installation and replacement by providing a gap between the end rack and the wall to allow dollies wider than the rack to access the rack;
- Minimize path length and transit time during maintenance and emergency egress;
- Accommodate redundant and symmetric overhead power and data cable tray layouts.

¹ OIT IS p.25, 3.1.2.2. Data Center Layout Standard, Table 12, ID 3, Equipment Rows, Orientation

² OIT RT, Floor Plans on Sheets 4 through 18 illustrate implementation of OIT IS 3.1.2.2.



Room Finishes – Raised Access Floor and Slab Depressions

TIL standards for the Main Computer Room distribute cold air to the face of rack rows through a raised access floor plenum (e.g. PG 18-12 p.2-14 Figs. 2.1 & 2.2). There is also a corresponding requirement for a structural slab depression of 24" (PG 18-12 Section 4, Room Design Standards), although OIT EDICT reports that, in the course of their extensive site visits, slab depressions are rarely implemented, and flat slabs with raised access ramps are used instead.

In contrast, OIT Standards deprecate raised floors for new construction (OIT IS Table 11, ID 2, Floor Height; and 3.1.3.4), requiring them only if justified by computational fluid dynamics (CFD) analysis. Reasons for deprecating raised access floor include:

- Capture cost savings;
- Eliminate requirements for slab depressions and association restrictions on location of space within a building;
- Improve access to network and power cables for installation, maintenance, and inspection;
- Overhead busways eliminate the need for licensed electrician to execute circuit changes;
- Improve efficiency through a heat containment configuration;
- Reduce seismic risk;
- Eliminate underfloor maintenance;
- Eliminate cooling losses due to drawdown or recirculation caused by venturi effects;
- Eliminate risk of airflow restriction caused by underfloor obstructions;
- Maximize space efficiency by eliminating ramps;
- Eliminate risk of structural deficiencies in the raised floor system.

In the event raised access floor is required, the OIT Standards have extensive standards to optimize airflow.

PG 18-12 specifications for access floors (p.2-10 & 11), such as structural performance and ramp requirements, remain in effect, but must be reconciled with the OIT Standards. For example, the higher rack and cabinet densities and capacities anticipated by the OIT Standards may require increasing the minimum structural performance specifications in PG 18-12.

Room Finishes – Ceiling

TIL standards require acoustical ceiling tile (ACT) for the majority of OIT spaces, with some additional space-specific criteria.

OIT Standards are mixed. The OIT IS does not explicitly prohibit suspended ceilings, but does place restrictions on use of the plenum space and recommends removal of existing suspended



ceilings. The OIT RT has stronger language and specifically prohibits suspended ceilings in newly constructed spaces.

In summary, the OIT Standards are similar to the TIL standards, with the exception that, in the strongest interpretation of OIT Standards intent, suspended acoustic tile ceilings are prohibited in new computing spaces, and, in existing spaces, are recommended to be removed or converted to egg-crate/grate tiles.

TIL Standards Excerpts:

- PG 18-12 p.2-11 – Ceilings:
 - Where required for sanitation or moisture resistance, ACT should have a washable plastic (Mylar) finish.
 - In the Main Computer Room, and other rooms containing IT equipment, the ceiling finish should minimize dust and be light-colored to maximize light reflectance. Acceptable products include “Clean Room” type or Mylar-faced panels in an aluminum suspension system. Layout of the ceiling grid should align with the access floor system.
 - Suspended ceilings are not recommended in the Demarc Room(s), Telecommunications Room(s), and Antenna Headend Equipment Room.
- PG 18-12 Section 4, p.4-12 — Exposed ceilings are also specified for HVAC and Electrical Equipment rooms serving the Computer Area (includes Main Computer Room) and the Telephone Equipment Room.

OIT Standards Excerpts:

- OIT IS p.43 Table 23 & p.45 3.1.3.4.1 – Legacy facilities are encouraged to maximize room height through removal of aesthetic suspended ceilings to maximize cooling efficiency.
- OIT RT Sheet 3 Mechanical/Structural Notes – Ceilings: No suspended ceilings allowed.

Room Occupancy – Shallow Rooms

Shallow rooms are telecommunications spaces that have no or very little floor space, having a depth of a few feet (there is no formal definition for this space). Telecommunications conduit or equipment therein is generally within arms-length of the doorway, and, instead of dedicated lighting or HVAC, utilize services from the adjacent space (corridor, etc.).

TIL standards are silent on this type of space, except as may be found in referenced codes and industry standards. OIT standards restrict the use of these spaces as follows:

“VA shall not design or building “shallow rooms” or similar closets. Shallow rooms are intended for access to vertical chases and riser cables installed there only. Where a



distribution TR is necessary in a location (i.e. the third floor of the west wing of a hospital), VA shall construct and operate out of a standardized TR.”³

HVAC Configuration

PG 18-12 provides HVAC standards for OIT spaces, such as room environmental parameters (temperature and relative humidity range), outside air percentage, and duct noise class.⁴ For MCRs in particular, it acknowledges the inefficiency of whole room air mixing and cooling, expresses a preference for separate and contained supply and return air, describes cold- and hot-air containment, and mentions other needs such as maintaining acceptable air pressure on IT equipment, preventing underfloor air dams, preventing short-cycling, proper tile selection, sealing access floor penetrations, and a potential need for computational fluid dynamics (CFD) analysis. Diagrams and room Design Standards indicate that use of both cold-air containment and hot-air containment is the basis-of-design.

The OIT Standards are generally similar to the TIL basis-of-design and provide additional specifications and implementation details. Significant deviations from the TIL standards include:

- Deprecation of access flooring from the default state to one requiring justification using CFD;
- Environmental conditions measured at the rack rather than room ambient air;
- More detailed equipment specifications (minimum tonnage, humidification system types, redundancy associated with data center rating, distribution of high-density racks, etc.)

Minimum Category Cable Rating

On the TIL, PG 18-10 allows Cat 5e, 6, and 6A for horizontal distribution⁵. It contains a recommendation for 5e, and an approval process for Cat 6 and 6A. Cat 6 and 6A are not explicitly prohibited. It does prohibit specific non-copper, copper-clad, and similar conductors.

The OIT Standards require Category 6A (Cat 6A) unshielded twisted-pair (UTP) cable for horizontal distribution (e.g. between telecommunications rooms and wall outlets). Factory terminations are preferred, but field terminations are permitted. The Cat 6A requirement is derived from recommendations for Category 6 (Cat 6) in ANSI/TIA-1179 Health Care Facility Telecommunications Infrastructure. Cat 6A is specified to ensure reliable 10-gigabit-per-second Ethernet (GbE) data transfer rates over a greater length than Category 6 cable is rated for, to enable Power Over Ethernet (PoE), to enable high-bandwidth video applications, and to enable proliferation of wireless access points and devices. Existing Cat 6 cable is allowed with an approved variance.

³ OIT IS p.26 3.1.2.2 Data Center Layout Standard, Implementation Guidance

⁴ PG 18-10 HVAC Design Manual (Nov 2017 rev. Mar 2019) also provides HVAC criteria for OIT spaces. Refer to the data sheets on pp.6-103–8.

⁵ PG 18-10 3.2, Table 3.1



Project teams must evaluate the technical requirements of the information systems and devices utilizing the horizontal distribution and select cable which provide best-value to VA. OIT EDICT must be included in any TIL-specified approvals process where there are criteria overlaps. Project teams are encouraged to consider future demands which may arise within a reasonable period after completion of the project when making best-value decisions.

For projects associated with the Electronic Health Records Modernization (EHRM) program, cabling must be determined in accordance with the Electronic Health Records Modernization Cabling Infrastructure Memorandum dated 23 September 2019. This can be obtained on the [OEHRM Collaboration Site](#).

Reliability and Redundancy

The TIL Telecom Standards specify data service reliability using the Uptime Institute four-level Tier system. In contrast, the OIT Standards utilize ANSI/TIA 942 Ratings. Neither require certification.

Project teams must follow the OIT Standards and utilize ANSI/TIA 942 Ratings. VA self-certifies utilizing the TIA checklist.

Manufacturer-Specific Equipment

The OIT RT contains manufacturer-specific equipment data. These, and any other manufacturer-specific requirements that may be present in the OIT Standards, are mere examples to illustrate implementation of written performance requirements. Neither the written performance requirements, nor the equipment data, are intended to require sole-source or otherwise non-competitive acquisitions which do not provide best-value to VA. In the event project teams encounter requirements which may unnecessarily restrict competition and hinder best-value solutions, the TIL maintainers and relevant subject matter experts identified in the standards publications must be notified so they may advise on the project-specific issue and plan for standards updates.



Attachment 2

BACKGROUND: This section provides detail on the authorities and responsibilities of OIT and CFM and their interaction, development of the OIT Standards, development of TIL Telecom standards, and plans to further develop OIT and TIL Telecom standards.

Office of Information and Technology

OIT is led by the Assistant Secretary for Information and Technology and Chief Information Officer (AS/CIO). The VA CIO is a statutory position created by the Information Technology Management Reform Act of 1996⁶ (ITMRA96). ITMRA96 also assigned the VA Secretary authority over various aspects of information technology including capital planning and investment control, performance and results-based management, and acquisition; and it assigned the VA CIO duties to advise the Secretary on those issues, as well as execute various information resource management responsibilities, to include developing VA's information technology architecture.

The authorities and responsibilities of the CIO, and the scope and structure of OIT, have since evolved through the issuance, revision, application, and rescission of various Public Laws, Executive Orders, Office of Management and Budget (OMB) Memoranda, VA Memoranda and Directives, and other instruments of federal and agency policy. The latest non-VA instruments driving VA and OIT policy relevant to the OIT Standards include:

- The Federal Information Technology Acquisition Reform Act (FITARA)⁷
- OMB Memorandum M-15-14, Management and Oversight of Federal Information Technology, June 10, 2015
- OMB Memorandum M-16-19, Data Center Optimization Initiative (DCOI), August 1, 2016
- OMB Memorandum M-17-26, Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda, June 15, 2017

These are implemented through the following VA policies relevant to the OIT Standards:

- Directive 6008 Acquisition and Management of VA Information Technology Resources
- Directive 6051 Enterprise Architecture
- Directive 6004 Configuration, Changes, and Release Management Programs

6008 establishes CIO authority and responsibility over “all information-related assets that are part of or interact with VA’s information networks, services, and capabilities.” “information-

⁶ Pub. L. 104-106, National Defense Authorization Act of 1996, Division E

⁷ Pub. L. 113-291, National Defense Authorization Act for Fiscal Year 2015, Title VIII, Subtitle D, December 12, 2014
— Established VA CIO as a presidential appointee to establish parity with the VA CFO.



related assets” is not formally defined in 6008, but, by review of the formally defined terms therein (e.g. information technology, IT-related, IT Infrastructure, etc. in §5), the intent is clear that **CIO authority over all VA information technology is comprehensive and without exception**. Information technology classifications in 6008 (e.g. IT, non-IT, clinical, medical devices, facility equipment, construction, etc. in §2) apply to sources of funding only, and not CIO authority.

Select provisions from these policies relevant to development and implementation of the OIT Standards, and VA organizational authorities and responsibilities for various aspects of information technology and telecommunications, are provided in Attachment 3.

Office of Construction and Facilities Management

The Office of Construction and Facilities Management (CFM) is led by an Executive Director, a statutory, career-reserved appointee of the Secretary (SECVA) reporting directly to the Deputy Secretary (DEPSECVA). This position was created by the Veterans Benefits, Health Care, and Information Technology Act of 2006 (Pub. L. 109-461), and is “responsible for overseeing and managing the planning, design, construction, and operations of [VA facilities and infrastructure,] including major and minor construction projects”, and **has a specific responsibility for “determining architectural and engineering requirements...”**. The Facilities Standards Service, within CFM’s Office of Facilities Planning, is the primary executor of this specific responsibility, and does so through the publication of standards on CFM’s Technical Information Library (TIL).

OIT Standards

The OIT Standards are currently authorized under specific CIO responsibilities defined in VA Directive 6008 to:

- “Ensure all VA information resources...are compliant with enterprise...standards...” [3.a(3)(d)]
- “Provide visibility through VA’s enterprise architectures to all...standards...to guide VA IT item design, acquisition, development, and deployment.” [3.a(3)(e)]
- “Develop, maintain, and assure completeness and proper use of standard IT configurations.” [3.a(3)(f)]
- “Oversee and collaborate with VA stakeholders at the local level...” [§3.a(3)(h)]

The OIT IS precedes 6008. It was initially developed in 2007 in response to a national data center consolidation initiative. Further development, in preparation for VA obligations under the Federal Data Center Consolidation Initiative (FDCCI) initiated in February 2010⁸, culminated

⁸ Federal CIO Memorandum February 26, 2010

https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/federal_data_center_consolidation_initiative_02-26-2010.pdf



in v1.0 in 2012. In response to issuance of Directive 6008 in August 2016, significant revisions were initiated by EDICT and are ongoing. This period also saw the development of the OIT RT. OIT IS v2.2, formally issued April 10, 2019, is the latest version approved by OIT and available for VA use.

The OIT Standards are a special case in several respects:

- VA Enterprise Architecture baselines and standards typically establish approved uses and configuration of IT hardware, software, and other specific IT technologies or processes. In contrast, the OIT Standards provide criteria for space and other aspects of facilities design.
- OIT is the only VA business unit which develops, publishes, and maintains detailed facilities requirements independently of CFM. This unusual situation is created by the rapid pace of change of IT infrastructure technologies and best practices within VA and throughout the information technology and health sectors, and by natural overlaps in OIT and CFM authorities, responsibilities, and expertise.
- The OIT Standards are currently published in the Information Technology Operations and Services (ITOPS) [Baseline and Configuration Management](#) document repository and the [VA Technical Reference Model \(TRM\)](#), VA intranet sites with limited exposure to project stakeholders.

Despite the authority of OIT to develop and promulgate the OIT Standards, project personnel are accustomed to relying on the TIL standards, consistent with CFM's more specific authority over architectural and engineering requirements. Posting the OIT Standards on the TIL is an effort to increase their prominence and authority, promote project personnel awareness, and require utilization and EDICT participation from the earliest project planning stages. It is a stop-gap to address an urgent need pending a more comprehensive effort toward full TIL integration.

Looking Ahead

Future alerts are anticipated as updates are made to OIT Standards, TIL Standards, and VA policies. Known short- and medium-term issues include:

- OIT IS v3.0 is proceeding through OIT's approvals process, with planned publication in the second quarter of fiscal year 2020 (January-March).
- Post-v3.0 updates to the OIT Standards, annually or as changes in technology may warrant.
- Updates to VA policies to implement OMB Memorandum M-19-19, Update to Data Center Optimization Initiative (DCOI), 25 June 2019.
- Project to integrate the OIT Standards into the TIL standards.



Long-term issues include:

- Establish a program of regular updates to TIL information technology and telecommunications standards which are well-coordinated with OIT standards development.



Attachment 3

VA POLICY EXCERPTS: The below are select VA policy excerpts relevant to this Standards Alert and which define organizational authorities and responsibilities. Those planning and managing work which requires the OIT Standards, or otherwise have an information technology component, must thoroughly review and understand the complete policies, and the terms and definitions therein.

OIT

- Directive 6008
Acquisition and Management of VA Information Technology Resources
 - “As the statutorily accountable official for the management and security of all of VA’s information resources, including VA operational information and associated resources such as personnel, equipment, funds, and IT, VA’s Chief Information Officer (CIO) has authority over all information-related assets that are part of or interact with VA’s information networks, services, and capabilities.” [1.]
 - Section 2. Policy is entirely about funding such as which items/service fall into IT and non-IT buckets, and definition of specific cases (Direct Medical Systems, Equipment, or Devices (DMSED), Facility Equipment, Construction Projects, etc.). This is distinct from authority and responsibility, which are covered in Sections 1 and 3.
 - “The Assistant Secretary for Information and Technology, as the Department’s CIO, in planning, managing, and overseeing the VA’s information resources, shall:” [3.a]
 - “Design, develop, implement, and maintain a VA IT governance structure to:” [3.a(3)]
 - “Ensure all VA information resources, including those funded outside the IT appropriation, are compliant with enterprise policy, rules, standards, and guidance related to IT, information management (IM), and information security (IS).” [3.a(3)(d)]
 - Provide visibility through the VA’s enterprise architecture to all policy, rules, standards, guidance, and configurations necessary to guide VA IT item design, acquisition, development, and deployment.” [3.a(3)(e)]
 - “Develop, maintain, and assure completeness and proper use of standard IT configurations.” [3.a(3)(f)]



- “Oversee and collaborate with VA stakeholders at the local level to ensure that IT-related capabilities funded and deployed at local sites are appropriately vetted and formally (sentence incomplete, ends abruptly).” [3.a(3)(h)]
 - “Under Secretaries, Assistant Secretaries, and Other Key Officials will:” [3.b]
 - “Ensure all VA IT and non-IT items/services which connect to any VA Network are subject to rules, standards, and oversight processes as prescribed by the VA CIO in order to comply with information assurance, accessibility, security, privacy, and enterprise architecture standards.” [3.b(1)]
 - “Integrate compliance with this policy within establish decision processes in which they oversee or participate;” [3.b(2)]
- Directive 6051
Enterprise Architecture
 - “Enterprise architecture is a strategic information asset base, which defines the Department’s mission; the information and technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs. It includes a baseline architecture...” [2.a]
 - “All VA IT systems and investments must comply with the Department’s Enterprise Architecture (EA).” [2.b]
- Directive 6004
Configuration, Changes, and Release Management Programs
 - “The purpose of this Directive is to establish Department-wide Configuration, Change, and Release Management Programs in compliance with the Federal Information Security Management Act of 2002 (FISMA), 44 USC §3541-3549, and Pub. L. 107-347, Title III, and VA Directive and Handbook 6500, Information Security Program, to provide Configuration, Change, and Release Management processes...This directive applies to all VA related components and information technology resources, including contracted IT systems and services.” [1]
 - “Configuration, Change, and Release Management Programs will be implemented and maintained by [OIT]”. [2.a]
 - “...each VA system owner must document, implement, and maintain Configuration, Change, and Release Management plans and processes.” [2.b]
 - “[Document and maintain] the configuration baseline(s) applicable to the deployed system.” [2.b(1)]



Attachment 4

REFERENCES:

(Alphabetical by type, ascending; then chronological or document number, ascending)

The references below were instrumental toward developing this Standards Alert and establishing context.

Office of Construction and Facilities Management (CFM) — Technical Information Library (TIL) Standards

PG 18-5 Equipment Guide List – Chapter 232 – Office of Information & Technology (Aug 2016)

<https://www.cfm.va.gov/til/equip.asp>

PG 18 -9 Space Planning Criteria – Chapter 232 – Office of Information & Technology (Oct 2016)

<https://www.cfm.va.gov/til/space.asp>

PG 18-12 Design Guide – Office of Information & Technology (Feb 2011)

<https://www.cfm.va.gov/til/dguide.asp>

PG 18-10 Design Manual – Telecommunications and Special Telecommunications Systems (Feb 2016)

<https://www.cfm.va.gov/til/dManual.asp>

TIL Homepage

<https://www.cfm.va.gov/til/index.asp>

Office of Information and Technology (OIT) Standards

Design Guide Templates for Critical Telecommunications Spaces in Clinical and Non-clinical Environments v1.0 (27 Dec 2018)

<https://www.cfm.va.gov/til/dGuide/OIT-DGTemplates-CriticalTelecommSpaces.pdf>

Infrastructure Standards for Telecommunications Spaces v2.2 (19 Feb 2019)

<https://www.cfm.va.gov/til/dguide/OIT-InfrastrucStdsTelecommSpaces.pdf>



Office of Management and Budget (OMB) Memoranda

M-96-20 Implementation of the Information Technology Management Reform Act of 1996
(4 Apr 1996)

<https://www.whitehouse.gov/wp-content/uploads/2017/11/1996-M-96-20-Implementation-of-the-Information-Technology-Management-Reform-Act-of-1996.pdf>

M-97-02 Funding Information Systems Investments (25 Oct 1996)

<https://www.whitehouse.gov/wp-content/uploads/2017/11/1997-M-97-02-Funding-Information-Systems-Investments.pdf>

M-97-16 Information Technology Architecture

<https://www.whitehouse.gov/wp-content/uploads/2017/11/1997-M-97-16-Information-Technology-Architectures.pdf>

M-15-14 Information Technology Architectures (18 Jun 1997)

<https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2015/m-15-14.pdf>

Rescinded by M-17-26, Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda, issued June 15, 2017.

M-16-19 Data Center Optimization Initiative (DCOI)

https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m_16_19_1.pdf

M-19-19 Update to Data Center Optimization Initiative (DCOI) (25 Jun 2019)

<https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-19-Data-Centers.pdf>

Public Laws

Clinger-Cohen Act See Public Law 104-106 and Federal Acquisition Reform Act

104-106 National Defense Authorization for Fiscal Year 1996, Division E,
Information Technology Management Reform (Feb 1996)
aka
Information Technology Management Reform Act of 1996

<https://www.govinfo.gov/content/pkg/PLAW-104publ106/html/PLAW-104publ106.htm>



107-347 Federal Information Security Modernization Act of 2002 (FISMA2002)

<https://www.govinfo.gov/app/details/PLAW-107publ347/>

109-114 Military Quality of Life and Veterans Affairs Appropriations Act, 2006

<https://www.govinfo.gov/content/pkg/PLAW-109publ114/html/PLAW-109publ114.htm>

Establish the VA Information Technology Systems appropriation, into which IT resources from VHA, NA, and VBA were consolidated.

109-461 Veterans Benefits, Health Care, and Information Technology Improvement Act

<https://www.govinfo.gov/app/details/PLAW-109publ461>

113-283 Federal Information Security Modernization Act of 2014 (FISMA2014)

<https://www.govinfo.gov/app/details/PLAW-113publ283>

113-291 National Defense Authorization Act (FY2015) (NDAA2015)

<https://www.govinfo.gov/app/details/PLAW-113publ291/>

113-291 Title VIII, Subtitle D

Federal Information Technology Acquisition Reform [Act] (FITARA)

<https://www.govinfo.gov/app/details/PLAW-113publ291/>

VA Budget Requests and Congressional Hearings; GAO Reports; OIG Reports

While specific citations and excerpts are not provided herein, these publicly available records provided valuable background on the evolution of OIT authority and organization, from Public Law 104-106 to present.

VA Directives

6004 Configuration, Changes, and Release Management Programs (28 Sep 2009)

https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=891&FTYPE=2

6008 Acquisition and Management of VA Information Technology Resources (02 Nov 2017)

https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=891&FTYPE=2

6051 Department of Veterans Affairs (VA) Enterprise Architecture (08 Apr 2016)

https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=891&FTYPE=2



VA Electronic Health Records Modernization (EHRM) Policy

Cabling Infrastructure Memorandum (23 Sep 2019)

https://dvagov.sharepoint.com/sites/VACO.OEHRMoffice/Misc/SitePages/Construction_Admn.aspx

This is an access-controlled VA intranet site.



VA OIT Standards and Criteria

VA Engineering and all contractors will ensure that all construction projects at any VA facility adhere to the standards and criteria set forth in this document. OIT may deem any infrastructure that does not meet these requirements as unfit to support VA network services.

A. CABLE REQUIREMENTS

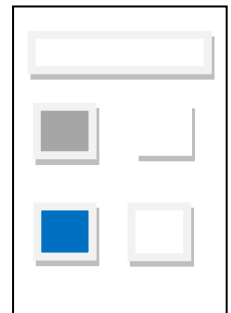
1. The cabling contractor shall be responsible for all parts and labor required to completely install and test the new cable infrastructure.
2. No cable shall terminate on equipment located in the interstitial at the Medical Center.
3. Fiber
 - a. Contractor is responsible for providing all closet connector housing units and required components to terminate fiber on both ends.
 - b. All fiber will be aqua OM4. The minimum pull shall be 24 strands.
 - c. Contractor will terminate at both ends with LC-LC connectors unless otherwise directed by a designated OIT representative.
 - d. At the primary Medical Center, all installations will be direct connections from the new IDF to the existing fiber rack in room BB102A.
 - e. At offsite locations, contractor must install fiber backbone linking all IDFs directly back to the ground floor primary IDF.
4. Voice feed cable
 - a. Quantity of CAT 3 cable pairs will be determined by an OIT representative prior to installation. A minimum of 50 telephone feed cable pairs will be pulled to the new IDF.
 - b. Installations in existing buildings located at the primary Medical Center
 - i. Cable must be terminated on 110 blocks at the MDF in room B167.
 - ii. Only interior gray cable shall be installed, no innerduct or exterior cable will be accepted.
 - iii. In new IDF, cable must be terminated on modular patch panels on the rack, one pair per jack. Pairs 24 and 25 will be a single two pair jack in position 24.
 - c. Installations in new buildings constructed on the primary Medical Center campus
 - i. Cable must be terminated on 110 blocks at the MDF in room B167.
 - ii. In the new building, terminate cable at ground floor IDF and branch cables evenly to all other IDFs.
 - iii. All cables run outside of a building must have gas tube protection at each end to protect it from the environmental elements.
 - d. Installations in buildings other than on the primary Medical Center campus
 - i. Contractor must provide minimum 25 pair CAT3 feed cable from the MPOE to the primary ground floor IDF.
 - ii. At MPOE end, feed cable must use terminations that match and are integrated into the network service provider (telco) provided existing cable environment.
 - iii. In MDF (ground floor primary IDF), feed cable must be terminated on eight position jacks in modular patch panels on the rack, one pair per jack on pins 4 and 5. Pairs 24 and 25 will be a single two pair jack. Pair 24 on pins 4 and 5, pair 25 on pins 3 and 6.
 - iv. In subsequent IDFs, feed cable must be terminated on eight position jacks in modular patch panels on the rack, one pair per jack on pins 4 and 5. Pairs 24 and 25 will be a single two pair jack. Pair 24 on pins 4 and 5, pair 25 on pins 3 and 6. Follow same scheme for any additional binder groups.

VA OIT Standards and Criteria

5. Workstation requirements
 - a. Copper cable runs must not exceed a distance of 100 meters (~328 feet).
 - b. Cable shall be CAT 6A, four pair, unshielded (UTP). Superior Essex or equivalent brand will be used unless otherwise specified by an OIT representative.
6. All cable runs shall follow the cable trays that are above the drop ceilings.
7. Cables shall not be attached to removable ceiling grid supports or laid directly on the ceiling grid. Cables shall not be attached to or supported by fire sprinkler heads, delivery systems or any environmental sensor in the ceiling air space.
8. All cable runs inside walls will be pulled by the contractor and shall be enclosed in Electrical Metallic Tubing (EMT) and single gang boxes.
9. The cabling contractor will be responsible for ensuring that the fire-rated structures (core walls) retain their existing fire-rating by installing proper sleeves and fire stops at all the accesses from the core area once the cabling effort has been completed.
10. All previously abandoned voice and/or data cable in the construction area shall be removed completely from end to end by the contractor once verified by VA OIT representative.

B. JACK CONFIGURATIONS

1. Data drops will be in a three jack configuration on a four port faceplate mounted on a single gang box or mud ring.
2. Wireless Access Point jacks must be a single port biscuit box.
3. Contractor will install VA OIT provided mounting hardware for all wall mount telephones.
4. All drops shall be wired to a T568a standard.
5. Only white, four gang, flush mount vertical classic series faceplates will be used.
6. Faceplates will be labeled in accordance with VA specifications
 - a. Numbering convention
 - i. Building number (where applicable)
 - ii. Floor, to include wing designation if applicable
 - iii. Panel
 - b. Jacks are to be labeled as: building – IDF – patch panel – jack port number. For example, in a typical 3 jack faceplate building 1, IDF room number B116, patch panel C, jack location 07 is to be identified as 1-B116-C-07. From this it will be assumed that the blue and white jacks are C-08 and C-09 respectively.
 - c. Prior to labeling, contractor shall obtain approval from OIT representative to ensure proposed numbering scheme meets OIT standards.
7. Contractor will terminate the workstation end with Panduit gray, blue, and white keystone jacks, and terminate the IDF end with the corresponding gray, blue, or white RJ45 port on the patch panel.
8. Each station will be tested and certified with full documentation provided to the VA representative.
9. Contractor will provide “as built” documentation identifying all jack locations and their associated labels.
10. There will be a minimum of one triple data drop location installed on every wall in all rooms regardless of the room designation or purpose.



VA OIT Standards and Criteria

C. WIRELESS NETWORKS

1. Areas with an existing wireless network
 - a. OIT is to be notified prior to the start of construction to allow for the removal of all wireless access points (WAPs).
 - b. VA Engineering or contractor must provide CAD drawings for OIT to design the wireless network a minimum of 90 days prior to cable installation.
 - c. Contractor will install new green CAT 6A cable to each WAP location and terminate on green jacks on the patch panel in the new IDF.
 - d. Contractor will install WAPs in locations designated by OIT representative.
2. Wireless network installation in new buildings
 - a. VA private wireless network
 - i. All new construction must include cabling for the VA wireless network using green CAT 6A cable.
 - ii. VA Engineering or contractor must provide CAD drawings for OIT to design the wireless network a minimum of 90 days prior to cable installation.
 - iii. OIT will provide the WAPs and associated hardware.
 - iv. Contractor will install WAPs in all locations identified on the predictive drawing provided by OIT.
 - v. Contractor should assume one WAP per approximately every 700sf.
 - vi. For locations greater than 12,000sf, VA OIT may elect to procure a separate contract for design and installation of the wireless network in conjunction with building construction. Contractor must confirm their wireless network responsibilities with VHA and OIT in projects of this size.
3. Guest (public) wireless network
 - a. New construction must also include cabling for the guest wireless network separate from the VA network.
 - b. OIT has no involvement with or responsibility for the public network. All cabling, hardware, network equipment, and transport circuits are to be provided by VA Engineering, Healthcare Technology Management (HTM), or their designated contractor.
 - c. All components of the guest network are required to reside outside of OIT rooms.

D. ELECTRICAL REQUIREMENTS

1. The cabling contractor is responsible for grounding and bonding the entire infrastructure provided in the project.
 - a. Use #6 grounding conductors and two-hole irreversible compression connectors to bond racks to the room's telecommunications grounding bus-bar (TGB).
 - b. The contractor shall provide and install the proper grounding kits for the voice terminations and patch panels as required by manufacturer.
 - c. The contractor shall ground and bond the telecommunications rack.
 - d. Contractor is also responsible to ensure grounding bus bar is properly grounded per NEC section 606.
2. A dedicated 120VAC 20A circuit equipped with NEMA 5-20R receptacle shall be mounted directly above each rack. The two 120V 20A circuits will have a dedicated uninterruptible power supply (UPS) plugged into the receptacles. The equipment rack will require two 6' multiple outlet power strips mounted at the back of the rack. Each individual power strip will be plugged into a separate UPS.
3. Each receptacle must be powered by a separate electrical panel.

VA OIT Standards and Criteria

4. A minimum of one electrical receptacle connected to E-power in all locations within the Medical Center campus or where otherwise available is required.
5. The National Electrical Code (NEC) will be adhered to for all installations in addition to any site-specific requirements.

E. DATA CLOSETS

1. Contractor will extend the telco circuit to the MDF or IDF as applicable.
2. Physical Requirements
 - a. IT closets shall house nothing other than IT equipment. Nurse call, panic alarms, access controls, CCTV and similar systems must not reside in IT closets.
 - b. Space must be a minimum of 120 sq. ft.
 - c. The IT closet is required to be enclosed with a hard lid ceiling.
 - d. Doors need to be fire rated in accordance with specifications required by VA Engineering management.
 - e. The closet requires a dedicated Environmental Control Unit (air conditioning) not part of the facility system.
 - f. In addition to the quantity of 4-inch conduit stubs contractor requires to terminate all cables in the IDF, two empty 4-inch conduit stubs must be made available for future expansion.
 - g. Conduits shall lead to the nearest accessible drop ceiling location, preferably in a hallway.
 - h. Contractor shall install an 8ft, ¾" fire rated plywood backboard on one wall in IDF. Board must be painted but allow for fire rating labels to be visible.
 - i. Data and phone closets are to be cleaned of all dust and debris from racks, walls, and floor.
3. Racks
 - a. Two 45U 7' x 19" two-post racks will be provided and installed by the contractor
 - b. Minimum three feet of clearance is required on all sides of racks, also accounting for the 26" depth of the UPS.
 - c. Cable managers will be provided by the contractor
 - i. Vertical cable management will be provided on both ends of each rack (including between racks) from the floor to top of rack.
 - ii. Racks shall be separated only by vertical cable managers.
 - iii. 2U dual sided horizontal cable managers (Panduit WMP1E) will be placed between each patch panel with a corresponding number of managers provided, but not installed, for the opposite rack (12 total).
 - d. Cable management will include ladder racks above the racks and on both sides of racks, extending to the wall where cables enter the closet.
 - e. Racks must be securely mounted to the floor.
4. Patch Panels
 - a. Fiber panel must be mounted in the highest position on the left rack .
 - b. A modular patch panel for CAT 3 copper feed cable termination will be installed directly under the fiber panel, separated only by a 2U horizontal cable manager.
 - c. Contractor will provide and install a minimum of six 48-port patch panels in the right rack.



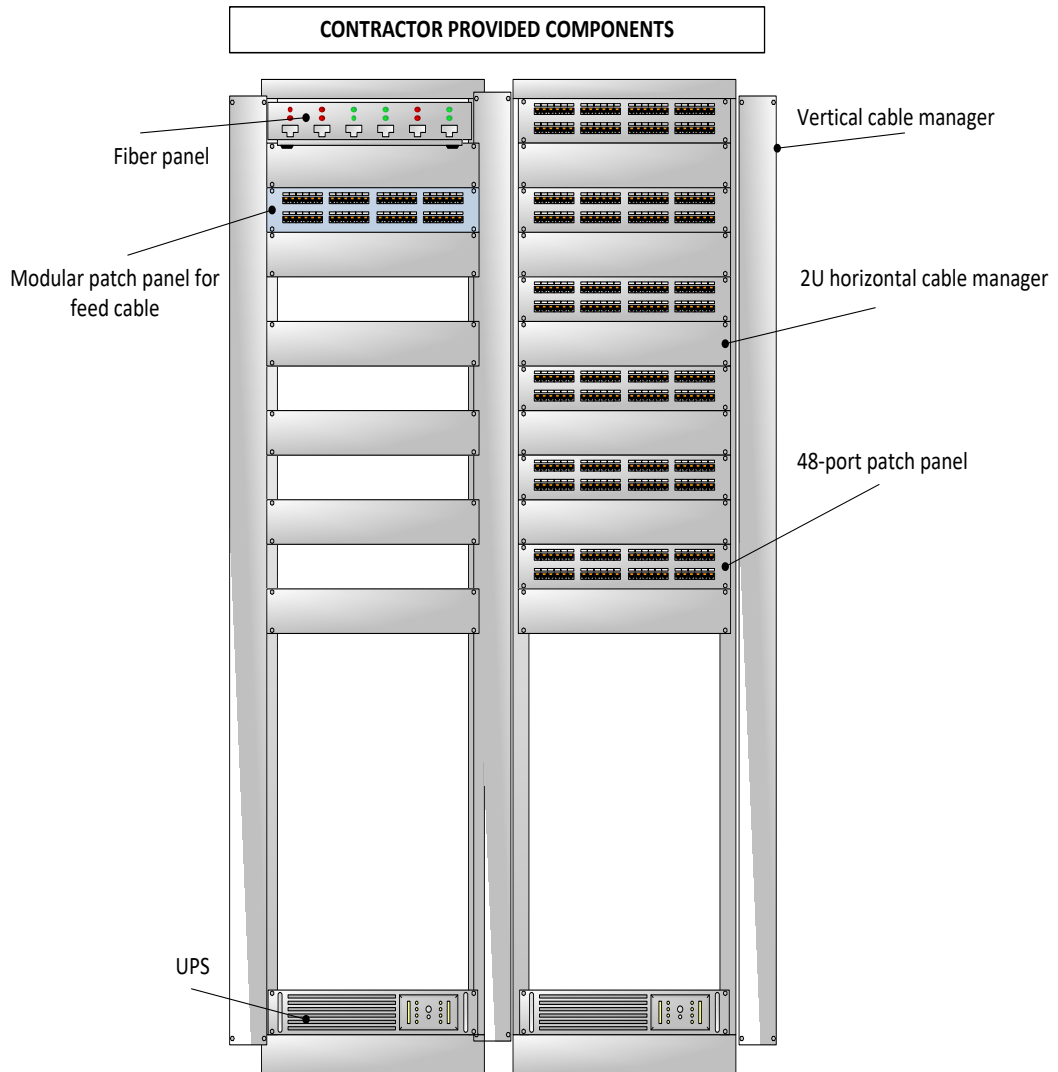
VA OIT Standards and Criteria

- d. Patch panels shall be labeled alphabetically in sequential order from the top position down, starting with "A."
 - e. Jacks on the patch panels do not need to be individually labeled, provided they follow the three jack sequence numbering scheme stated above (B.4.b) and correspond to the faceplates in which they are connected.
 - f. Single cable drops (wall phones or POTS lines, etc.) should be terminated at the bottom of the last panel, so as to not disrupt the three jack consecutive numbering scheme.
 - g. Standard rack layout depicting contractor responsibilities is diagramed below.
5. UPS
- a. Two uninterruptible power supply (UPS) units will be provided by and installed in each IT closet by the contractor.
 - b. One UPS will be installed in each rack.
 - c. UPS must be in the bottom position of the rack.
 - d. The model to be installed will be a rack mountable APC SMART-UPS X 2200VA LCD 100-127V with NIC (model SMT2200RM2UC) or equivalent.
 - e. UPS must also include the compatible network management card (model AP9630).

F. VA (NON-IT) PROVIDED SYSTEMS

1. A scramble pad compatible with the existing VA access control system must be installed on all IT closet doors.
2. A security camera monitored by VA Police must be placed in the vicinity of the IT closet to record video footage of all who enter and exit the room.
3. Wireless temperature sensor will be installed as part of the existing VA Engineering monitoring system.

VA OIT Standards and Criteria



SOCAMES 6 Design Alert 1

Problem

During a recent construction activity of cable upgrades to an existing telecommunication room (TR) at an Initial Operating Capability (IOC) site, it was discovered during cable testing procedures that some of the cables being upgraded were greater in length to the end user device than standards allows.

Background

ANSI/TIA-568.D, "Balanced Twisted-Pair Telecommunications Cabling and Components" (Sep 2018) version of industry standards for telecommunication room fixed cabling installation, limits the total length of a network Unshielded Twisted Pair (UTP) cable segment to 100 meters. The 100 meters is broken down as 10 meters for patch cables and 90 meters for total fixed cabling. Cable length requires a three-dimensional assessment to ensure that the fixed cables being installed do not exceed the specified UTP cable segment of 90 meters of fixed cable length.

There are several scenarios that require an assessment to occur to ensure that a telecommunication rooms UTP cable segments do not exceed 90 meters.

Scenario 1: The installation of a new telecommunication room to serve an area.

Scenario 2: The relocation of an existing telecommunication room to serve an area.

Scenario 3: The installation of new cabling upgrades in a telecommunication room that will remain in place to serve an area.

Scenario 4: An existing telecommunication room that will not receive any cabling upgrades.

Solution

To ensure that an assessment is performed for each of the four telecommunication room scenarios listed above, our office in conjunction with the SD-DCIE team is providing a recommended three-dimensional estimation approach that can be shared with your respective facility leads and design team to verify all telecommunication rooms do not exceed the specified UTP cable segment of 90 meters.

Step 1: Ensure you have an accurate floor plan that depicts the locations of the telecommunication rooms serving the facility.

Step 2: Utilizing AutoCAD or rule, center on the location of the telecommunication room being assessed. From the center of the room project out lines, 80 meters in length from that point, in the plan north, south, east and west respectively.

Step 3: At the end each of the 80 meters lines created, connect a line 45 degrees from that point out to the next end point creating a diamond.

Step 4: Validate that all areas served by that telecommunication room fall within the parameters of the diamond overlay.

Step 5: If the area served by that telecommunication room is within the diamond overlay then the distance, as provided by the estimation tool, is adequate for that telecommunication room.

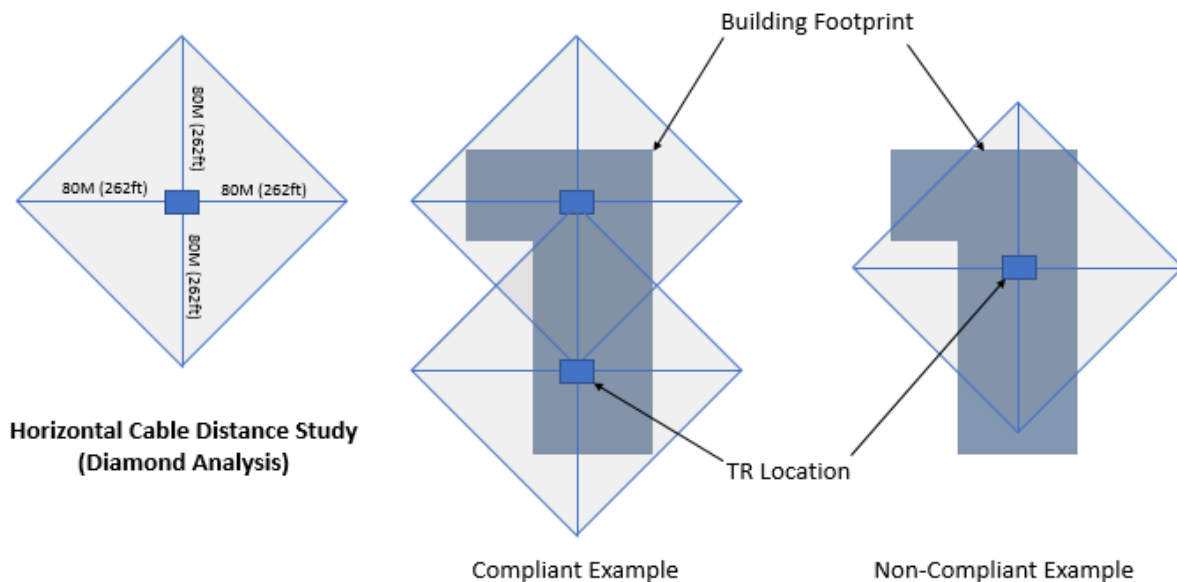
Step 6: If the area served by that telecommunication room is outside the diamond overlay then the distance, as provided by the estimation tool, is inadequate for that telecommunication room and further investigation is required by electronically testing the cable lengths to see if they pass or physical measurement. Any UTP cabling that does not pass testing protocols and is too long will need to have further design considerations to remedy the distance issue.

Notes

Since it is necessary to account for vertical cable distance, installation of slack for bypassing obstructions, cable management, bend radii and other in-situ obstacles 80 meters is utilized instead of the 90 meters acceptable length. This is to provide a realistic estimation of coverage of the representative telecommunication room.

This estimation tool is a recommended approach to validate fixed cable lengths meet the standards. Designers and installers remain responsible for ensuring actual cable distances do not exceed the limits in the standards.

Below is a diagram of an example demonstrating the use of the estimation tool.



SECURITY REQUIREMENTS - FACILITY SECURITY LEVEL II

THESE PARAGRAPHS CONTAIN ADDITIONAL SECURITY REQUIREMENTS, AND, UNLESS INDICATED OTHERWISE, ARE TO BE PRICED AS PART OF THE BUILDING SPECIFIC AMORTIZED CAPITAL (BSAC). WHERE THEY ARE IN CONFLICT WITH ANY OTHER REQUIREMENTS ON THIS LEASE, THE STRICTEST SHALL APPLY.

DEFINITIONS:

CRITICAL AREAS - The areas that house systems that if damaged or compromised could have significant adverse consequences for the facility, operation of the facility, or mission of the agency or its occupants and visitors. These areas may also be referred to as “limited access areas,” “restricted areas,” or “exclusionary zones.” Critical areas do not necessarily have to be within Government-controlled space (e.g., generators, air handlers, electrical feeds which could be located outside Government-controlled space).

SENSITIVE AREAS – Sensitive areas include vaults, SCIFs, evidence rooms, war rooms, and sensitive documents areas. Sensitive areas are primarily housed within Government-controlled space.

FACILITY ENTRANCES, LOBBY, COMMON AREAS, NON-PUBLIC, AND UTILITY AREAS.

FACILITY ENTRANCES AND LOBBY

EMPLOYEE ACCESS CONTROL AT ENTRANCES (SHELL)

The Lessor shall provide key or electronic access control for the entrance to this building. All Government employees, under this lease, shall be allowed access to the leased space (including after-hours access).

COMMON AREAS, NON-PUBLIC, AND UTILITY AREAS.

PUBLIC RESTROOM ACCESS (SHELL)

The Government reserves the right to control access to public restrooms located within the Space.

SECURING CRITICAL AREAS (SHELL)

The Lessor shall secure areas designated as Critical Areas to restrict access:

- A. Keyed locks, keycards, or similar security measures shall strictly control access to mechanical areas. Additional controls for access to keys, keycards, and key codes shall be strictly maintained. The Lessor shall develop and maintain accurate HVAC diagrams and HVAC system labeling within mechanical areas.

LESSOR: _____ GOVERNMENT: _____

- B. Roofs with HVAC systems shall also be secured. Fencing or other barriers may be required to restrict access from adjacent roofs based on a Government Building Security Assessment. Roof access shall be strictly controlled through keyed locks, keycards, or similar measures. Fire and life safety egress shall be carefully reviewed when restricting roof access.
- C. At a minimum, Lessor shall secure building common areas including sprinkler rooms, electrical closets, telecommunications rooms.

VISITOR ACCESS CONTROL (SHELL)

Entrances are open to the public during business hours. After hours, visitor entrances are secured, and have a means to verify the identity of persons requesting access prior to allowing entry into the Space.

INTERIOR (GOVERNMENT SPACE)

DESIGNATED ENTRANCES (SHELL)

The Government shall have a designated main entrance.

IDENTITY VERIFICATION (SHELL)

The Government reserves the right to verify the identity of persons requesting access to the Space prior to allowing entry.

FORMAL KEY CONTROL PROGRAM (SHELL)

The Government reserves the right to implement a formal key control program. The Lessor shall have a means of allowing the electronic disabling of lost or stolen access media, if electronic media is used.

SITES AND EXTERIOR OF THE BUILDING

SIGNAGE

POSTING OF SIGNAGE IDENTIFYING THE SPACE AS GOVERNMENTAL (SHELL)

The Lessor shall not post sign(s) or otherwise identify the facility and parking areas as a Government, or specific Government tenant, occupied facility, including during construction, without written Government approval.

POSTING OF REGULATORY SIGNAGE (SHELL)

The Government may post or request the Lessor to post regulatory, statutory, sensitive areas and site specific signage.

LANDSCAPING

LANDSCAPING REQUIREMENTS (SHELL)

Lessor shall maintain landscaping (trees, bushes, hedges, land contour, etc.) around the facility. Landscaping shall be neatly trimmed in order to minimize the opportunity for concealment of individuals and packages/containers. Landscaping shall not obstruct the views of security guards and CCTV cameras, or interfere with lighting or IDS equipment.

CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN (SHELL)

The Lessor shall separate from public access, restricted areas as designated by the Government, through the application of Crime Prevention Through Environmental Design (CPTED) principles by using trees, hedges, berms, or a combination of these or similar features, and by fences, walls, gates and other barriers, where feasible and acceptable to the Government.

HAZMAT STORAGE

If there is HAZMAT storage, Lessor shall locate it in a restricted area or storage container away from loading docks, entrances, and uncontrolled parking.

PLACEMENT OF RECEPTACLES, CONTAINERS, AND MAILBOXES

Trash receptacles, containers, mailboxes, vending machines, or other fixtures and/or features that could conceal packages, brief cases, or other portable containers shall be located 10 feet away from building.

SECURITY SYSTEMS

CLOSED CIRCUIT TELEVISION SYSTEM (CCTV)

LESSOR PROVIDED DESIGN, INSTALLATION, AND MAINTENANCE

The lessor shall design, install, and maintain a Closed Circuit Television (CCTV) system as described in this section. The CCTV system will support the entry control system (at entrances and exits to the space), with time lapse video recording, that will allow Government employees to view and communicate remotely with visitors before allowing access to the Space. As determined by the Government the CCTV system shall provide unobstructed coverage of designated pedestrian entrances and exits. Technical review of the proposed system shall be coordinated with the Government security representative, at the direction of the Contracting Officer, prior to installation. CCTV system testing and acceptance shall be conducted by the Government prior to occupancy. The CCTV system shall comply with the Architectural Barriers Act, section F230.0. The Government will centrally monitor the CCTV system. Government specifications are available from the Lease Contracting Officer. CCTV system components which fail or require maintenance or which fail during testing should be serviced in accordance with the Security System Maintenance Criteria listed below.

Security System Maintenance Criteria: The Lessor, in consultation and coordination with a security provider, either internal or external, as determined by the Lease Contracting Officer, and the Government security representative, shall implement a preventive maintenance program for all security systems the

LESSOR: _____ GOVERNMENT:

Lessor has installed. Any critical component that becomes inoperable must be replaced or repaired by the Lessor within 5 business days. Critical components are those required to provide security (IDS, CCTV, access control, etc.) for a perimeter access point or critical area. "Replacement" may include implementing other temporary measures in instances where the replacement or repair is not achievable within the specified time frame (e.g. a temporary barrier to replace an inoperable pop-up vehicle barrier, etc.). Failure by the Lessor to provide sufficient replacement measures within the timeframe identified above may result in the Government's providing guard service, the cost of which must be reimbursed by the Lessor.

GOVERNMENT PROVIDED PRODUCT, INSTALLATION, AND MAINTENANCE

The Government shall provide and install an entry control system, with time lapse video recording, that will allow Government employees to view and communicate remotely with visitors before allowing access. This Closed Circuit Television (CCTV) system shall provide the Government with unobstructed coverage, as determined by the Government, of designated pedestrian entrances and exits. The Lessor shall permit twenty-four hour CCTV coverage and recording, provided and operated by the Government. The Government will centrally monitor the CCTV surveillance. Government specifications are available from the Contracting Officer. The Lessor shall post necessary regulatory, statutory, and/or site specific signage, as determined by the Government.

The Lessor, at the notice to proceed stage of the procurement, shall advise the Government of the appropriate time to install the equipment during the construction of the Space. The Lessor shall facilitate the installation by allowing access to electrical panels and other areas of the building as necessary.

INTRUSION DETECTION SYSTEM (IDS)

LESSOR PROVIDED DESIGN, INSTALLATION, AND MAINTENANCE

The Lessor shall design, install, and maintain an Intrusion Detection System (IDS) as described in this section. The Government requires an IDS, which will cover perimeter entry and exit doors, and operable ground-floor windows. Basic Security-in-Depth IDS components include: magnetic door switch(s), alarm system keypad, passive infrared sensor(s) (PIR), an alarm panel (to designated monitoring center) and appropriate communication method i.e. telephone and/or Internet connection, glass-break detector, magnetic window switches or shock sensors. Technical review of the proposed system shall be coordinated with the Government security representative, at the direction of the Lease Contracting Officer, prior to installation. System testing and acceptance shall be conducted by the Government prior to occupancy.

Basic Security-in-Depth IDS shall be connected to and monitored at a central station operated by the Department of Homeland Security Megacenters. Emergency notification lists shall be coordinated with the monitoring station to include all applicable Government and lessor points of contact. Monitoring shall be designed to facilitate a real-time detection of an incident, and to coordinate an active response to an incident. The Lessor must complete the Megacenters Alarm Requirements (MAR) application process specified by the Government to meet the monitoring requirements for a functional IDS. Components which fail or require maintenance, or which fail during testing shall be serviced in accordance with the Security System Maintenance Criteria listed below.

LESSOR: _____ GOVERNMENT:

Security System Maintenance Criteria: The Lessor, in consultation and coordination with a security provider, either internal or external, as determined by the Lease Contracting Officer, and the Government security representative, shall implement a preventive maintenance program for all security systems the Lessor has installed. Any critical component that becomes inoperable must be replaced or repaired by the Lessor within 5 business days. Critical components are those required to provide security (IDS, CCTV, access control, etc.) for a perimeter access point or critical area. "Replacement" may include implementing other temporary measures in instances where the replacement or repair is not achievable within the specified time frame (e.g. a temporary barrier to replace an inoperable pop-up vehicle barrier, etc.). Failure by the Lessor to provide sufficient replacement measures within the timeframe identified above may result in the Government's providing guard service, the cost of which must be reimbursed by the Lessor.

GOVERNMENT PROVIDED SCOPE AND PRODUCT, INSTALLATION, AND MAINTENANCE The Lessor shall permit installation of a perimeter Intrusion Detection System (IDS) to be operated by the Government. The Government shall provide and install an IDS on perimeter entry and exit doors, and operable ground-floor windows. Basic Security-in-Depth IDS— include: magnetic door switch(s), alarm system keypad, passive infrared sensor(s) (PIR), an alarm panel (to designated monitoring center) and appropriate communication method i.e. telephone and/or Internet connection, glass-break detector, magnetic window switches or shock sensors.

Basic Security-in-Depth IDS shall be connected and monitored at a central station. Emergency notification lists shall be coordinated with the monitoring station to include all applicable Government and Lessor points of contact. Monitoring shall be designed to facilitate a real-time detection of an incident, and to coordinate an active response to an incident.

The Lessor, at the notice to proceed stage of the procurement, shall advise the Government of the appropriate time to install the equipment during the construction of the Space. The Lessor shall facilitate the installation by allowing access to electrical panels and other areas of the building, as necessary.

DURESS ALARM

LESSOR PROVIDED DESIGN, INSTALLATION, AND MAINTENANCE

The Lessor shall design, install, and maintain a duress alarm system as described. Technical review shall be coordinated with the Government security representative, at the direction of the Contracting Officer, prior to installation. System testing and acceptance shall be conducted by the Government prior to occupancy. This system shall comply with the Architectural Barriers Act, section F230.0.

The Lessor in consultation and coordination with the security provider and Government shall conduct security system performance testing annually. Testing must be based on established, consistent agency-specific protocols, documented and furnished to the Contracting Officer. Components which fail or require maintenance or which fail during testing should be serviced in accordance with the Security System Maintenance Criteria listed below.

Security System Maintenance Criteria: The Lessor in consultation and coordination with a security provider, either internal or external, as determined by the Lease Contracting Officer, and the Government

security representative shall implement a preventive maintenance program for all security systems they have installed. Any critical component that becomes inoperable must be replaced or repaired within 5 business days. Critical components are those required to provide security (IDS, CCTV, access control, etc.) for a perimeter access point or critical area. "Replacement" may include implementing other temporary measures in instances where the replacement or repair is not achievable within the specified time frame (e.g. a temporary barrier to replace an inoperable pop-up vehicle barrier, etc.). Failure by the Lessor to provide sufficient replacement measures within the timeframe identified above may result in the Government's providing guard service, the cost of which must be reimbursed by the Lessor.

GOVERNMENT PROVIDED SCOPE, PRODUCT, INSTALLATION, AND MAINTENANCE

The Lessor shall permit installation of a duress alarm system to be provided and operated by the Government. The Government, in coordination with a security provider, either internal or external, as determined by the Contracting Officer, shall document and implement duress procedures for emergency situations.

The Lessor, at the notice to proceed stage of the procurement, shall advise the Government of the appropriate time to install the equipment during the construction of the Space and shall facilitate the installation, including access to electrical panels and other areas of the building, as necessary.

STRUCTURE

WINDOWS

No countermeasures are required for baseline standard.

OPERATIONS AND ADMINISTRATION

LESSOR TO WORK WITH FACILITY SECURITY COMMITTEE (FSC) (SHELL)

The Lessor shall cooperate and work with the buildings Facility Security Committee (FSC) throughout the term of the lease.

ACCESS TO BUILDING INFORMATION (SHELL)

Building Information—including mechanical, electrical, vertical transport, fire and life safety, security system plans and schematics, computer automation systems, and emergency operations procedures—shall be strictly controlled. Such information shall be released to authorized personnel only, approved by the Government, by the development of an access list and controlled copy numbering. The Contracting Officer may direct that the names and locations of -Government tenants not be disclosed in any publicly accessed document or record. If that is the case, the Government may request that such information not be posted in the building directory.

Lessor shall have emergency plans and associated documents readily available in the event of an emergency.

CYBERSECURITY (SHELL)

- A. Lessors are prohibited from connecting any portion of their building and access control systems (BACS) to any federally-owned or operated IT network. BACS include systems providing fire and life safety control, physical access control, building power and energy control, electronic surveillance, and automated HVAC, elevator, or building monitoring and control services (including IP addressable devices, application servers, or network switches).
- B. In the event of a cybersecurity incident related to BACS, the Lessor shall initially assess the cyber incident, identify the impacts and risks to the Building and its occupants, and follow their organization's cyber and IT procedures and protocols related to containing and handling a cybersecurity incident. In addition, the Lessor shall immediately inform the Lease Contracting Officer's (LCO's) designated representative, i.e., the Lease Administration Manager (LAM), about cybersecurity incidents that impact a federal tenant's safety, security, or proper functioning.
- C. Lessors are encouraged to put into place the following cyber protection measures in order to safeguard facilities and occupants:
1. Engineer and install BACS to comply with the Department of Homeland Security Industrial Control Systems Computer Emergency Response Team (DHS ICS-CERT) cyber security guidance and recommendations (<https://ics-cert.us-cert.gov/Recommended-Practices>).
 2. Refer to the National Institute of Standards and Technology Cyber Security Framework (NIST-CSF) (<https://www.nist.gov/cyberframework>) and cybersecurity guidance in the DHS Commercial Facilities Sector-Specific Plan (<https://www.dhs.gov/publication/nipp-ssp-commercial-facilities-2015>) for best practices to manage cyber risks.
 3. Encourage vendors of BACS to secure these devices and software through the following:
 - a. Develop and Institute a proper Configuration Management Plan for the BACS devices and applications, so that the system can be supported.
 - b. Safeguard sensitive data and/or login credentials through the use of strong encryption on devices and applications. This means using NIST- approved encryption algorithms, secure protocols (i.e., Transport Layer Security (TLS) 1.1, TLS 1.2, TLS 1.3) and Federal Information Processing Standard (FIPS) 140-2 validated modules.
 - c. Disable unnecessary services in order to protect the system from unnecessary access and a potential exposure point by a malicious attacker. Examples include File Transfer Protocol-FTP (a protocol used for transferring files to a remote location) and Telnet (allowing a user to issue commands remotely). Additionally, use of protocols that transmit data in the clear (such as default ZigBee) should be avoided, in favor of protocols that are encrypted.
 - d. Close unnecessary open ports to secure against unprivileged access.
 - e. Monitor and free web applications and supporting servers of common vulnerabilities in web applications, such as those identified by the (Open Web Application Security Project (OWASP) Top 10 Project (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)).

- f. Enforce Least Privilege, where proper permissions are enforced on a device or application so that a malicious attacker cannot gain access to all data. Enforcing Least Privilege will only allow users to access data they are allowed to see. Additional information can be found at <https://www.beyondtrust.com/blog/what-is-least-privilege/>
- g. Protect against Insufficient User Access Auditing, where device or application does not have a mechanism to log/track activity by user. Enforce changing of factory default Username and Password to prevent unauthorized entry into the BACS system.
- h. Use updated antivirus software subscription at all times. Kaspersky-branded products or services, prohibited from use by the Federal Government, are not to be utilized.
- i. Conduct antivirus and spyware scans on a regular basis. Patching for workstations and server Operating System (OS), as well as vulnerability patching should follow standard industry best practices for software development life cycle (SDLC).
- j. Discontinue the use of end of life (EOL) systems and use only applications/systems that are supported by the manufacturer.
- k. Operating Systems must be supported by the vendor for security updates (e.g., do not use Windows Server 2003).
- l. Proposed standard installation, operation, maintenance, updates, and/or patching of software shall not alter the configuration settings from the approved United States Government Configuration Baseline (USGCB) or tenant agency guidance (if applicable).
- m. Disallow the use of commercially-provided circuits to manage building systems and install building systems on a protected network, safeguarded by the enterprise firewalls in place. Workstations or servers running building monitor and control systems are not connected and visible on the public internet.
- n. Systems should have proper system configuration hardening and align with Center for Internet Security ([CIS](https://www.cisecurity.org/cis-benchmarks/)) benchmarks or other industry recognized benchmarks. Additional information can be found at <https://www.cisecurity.org/cis-benchmarks/>.

Date: **FEB 26 2018**

From: Acting Principal Executive Director, Office of Acquisition, Logistics, and Construction (003)
Assistant Secretary for Office of Operations, Security, and Preparedness (007)

Subj: Real Property Policy Memorandum 2018-02 Physical Security Standards for Leased Facilities
(Existing Space and Lease Construction Projects) (VAIQ 7866496)

To: Office of Real Property (003C1E)
Veterans Integrated Service Network Directors
Department of Veterans Affairs Lease Contracting Officers
Department of Veterans Affairs Leasing Officials

1. As the Department of Veterans Affairs (VA) leasing program has developed and increased in complexity in recent years, the Office of Acquisition, Logistics, and Construction and the Office of Operations, Security, and Preparedness (OSP) now need to officially differentiate between the standards, processes, and policies applicable to owned VA facilities versus leased facilities. VA has engaged in extensive discussions with the Congressional Budget Office, Office of Management and Budget, and the General Services Administration as to the best way for VA to move forward with its leasing program while ensuring compliance with applicable statutes and budgetary treatment requirements. These discussions resulted in a mandate from Congress and the Administration that VA re-examine how it conducts its leasing program and implement changes to bring it into better alignment with Federal requirements and similar programs at other Federal Departments.

2. In furtherance of these efforts, we are hereby implementing the following policies:

a. In response to the Government Accountability Office Report "VA Facility Security" dated January 2018, VA adopts all elements of the Interagency Security Standards (ISC) for its leased facilities. Resiliency requirements will be implemented via the most current version of the National Fire Protection Association 99: Health Care Facilities Code, structural provisions of local building codes, and directions incorporated in the Agency Specific Requirements (ASR) for each leased facility.

b. All leased facilities will, at a minimum, be designated Facility Security Level (FSL) II. Detailed FSL information will be incorporated in the ASR for each leased facility.

c. The Director of the parent VA Medical Center and/or the VISN Network Director may add physical security requirements beyond those listed in the attachment to this Memorandum. However, any such requested additional physical security requirements must be analyzed through an ISC-compliant risk assessment and approved by the Office of Security and Law Enforcement and the Deputy Under Secretary for Health for Operations

Subject: Real Property Policy Memorandum 2018-02 Physical Security Standards for Leased Facilities (Existing Space and Lease Construction Projects) (VAIQ 7866496)

and Management. Requested additional physical security requirements must also be priced as tenant improvements and paid in lump sum to prevent exceeding prospectus rental rates and/or qualifying the lease as a capital asset pursuant to budgetary treatment requirements of the Office of Management and Budget's Circular A-11.

d. For leased facilities in procurement or under construction as of the date of this Memorandum, the Lease Contracting Officer, working in concert with the project team, may change the lease requirements to align with those described in this Memorandum when it is in the best interest of the Government. In the event this change conflicts with a requirement included within the prospectus, such changes will be routed to the Deputy Under Secretary for Health for Operations and Management for approval.

3. In an effort to comply with the ISC, decrease project delivery times, increase competition, and lower delivery costs, VA leasing projects are no longer required to conform to:

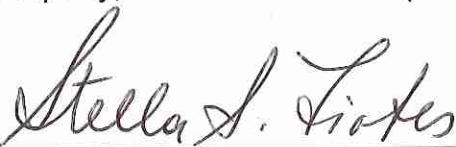
a. Physical Security Design Manual for VA Life-Safety Protected Facilities (<https://www.cfm.va.gov/til/PhysicalSecurity/dmPhySecLS.pdf>);

b. Physical Security Design Manual for VA Mission Critical Facilities (<https://www.cfm.va.gov/til/PhysicalSecurity/dmPhySecMC-2007.pdf>); and

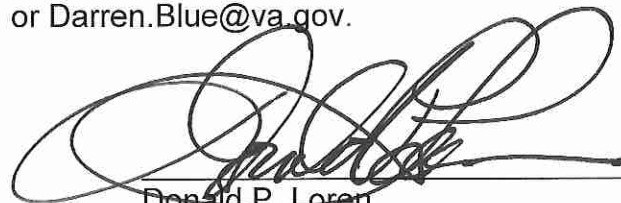
c. Appendix B, Physical Security Requirements and Options, VA Handbook 0730 (See VA Publications <https://www.va.gov/vapubs/index.cfm>).

4. The policies and information contained in this Memorandum supersede any other published guidance on these topics. In collaboration with VA Administrations, including OSP, the Office of Construction and Facilities Management is responsible for the development of any further definition or process to support these policies, which remain in effect until rescinded.

5. If you have any questions, please contact the Associate Executive Director, Office of Real Property, Mr. Darren Blue at (202) 632-4641 or Darren.Blue@va.gov.



Stella S. Fiotes, AIA
Acting Principal Executive Director
Office of Acquisition, Logistics, and
Construction



Donald P. Loren
Assistant Secretary for Operations,
Security, and Preparedness

Attachment: Facility Security Level II Standards

ATTACHMENT

INSTRUCTIONS TO LEASING SPECIALISTS: THE FOLLOWING BASELINE SPECIFICATIONS REPRESENT THE FULL EXTENT OF SECURITY SPECIFICATIONS AVAILABLE TO LEVEL II REQUIREMENTS UNDER THE ISC.

THESE ARE THE MINIMUM BASELINE REQUIREMENTS (MANDATORY). THE LCO MAY INCLUDE ADDITIONAL REQUIREMENTS, IF REQUESTED BY THE VA MEDICAL CENTER DIRECTOR IN WRITING. ADDITIONAL REQUIREMENTS MUST BE IDENTIFIED THROUGH PROGRAMMATIC OR RISK BASED ASSESSMENT BY THE VA CHIEF OF POLICE OR THEIR DESIGNEE. ANY ADDITIONAL REQUIREMENTS NOT SUPPORTED BY RISK ASSESSMENT MAYBE INCLUDED, BUT MUST BE FUNDED AS TENANT SPECIFIC SECURITY (TIS) AND NOT AS BSAC.

SECURITY REQUIREMENTS - FACILITY SECURITY LEVEL II

THESE PARAGRAPHS CONTAIN ADDITIONAL SECURITY REQUIREMENTS, AND, UNLESS INDICATED OTHERWISE, ARE TO BE PRICED AS PART OF THE BUILDING SPECIFIC AMORTIZED CAPITAL (BSAC). WHERE THEY ARE IN CONFLICT WITH ANY OTHER REQUIREMENTS ON THIS LEASE, THE STRICTEST SHALL APPLY.

DEFINITIONS:

CRITICAL AREAS - The areas that house systems that if damaged or compromised could have significant adverse consequences for the facility, operation of the facility, or mission of the agency or its occupants and visitors. These areas may also be referred to as "limited access areas," "restricted areas," or "exclusionary zones." Critical areas do not necessarily have to be within Government-controlled space (e.g., generators, air handlers, electrical feeds which could be located outside Government-controlled space).

SENSITIVE AREAS - Sensitive areas include vaults, pharmacy, SCIFs, evidence rooms, war rooms, and sensitive documents areas. Sensitive areas are primarily housed within Government-controlled space.

FACILITY ENTRANCES, LOBBY, COMMON AREAS, NON-PUBLIC, AND UTILITY AREAS.

FACILITY ENTRANCES AND LOBBY

EMPLOYEE ACCESS CONTROL AT ENTRANCES (SHELL)

The Lessor shall provide key or electronic access control for the entrance to this building. All Government employees, under this, shall be allowed access to the leased space (including after-hours access).

COMMON AREAS, NON-PUBLIC, AND UTILITY AREAS.

PUBLIC RESTROOM ACCESS (SHELL)

The Government reserves the right to control access to public restrooms located within the Space.

ACTION REQUIRED. INSERT OTHER CRITICAL AREAS AS DEFINED BY THE CLIENT AGENCY.

SECURING CRITICAL AREAS (SHELL)

The Lessor shall secure areas designated as Critical Areas to restrict access:

- A. Keyed locks, keycards, or similar security measures shall strictly control access to mechanical areas. Additional controls for access to keys, keycards, and key codes shall be strictly maintained. The Lessor shall develop and maintain accurate HVAC diagrams and HVAC system labeling within mechanical areas.
- B. Roofs with HVAC systems shall also be secured. Fencing or other barriers may be required to restrict access from adjacent roofs based on a Government Building Security Assessment. Roof access shall be strictly controlled through keyed locks, keycards, or similar measures. Fire and life safety egress shall be carefully reviewed when restricting roof access.
- C. At a minimum, Lessor shall secure building common areas including sprinkler rooms, electrical closets, telecommunications rooms.

VISITOR ACCESS CONTROL (SHELL)

Entrances are open to the public during business hours. After hours, visitor entrances are secured, and have a means to verify the identity of persons requesting access prior to allowing entry into the Space.

INTERIOR (GOVERNMENT SPACE)

DESIGNATED ENTRANCES (SHELL)

The Government shall have a designated main entrance.

IDENTITY VERIFICATION (SHELL)

The Government reserves the right to verify the identity of persons requesting access to the Space prior to allowing entry.

FORMAL KEY CONTROL PROGRAM (SHELL)

The Government reserves the right to implement a formal key control program. The Lessor shall have a means of allowing the electronic disabling of lost or stolen access media, if electronic media is used.

SITES AND EXTERIOR OF THE BUILDING

SIGNAGE

POSTING OF SIGNAGE IDENTIFYING THE SPACE AS GOVERNMENTAL (SHELL)

The Lessor shall not post sign(s) or otherwise identify the facility and parking areas as a Government, or specific Government tenant, occupied facility, including during construction, without written Government approval.

POSTING OF REGULATORY SIGNAGE (SHELL)

The Government may post or request the Lessor to post regulatory, statutory, sensitive areas and site specific signage.

LANDSCAPING

LANDSCAPING REQUIREMENTS (SHELL)

Lessor shall maintain landscaping (trees, bushes, hedges, land contour, etc.) around the facility. Landscaping shall be neatly trimmed in order to minimize the opportunity for concealment of individuals and packages/containers. Landscaping shall not obstruct the views of security guards and CCTV cameras, or interfere with lighting or IDS equipment.

CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN (SHELL)

The Lessor shall separate from public access, restricted areas as designated by the Government, through the application of Crime Prevention Through Environmental Design (CPTED) principles by using trees, hedges, berms, or a combination of these or similar features, and by fences, walls, gates and other barriers, where feasible and acceptable to the Government.

HAZMAT STORAGE

If there is HAZMAT storage, lessor shall locate it in a restricted area or storage container away from loading docks, entrances, and uncontrolled parking.

PLACEMENT OF RECEPTACLES, CONTAINERS, AND MAILBOXES

Trash receptacles, containers, mailboxes, vending machines, or other fixtures and/or features that could conceal packages, brief cases, or other portable containers shall be located 10 feet away from building.

SECURITY SYSTEMS

THE FOLLOWING CCTV, IDS, AND DURESS ALARMS ITEMS ARE TO BE INSTALLED BY EITHER THE LESSOR OR PARENT VA MEDICAL CENTER. CONSULT WITH PARENT VA MEDICAL CENTER TO DETERMINE WHICH VERSIONS APPLY. WHEN CHOOSING PARAGRAPHS REQUIRING LESSOR INSTALLATION, ESPECIALLY FOR DURESS ALARMS, OBTAIN SPECIFICATIONS FROM FPS AND PARENT VA MEDICAL CENTER

CLOSED CIRCUIT TELEVISION SYSTEM (CCTV)

ACTION REQUIRED: LEASING SPECIALIST MUST CHOOSE 1 OF THE 2 FOLLOWING PARAGRAPHS (LESSOR PROVIDED OR GOVERNMENT PROVIDED) AND DELETE THE OTHER PARAGRAPH.

LESSOR PROVIDED DESIGN, INSTALLATION, AND MAINTENANCE

The lessor shall design, install, and maintain a Closed Circuit Television (CCTV) system as described in this section. The CCTV system will support the entry control system (at entrances and exits to the space), with time lapse video recording, that will allow Government employees to view and communicate remotely with visitors before allowing access to the Space. As determined by the Government the CCTV system shall provide unobstructed coverage of designated pedestrian entrances and exits. Technical review of the proposed system shall be coordinated with the Government security representative, at the direction of the Contracting Officer, prior to installation. CCTV system testing and acceptance shall be conducted by the Government prior to occupancy. The CCTV system shall comply with the Architectural Barriers Act, section F230.0. The Government will centrally monitor the CCTV system. Government specifications are available from the Lease Contracting Officer. CCTV system components which fail or require maintenance or which fail during testing should be serviced in accordance with the Security System Maintenance Criteria listed below.

Security System Maintenance Criteria: The Lessor, in consultation and coordination with a security provider, either internal or external, as determined by the Lease Contracting Officer, and the Government security representative, shall implement a preventive maintenance program for all security systems the Lessor has installed. Any critical component that becomes inoperable must be replaced or repaired by the Lessor within 5 business days. Critical components are those required to provide security (IDS, CCTV, access control, etc.) for a perimeter access point or critical area. "Replacement" may include implementing other temporary measures in instances where the replacement or repair is not achievable within the specified time frame (e.g. a temporary barrier to replace an inoperable pop-up vehicle barrier, etc.). Failure by the Lessor to provide sufficient replacement measures within the timeframe identified above may result in the Government's providing guard service, the cost of which must be reimbursed by the Lessor.

GOVERNMENT PROVIDED PRODUCT, INSTALLATION, AND MAINTENANCE

The Government shall provide and install an entry control system, with time lapse video recording, that will allow Government employees to view and communicate remotely with visitors before allowing access. This Closed Circuit Television (CCTV) system shall provide the Government with unobstructed coverage, as determined by the Government, of designated pedestrian entrances and exits. The Lessor shall permit twenty-four hour CCTV coverage and recording, provided and operated by the Government. The Government will centrally monitor the CCTV surveillance. Government specifications are available from the Contracting Officer. The Lessor shall post necessary regulatory, statutory, and/or site specific signage, as determined by the Government.

The Lessor, at the notice to proceed stage of the procurement, shall advise the Government of the appropriate time to install the equipment during the construction of the Space. The Lessor shall facilitate the installation by allowing access to electrical panels and other areas of the building as necessary.

INTRUSION DETECTION SYSTEM (IDS)

ACTION REQUIRED: LEASING SPECIALIST MUST CHOOSE 1 OF THE 2 FOLLOWING PARAGRAPHS (LESSOR PROVIDED OR GOVERNMENT PROVIDED) AND DELETE THE OTHER PARAGRAPH.

LESSOR PROVIDED DESIGN, INSTALLATION, AND MAINTENANCE

The Lessor shall design, install, and maintain an Intrusion Detection System (IDS) as described in this section. The Government requires an IDS, which will cover perimeter entry and exit doors, and operable ground-floor windows. Basic Security-in-Depth IDS components include: magnetic door switch(s), alarm system keypad, passive infrared sensor(s) (PIR), an alarm panel (to designated monitoring center) and appropriate communication method i.e. telephone and/or Internet

connection, glass-break detector, magnetic window switches or shock sensors. Technical review of the proposed system shall be coordinated with the Government security representative, at the direction of the Lease Contracting Officer, prior to installation. System testing and acceptance shall be conducted by the Government prior to occupancy.

Basic Security-in-Depth IDS shall be connected to and monitored at a central station operated by parent VA Medical Center or other location. Emergency notification lists shall be coordinated with the monitoring station to include all applicable Government and lessor points of contact. Monitoring shall be designed to facilitate a real-time detection of an incident, and to coordinate an active response to an incident. The Lessor must complete the Megacenter Alarm Requirements (MAR) application process specified by the Government to meet the monitoring requirements for a functional IDS. Components which fail or require maintenance or which fail during testing shall be serviced in accordance with the Security System Maintenance Criteria listed below.

Security System Maintenance Criteria: The Lessor, in consultation and coordination with a security provider, either internal or external, as determined by the Lease Contracting Officer, and the Government security representative, shall implement a preventive maintenance program for all security systems the Lessor has installed. Any critical component that becomes inoperable must be replaced or repaired by the Lessor within 5 business days. Critical components are those required to provide security (IDS, CCTV, access control, etc.) for a perimeter access point or critical area. "Replacement" may include implementing other temporary measures in instances where the replacement or repair is not achievable within the specified time frame (e.g. a temporary barrier to replace an inoperable pop-up vehicle barrier, etc.). Failure by the Lessor to provide sufficient replacement measures within the timeframe identified above may result in the Government providing guard service, the cost of which must be reimbursed by the Lessor.

GOVERNMENT PROVIDED SCOPE AND PRODUCT, INSTALLATION, AND MAINTENANCE The Lessor shall permit installation of a perimeter Intrusion Detection System (IDS) to be operated by the Government. The Government shall provide and install an IDS on perimeter entry and exit doors, and operable ground-floor windows. Basic Security-in-Depth IDS include: magnetic door switch(s), alarm system keypad, passive infrared sensor(s) (PIR), an alarm panel (to designated monitoring center) and appropriate communication method i.e. telephone and/or Internet connection, glass-break detector, magnetic window switches or shock sensors.

Basic Security-in-Depth IDS shall be connected and monitored at a central station. Emergency notification lists shall be coordinated with the monitoring station to include all applicable Government and Lessor points of contact. Monitoring shall be designed to facilitate a real-time detection of an incident, and to coordinate an active response to an incident.

The Lessor, at the notice to proceed stage of the procurement, shall advise the Government of the appropriate time to install the equipment during the construction of the Space. The Lessor shall facilitate the installation by allowing access to electrical panels and other areas of the building, as necessary.

DURESS ALARM

ACTION REQUIRED: LEASING SPECIALIST MUST CHOOSE 1 OF THE 2 FOLLOWING PARAGRAPHS (LESSOR PROVIDED OR GOVERNMENT PROVIDED) AND DELETE THE OTHER PARAGRAPH.

LESSOR PROVIDED DESIGN, INSTALLATION, AND MAINTENANCE

The Lessor shall design, install, and maintain a duress alarm system as described. THE GOVERNMENT SHALL PROVIDE A SCOPE OF WORK FOR A DURESS ALARM SYSTEM. (LCO SHOULD ADD SPECIFIC SCOPE HERE) Technical review shall be coordinated with the Government security representative, at the direction of the Contracting Officer, prior to installation. System testing and acceptance shall be conducted by the Government prior to occupancy. This system shall comply with the Architectural Barriers Act, section F230.0.

The lessor in consultation and coordination with the security provider and Government shall conduct security system performance testing annually. Testing must be based on established, consistent agency-specific protocols, documented and furnished to the Contracting Officer. Components which fail or require maintenance or which fail during testing should be serviced in accordance with the Security System Maintenance Criteria listed below.

Security System Maintenance Criteria: The Lessor in consultation and coordination with a security provider, either internal or external, as determined by the Lease Contracting Officer, and the Government security representative shall implement a preventive maintenance program for all security systems they have installed. Any critical component that becomes inoperable must be replaced or repaired within 5 business days. Critical components are those required to provide security (IDS, CCTV, access control, etc.) for a perimeter access point or critical area. "Replacement" may include implementing other temporary measures in instances where the replacement or repair is not achievable within the specified time frame (e.g. a temporary barrier to replace an inoperable pop-up vehicle barrier, etc.). Failure by the Lessor to provide sufficient replacement measures within the timeframe identified above may result in the Government's providing guard service, the cost of which must be reimbursed by the Lessor.

GOVERNMENT PROVIDED SCOPE, PRODUCT, INSTALLATION, AND MAINTENANCE

The Lessor shall permit installation of a duress alarm system to be provided and operated by the Government. The Government, in coordination with a security provider, either internal or external, as determined by the Contracting Officer, shall document and implement duress procedures for emergency situations.

The Lessor, at the notice to proceed stage of the procurement, shall advise the Government of the appropriate time to install the equipment during the construction of the Space and shall facilitate the installation, including access to electrical panels and other areas of the building, as necessary.

STRUCTURE

WINDOWS

SHATTER-RESISTANT WINDOW PROTECTION

The Lessor shall provide and install, shatter-resistant material not less than 0.18 millimeters (7 mil) thick on all exterior windows in Government-occupied space meeting the following properties - Film composite strength and elongation rate measured at a strain rate not exceeding 50% per minute shall not be less than the following:

- Yield Strength: 12,000 psi
- Elongation at yield: 3%
- Longitudinal Tensile strength: 22,000 psi
- Traverse Tensile strength: 25,000 psi
- Longitudinal Elongation at break: 90%
- Traverse Elongation at break: 75%

THE ALTERNATIVE METHOD is for the Lessor to provide a window system that conforms to a minimum glazing performance condition of "3b" for a high protection level and a low hazard level. Window systems shall be certified as prescribed by WINGARD PE 4.3 or later to GSA performance condition 3b in accordance with the GSA Standard Test Method for Glazing and Window Systems Subject to Dynamic loadings or Very low Hazard (in accordance with ASTM F 1642, Standard Test Method for Glazing or Glazing Systems Subject to Air Blast loading) in response to air blast load of 4 psi/28 psi-msec.

If the lessor chooses the Alternative Method, they shall provide a description of the shatter-resistant window system and provide certification from a licensed professional engineer that the system as offered meets the above standard. Prior to installation, this will be provided for evaluation by the Government, whose approval shall not be unreasonably withheld.

OPERATIONS AND ADMINISTRATION

LESSOR TO WORK WITH VA POLICE (SHELL)

The Lessor shall cooperate and work with the buildings' VA Police throughout the term of the lease.

ACCESS TO BUILDING INFORMATION (SHELL)

Building Information--including mechanical, electrical, vertical transport, fire and life safety security system plans and schematics, computer automation systems, and emergency operations procedures--shall be strictly controlled. Such information shall be released to authorized personnel only, approved by the Government, by the development of an access list and controlled copy numbering. The Contracting Officer may direct that the names and locations of Government tenants not be disclosed in any publicly accessed document or record. If that is the case, the Government may request that such information not be posted in the building directory.

Lessor shall have emergency plans and associated documents readily available in the event of an emergency.

VASD Police Standards & Criteria

FOR LEASES ONLY

VA Engineering and all contractors/Lessor(s) will ensure that all construction projects (new or renovation) at any VA owned or lease asset will adhere to the standards and criteria as defined by

- *Physical Security Design Manual for Life-Safety Protected Facilities*
- *Physical Security Design Manual for VA Mission Critical Facilities*
- *Appendix B, Physical Security Requirements and Options, VA Handbook 0730*

FOR LEASES ONLY (Minor or Major): In effort to comply with the physical security, decrease project delivery times, increase competition, and lower delivery costs, VA Leases project can conform to Appendix A for minimum requirement with the approval of greater than or equal to VASD Physical Security Specialist.

- Attachment A: *Real Property Policy Memorandum 2018-02 Physical Security Standards for Leased Facilities (Existing Space and Lease Construction Projects) (VAIQ 7866496)*
- All leased facility will, at a minimum, be designated Facility Security Level (FSL) II. Detailed FSL information will be incorporated in the ASR/Solicitation for each leased facility prior of award.

The information below will coincide with the required standard and criteria listed above (unless stated otherwise) in order to capture specific requirement, due to the nature/function of the leased building. All the information below and attachment was reviewed and approved by the designated COR and greater than or equal to VASD Physical Security Specialist.

1. VA Standard/Policy/Directive/Memo Requirements

1.1. The lessor/contractor shall be responsible to comply with the following list below as well as adhere to all information listed in this document.

- 1.1.1. Attachment A: *Real Property Policy Memorandum 2018-02 Physical Security Standards for Leased Facilities (Existing Space and Lease Construction Projects) (VAIQ 7866496)*
- 1.1.2. Attachment B: *HSPD 12*
- 1.1.3. Attachment C: *NIST.FIPS.201-2*

2. Security Systems Hardware, Software, and Maintenance Requirements

2.1. Closed Circuit Television System (CCTV)

- 2.1.1. The lessor shall be responsible for all parts, labor, and maintenance required to completely furnish, install, test, and turnover the CCTV security system. The lessor shall also maintain the latest software for all security system that require continuous software updates.
- 2.1.2. Dummy or fake cameras will not be utilized at any time.
- 2.1.3. Lessor shall comply to the standard/policy/directive/memo requirements listed above.
- 2.1.4. Dependent upon the condition of existing CCTV, the government may in their best interest utilized the existing system to minimize cost impact. Re-using the existing system will require the lessor to provide specs to allow the government to determine whether it's feasible or not.
- 2.1.5. Lessor shall furnish and install similar or equal to the following:

- 2.1.5.1. Closed circuit television system (CCTV), industrial quality, one station (Camera & monitor)
- 2.1.5.2. Additional cameras will be needed dependent upon layout of space.
- 2.1.5.3. Shall come with built-in video motion detection that shall automatically monitor and process information from each camera. The camera motion detection shall detect motion within the camera's field of view and provide automatic visual, remote alarms as a result of detected motion.
- 2.1.5.4. Shall be programmed to digitally flip from color to black and white at dusk and vice versa at low light conditions.
- 2.1.5.5. Will be fitted with AI/DC lenses to ensure the image quality under different light conditions.
- 2.1.5.6. Recommended Hardware/Software (Similar or Equal)**
 - 2.1.5.6.1. Avigilon Control Center H4 or H5 series cameras with analytics
 - 2.1.5.6.2. Equipped with UPS.
 - 2.1.5.6.3. <https://www.avigilon.com/>
 - 2.1.5.6.4. Avigilon Network Video Recorder (NVR) capable of storing 15 days or more of recording footage.
 - 2.1.5.6.5. Optimized Recording Storage Management: Unique data storage and archiving solution that combines superior performance and scalability and cost-efficient long-term video storage
- 2.1.5.7. To be a local standalone system (Refer to "Other Security Requirement" for more detail)
- 2.1.6. Lessor shall provide the Government submittals of the proposed CCTV security systems prior of purchase and installation.
- 2.1.7. Camera Schedule - A camera schedule shall be developed for each camera. Contractors shall coordinate with the Government representative to determine camera starting numbers and naming conventions. All drawings shall identify wire and cable standardization methodology. Color coding of all wiring conductors and jackets is required and shall be communicated consistently throughout the drawings package submittal. At a minimum, the camera schedule shall include the following information:
 - 2.1.7.1. Item Number
 - 2.1.7.2. Camera Number
 - 2.1.7.3. Naming Conventions
 - 2.1.7.4. Description of Camera Coverage
 - 2.1.7.5. Camera Location
 - 2.1.7.6. Floor Plan Sheet Number
 - 2.1.7.7. Camera Type
 - 2.1.7.8. Mounting Type
 - 2.1.7.9. Standard Detail Reference
 - 2.1.7.10. Power Input & Draw
 - 2.1.7.11. Power Panel Location
 - 2.1.7.12. Remarks Column for Camera
- 2.2. Motion Intrusion / Intrusion Detection System
 - 2.2.1. The lessor shall be responsible for all parts, labor, and maintenance required to completely furnish, install, test, and turnover the Intrusion Detection System (IDS).
 - 2.2.2. Lessor shall comply to the standard/policy/directive/memo requirements listed above.

- 2.2.3. Lessor shall provide a monitoring company service who notifies VAPD of any alarms that occur within the agreed lease perimeter. The Lessor will continue to provide this service of IDS until the lease term agreement ends.
- 2.2.4. Lessor shall provide the Government submittals of the proposed IDS prior of purchase and installation.
- 2.2.5. All equipment associated within the IDS shall be rated for continuous operation. Environmental conditions (i.e. temperature, humidity, wind, and seismic activity) shall be taken under consideration at each facility and site location prior to installation of the equipment.
- 2.2.6. All equipment shall operate on 120 or 240 volts alternating current (VAC); 50 Hz or 60 Hz AC power system unless documented otherwise in subsequent sections listed within this specification. All equipment shall have a back-up source of power (UPS) that will provide a minimum of 96 hours of run time in the event of a loss of primary power to the facility.
- 2.2.7. The system shall be designed, installed, and programmed in a manner that will allow for ease of operation, programming, servicing, maintenance, testing, and upgrading of the system.
- 2.2.8. The motion intrusion detectors will cover all entrances into the agreed upon lease building/space.
- 2.2.9. Lessor Supervision: System components shall be continuously monitored for normal, alarm, supervisory, and trouble conditions. Indicate deviations from normal conditions at any location in system. Indication includes identification of device or circuit in which deviation has occurred and whether deviation is an alarm or malfunction.
- 2.2.10. System Control: Central-station control unit shall directly monitor intrusion detection units and connecting wiring.
- 2.2.11. System shall automatically reboot program without error or loss of status or alarm data after any system disturbance.
- 2.2.12. Ensure that IDS is fully integrated with other security subsystems as required to include, but not limited to, the CCTV, EPPS, and Physical Access Control System and Database Management. The IDS provided shall not limit the expansion and growth capability to a single manufacturer and shall allow modular expansion with minimal equipment modifications.
- 2.2.13. IDS Components: The IDS shall consist of, but not be limited to, the following components:
 - 2.2.13.1. Control Panel
 - 2.2.13.2. Exterior Detection Devices (Sensors)
 - 2.2.13.3. Interior Detection Devices (Sensors)
 - 2.2.13.4. Power Supply
 - 2.2.13.5. Enclosures
 - 2.2.13.6. Sounding alarm ranging within 80-90db.

2.3. Access Control

- 2.3.1. The lessor shall be responsible for all parts, labor, and maintenance required to completely furnish, install, test, and turnover the Access Control System.
- 2.3.2. The lessor shall design, install, and maintain the Access Control System as described in this section. Access control system sole purpose is to monitor who comes in and out of the lease premises.

- 2.3.3. Lessor shall comply to the standard/policy/directive/memo requirements listed above.
- 2.3.4. Access control (Hardware and software) must be HSPD 12 and FIPS 201-2 compliant. Refer to Attachment B & C.
- 2.3.5. Recommended Hardware/Software (Similar or equal)
 - 2.3.5.1. Hardware: AMAG
 - 2.3.5.1.1. <https://www.amag.com/>
 - 2.3.5.2. Software: Symmetry
 - 2.3.5.2.1. Compatible with Federal or Homeland Security package.
 - 2.3.5.2.2. <https://www.amag.com/access-control>
- 2.3.6. Access control, computerized Card/PIV reader, quantity of door(s) is dependent upon total entry/exit of lease building. To include all hardware, software, lockset, and/or wiring.
- 2.3.7. To be a local standalone system (Refer to "Other Security Requirement" for more detail)
- 2.3.8. Physical Access Control System (PACS) shall consist but not limited to:
 - 2.3.8.1. Head-End equipment server,
 - 2.3.8.2. One or more networked PC-based workstations
 - 2.3.8.3. Physical Access Control System and Database Management Software
 - 2.3.8.4. Credential validation software/hardware
 - 2.3.8.5. Field installed controllers
 - 2.3.8.6. Access card reader with number pad, must be able to read PIV
 - 2.3.8.7. Supportive information system
 - 2.3.8.8. Door locks and sensors
 - 2.3.8.9. Power supplies and to be equipped with UPS
 - 2.3.8.10. Interfaces with:
 - 2.3.8.10.1. Video Surveillance and Assessment System,
 - 2.3.8.10.2. Gate, turnstile, and traffic arm controls,
 - 2.3.8.10.3. Automatic door operators,
 - 2.3.8.10.4. Intrusion Detection System,
 - 2.3.8.10.5. Intercommunication System
 - 2.3.8.10.6. Fire Protection System,
 - 2.3.8.10.7. HVAC,
 - 2.3.8.10.8. Building Management System,
 - 2.3.8.10.9. Elevator Controls,
- 2.3.9. PACS system shall support:
 - 2.3.9.1. Multiple credential authentication modes,
 - 2.3.9.2. Bidirectional communication with the reader,
 - 2.3.9.3. Incident response policy implementation capability; system shall have capability to automatically change access privileges for certain user groups to high security areas in case of incident/emergency.
 - 2.3.9.4. Visitor management,

2.4. Other Security Requirement

- 2.4.1. All security software must be compatible and installed on one single workstation/CPU.
- 2.4.2. Workstation/CPU including a viewing monitor will be a local standalone system placed inside a wall mount; enclosed, lockable rack closet equipped with a pull-out keyboard tray.
- 2.4.3. The lessor shall cooperate and work with the buildings' VASD Police throughout the term of the lease.

2.4.4. All equipment shall have surge protection.

2.5. Security System Maintenance Criteria:

2.5.1. The Lessor, in consultation and coordination with a security provider, either internal or external, as determined by the Lease Contracting Officer, and the Government COR and VASD security specialist representative, shall implement a preventive maintenance program for all security systems the Lessor has installed. Any critical component that becomes inoperable must be replaced or repaired by the Lessor within 5 business days. Critical components are those required to provide security (IDS, CCTV, access control, etc.) for a perimeter access point or critical area. "Replacement" may include implementing other temporary measures in instances where the replacement or repair is not achievable within the specified time frame (e.g. a temporary barrier to replace an inoperable pop-up vehicle barrier, etc.). Failure by the Lessor to provide sufficient replacement measures within the timeframe identified above may result in the Government's providing guard service, the cost of which must be reimbursed by the Lessor.

3. Structure

3.1. Windows

3.1.1. The lessor shall provide and install security meshing on all exterior glass under the following criteria:

3.1.1.1. Windows or skylights below 18 feet (4 m) from ground level or the roof of a lower abutment, or less than 18 feet (4 m) from windows of an adjoining building, or accessible by a building ledge leading to windows of other floor rooms, shall have forced entry construction of stainless steel woven security mesh.

3.1.1.1.1. All #304 stainless steel woven mesh 0.7 mm (.028 in.) wire diameter, with tensile strength of 15 kg/mm (800 pounds per linear inch).

3.1.1.1.2. Mesh 12x12 per 25 mm (1 in.) with main and sub frames of 2.7 mm (12 gauges) carbon steel with baked enamel finish and internal key locking slide bolts.

(k) recommended research and development on technologies designed to enhance screening effectiveness and further protect privacy interests; and

(l) a plan for incorporating known traveler programs into the screening procedures, where appropriate.

(7) Not later than 90 days after the date of this directive, the Secretary of Homeland Security, in coordination with the heads of the Federal departments and agencies listed in section 4 of this directive, shall also provide to me, through the Assistant to the President for Homeland Security and the Director of the Office of Management and Budget, a prioritized investment and implementation plan for a systematic approach to terrorist-related screening that optimizes detection and interdiction of suspected terrorists and terrorist activities. The plan shall describe the scope, governance, principles, outcomes, milestones, training objectives, metrics, costs, and schedule of activities to implement the policy set forth in section 1 of this directive. The Secretary of Homeland Security shall further provide a report on the status of the implementation of the plan to me through the Assistant to the President for Homeland Security 6 months

after the date of this directive and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

(8) In order to ensure comprehensive and coordinated terrorist-related screening procedures, the implementation of this directive shall be consistent with Government-wide efforts to improve information sharing. Additionally, the reports and plan required under sections 4 and 7 of this directive shall inform development of Government-wide information sharing improvements.

(9) This directive does not alter existing authorities or responsibilities of department and agency heads including to carry out operational activities or provide or receive information. This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees, or agents, or any other person.

GEORGE W. BUSH

Homeland Security Presidential Directive/HSPD-12—Policy for a
Common Identification Standard for Federal Employees and Contractors
August 27, 2004

Subject: Policy for a Common Identification Standard for Federal Employees and Contractors

(1) Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a man-

datory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

(2) To implement the policy set forth in paragraph (1), the Secretary of Commerce shall promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification (the "Standard") not later than 6 months

after the date of this directive in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy. The Secretary of Commerce shall periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies.

(3) "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The Standard shall not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).

(4) Not later than 4 months following promulgation of the Standard, the heads of executive departments and agencies shall have a program in place to ensure that identification issued by their departments and agencies to Federal employees and contractors meets the Standard. As promptly as possible, but in no case later than 8 months after the date of promulgation of the Standard, the heads of executive departments and agencies shall, to the maximum extent practicable, require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. Departments and agencies shall implement this directive in a manner consistent with ongoing Government-wide activities, policies and

guidance issued by OMB, which shall ensure compliance.

(5) Not later than 6 months following promulgation of the Standard, the heads of executive departments and agencies shall identify to the Assistant to the President for Homeland Security and the Director of OMB those Federally controlled facilities, Federally controlled information systems, and other Federal applications that are important for security and for which use of the Standard in circumstances not covered by this directive should be considered. Not later than 7 months following the promulgation of the Standard, the Assistant to the President for Homeland Security and the Director of OMB shall make recommendations to the President concerning possible use of the Standard for such additional Federal applications.

(6) This directive shall be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5 U.S.C. 552a) and other statutes protecting the rights of Americans.

(7) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance. This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees or agents, or any other person.

(8) The Assistant to the President for Homeland Security shall report to me not later than 7 months after the promulgation of the Standard on progress made to implement this directive, and shall thereafter report to me on such progress or any

recommended changes from time to time as appropriate.

GEORGE W. BUSH

The President's Radio Address
August 28, 2004

Good morning. In the 3 years since our country was attacked, America has remained on the offensive against terrorist enemies wherever they hide and plot. Part of that offensive has been to reorganize our Government so that all our intelligence and law enforcement agencies cooperate effectively to expose and disrupt threats against America.

The Commission on Terrorist Attacks Upon the United States, also known as the 9/11 Commission, concluded that these efforts have made America safer. They also concluded that America is still not safe. I agree with both of those conclusions, and so my administration is taking additional actions to reform our intelligence services and improve America's ability to find, track, and stop dangerous terrorists.

This week, I signed a series of Executive orders to ensure that the people in Government responsible for defending America and countering terrorism have the best possible information and support to identify threats and to protect the homeland. Some of these orders reflect specific recommendations of the 9/11 Commission. All of them are essential to America's security as we wage the war on terror.

First, I have ordered the Director of Central Intelligence to perform the functions of the National Intelligence Director within the constraints of existing law, until Congress establishes that position. I agree with the 9/11 Commission that America needs a single official to coordinate the foreign and domestic activities of the intelligence community with authority over personnel, budgeting, and policy. I am working

with Members of Congress to create this position, and while we act, the Director of Central Intelligence will play an expanded role. I also urge Congress to act swiftly on my nomination of Porter Goss, a proven reformer with decades of experience in intelligence to lead the CIA.

Second, I have ordered the establishment of a National Counterterrorism Center. This new center builds on the capabilities of the Terrorist Threat Integration Center, which I created more than a year ago. The Center will become our Government's central knowledge bank for information about known and suspected terrorists and will help ensure effective joint action across the Government so that our efforts against terrorists are unified in priority and purpose. Center personnel will also prepare the daily terrorism threat report that comes to me and to senior Government officials.

Third, we're making sure that all agencies of our Government share vital threat information. I have ordered the Director of Central Intelligence to ensure that we have common standards and clear accountability measures for intelligence sharing across the agencies of our Government. I have established a new Information Systems Council to identify and break down any remaining barriers to the rapid sharing of threat information by America's intelligence agencies, law enforcement agencies, and State and local governments. To continue to protect the freedoms and privacy of our citizens, I've established a Civil Liberties Board to monitor information-sharing practices.

FIPS PUB 201-2

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Personal Identity Verification (PIV) of Federal Employees and Contractors

*Computer Security Division
Information Technology Laboratory*

<http://dx.doi.org/10.6028/NIST.FIPS.201-2>

August 2013



U.S. DEPARTMENT OF COMMERCE
Penny Pritzker, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

Acknowledgements

NIST would like to acknowledge the significant contributions of the Identity, Credential, and Access Management Subcommittee (ICAMSC) and the Smart Card Interagency Advisory Board (IAB) for providing valuable contributions to the development of technical frameworks on which this Standard is based.

Special thanks to those who have participated in the business requirements meeting and provided valuable comments in shaping this Standard.

FOREWORD

The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of the Federal Information Security Management Act (FISMA) of 2002.

Comments concerning FIPS publications are welcomed and should be addressed to the Director, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900.

Charles H. Romine, Director
Information Technology Laboratory

ABSTRACT

This Standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to Federally controlled government facilities and logical access to government information systems.

The Standard contains the minimum requirements for a Federal personal identity verification system that meets the control and security objectives of Homeland Security Presidential Directive-12 [HSPD-12], including identity proofing, registration, and issuance. The Standard also provides detailed specifications that will support technical interoperability among PIV systems of Federal departments and agencies. It describes the card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the card. The physical card characteristics, storage media, and data elements that make up identity credentials are specified in this Standard. The interfaces and card architecture for storing and retrieving identity credentials from a smart card are specified in Special Publication 800-73, *Interfaces for Personal Identity Verification*. The interfaces and data formats of biometric information are specified in Special Publication 800-76, *Biometric Specifications for Personal Identity Verification*. The requirements for cryptographic algorithms are specified in Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*. The requirements for the accreditation of the PIV Card issuers are specified in Special Publication 800-79, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*. The unique organizational codes for Federal agencies are assigned in Special Publication 800-87, *Codes for the Identification of Federal and Federally-Assisted Organizations*. The requirements for card readers are specified in Special Publication 800-96, *PIV Card to Reader Interoperability Guidelines*. The format for encoding the chain-of-trust for import and export is specified in Special Publication 800-156, *Representation of PIV Chain-of-Trust for Import and Export*. The requirements for issuing PIV derived credentials are specified in Special Publication 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*.

This Standard does not specify access control policies or requirements for Federal departments and agencies.

Keywords: architecture, authentication, authorization, biometrics, credential, cryptography, Federal Information Processing Standards (FIPS), HSPD-12, identification, identity, infrastructure, model, Personal Identity Verification, PIV, public key infrastructure, PKI, validation, verification.

**Federal Information Processing Standards 201
2013**

**Announcing the
Standard for**

**Personal Identity Verification (PIV)
of
Federal Employees and Contractors**

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to the Federal Information Security Management Act (FISMA) of 2002.

1. Name of Standard.

FIPS PUB 201-2: Personal Identity Verification (PIV) of Federal Employees and Contractors.¹

2. Category of Standard.

Information Security.

3. Explanation.

Homeland Security Presidential Directive-12 [HSPD-12], dated August 27, 2004, entitled “Policy for a Common Identification Standard for Federal Employees and Contractors,” directed the promulgation of a Federal standard for secure and reliable forms of identification for Federal employees and contractors. It further specified secure and reliable identification that—

- (a) is issued based on sound criteria for verifying an individual employee’s identity;
- (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
- (c) can be rapidly authenticated electronically; and
- (d) is issued only by providers whose reliability has been established by an official accreditation process.

The directive stipulated that the Standard include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. Executive departments and agencies are required to implement the Standard for identification issued to Federal employees and contractors in gaining physical access to controlled facilities and logical access to controlled information systems.

4. Approving Authority.

Secretary of Commerce.

¹ This Standard is in response to Homeland Security Presidential Directive-12, which states that it is “intended only to improve the internal management of the executive branch of the Federal Government.”

5. Maintenance Agency.

Department of Commerce, NIST, Information Technology Laboratory (ITL).

6. Applicability.

This Standard is applicable to identification issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems, except for “national security systems” as defined by 44 U.S.C. 3542(b)(2) [SP 800-59]. Except as provided in [HSPD-12], nothing in this Standard alters the ability of government entities to use the Standard for additional applications.

Special-Risk Security Provision—The U.S. Government has personnel, facilities, and other assets deployed and operating worldwide under a vast range of threats (e.g., terrorist, technical, intelligence), particularly heightened overseas. For cardholders with particularly sensitive threats while outside the contiguous United States, the issuance, holding, and/or use of PIV Cards with full technical capabilities as described herein may result in unacceptably high risk. In such cases of extant risk (e.g., to facilities, individuals, operations, the national interest, or the national security), by the presence and/or use of full-capability PIV Cards, the head of a department or independent agency may issue a select number of maximum security PIV Cards that do not contain (or otherwise do not fully support) the wireless and/or biometric capabilities otherwise required/referenced herein. To the greatest extent practicable, heads of departments and independent agencies should minimize the issuance of such special-risk security PIV Cards so as to support interagency interoperability and the President’s policy. Use of other risk-mitigating technical (e.g., high-assurance on-off switches for the wireless capability) and procedural mechanisms in such situations is preferable, and as such is also explicitly permitted and encouraged. As protective security technology advances, the need for this provision will be re-assessed as the Standard undergoes the normal review and update process.

7. Specifications.

Federal Information Processing Standards (FIPS) 201 Personal Identity Verification (PIV) of Federal Employees and Contractors.

8. Implementations.

This Standard satisfies the control objectives, security requirements, and technical interoperability requirements of [HSPD-12]. The Standard specifies implementation of identity credentials on integrated circuit cards for use in a Federal personal identity verification system.

A PIV Card must be personalized with identity information for the individual to whom the card is issued, in order to perform identity verification both by humans and automated systems. Humans can use the physical card for visual comparisons, whereas automated systems can use the electronically stored data on the card to conduct automated identity verification. In implementing PIV systems and pursuant to Section 508 of the Rehabilitation Act of 1973 (the Act), as amended, agencies have the responsibility to accommodate federal employees and contractors with disabilities to have access to and use of information and data comparable to the access to and use of such information and data by federal employees and contractors who are not individuals with disabilities. In instances where Federal agencies assert exceptions to Section 508 accessibility requirements (e.g., undue burden, national security, commercial non-availability), Sections 501 and 504 of the Act requires Federal agencies to provide reasonable accommodation for federal employees and contractors with disabilities whose needs are not met by the

baseline accessibility provided under Section 508. While Section 508 compliance is the responsibility of Federal agencies and departments, this Standard specifies options to aid in implementation of the requirements:

- + Section 4.1.4.3 specifies Zones 21F and 22F as an option for orientation markers of the PIV Card.
- + Section 2.8 describes an alternative to the National Criminal History Check (NCHC) in instances where an applicant has unclassifiable fingerprints.
- + Sections 2.8, and 2.9 specify alternative methods for the 1:1 biometric match required at PIV Card issuance, reissuance, and reset.
- + Section 6 defines authentication mechanisms with varying characteristics for both physical and logical access (e.g., with or without PIN, over contact, contactless, or virtual contact interface).

Federal departments and agencies must use accredited issuers to issue identity credentials for Federal employees and contractors. For this purpose, NIST provided guidelines for the accreditation of PIV Card issuers in [SP 800-79]. The Standard also covers security and interoperability requirements for PIV Cards. For this purpose, NIST has established the PIV Validation Program that tests implementations for conformance with this Standard as specified in [SP 800-73] and [SP 800-78]. Additional information on this program is published and maintained at <http://csrc.nist.gov/groups/SNS/piv/npivp/>. The U.S. General Services Administration (GSA) has set up the FIPS 201 Evaluation Program to evaluate conformance of different families of products that support the PIV processes of this Standard – see Appendix A.5.

The Office of Management and Budget (OMB) provides implementation oversight for this Standard. The respective numbers of agency-issued 1) general PIV Cards and 2) special-risk PIV Cards (issued under the Special-Risk Security Provision) are subject to annual reporting to the OMB under the annual reporting process in a manner prescribed by OMB.

9. Effective Date.

This Standard is effective immediately and supersedes FIPS 201-1 (Change Notice 1). New optional features of this Standard that depend upon the release of new or revised NIST Special Publications are effective upon final publication of the supporting Special Publications.

10. Implementation Schedule.

This Standard mandates the implementation of some PIV Card features that were optional to implement in FIPS 201-1. To comply with FIPS 201-2, all new and replacement PIV Cards shall be issued with the mandatory PIV Card features no later than 12 months after the effective date of this Standard.

Accreditations of PIV Card issuers (PCIs) that occur 12 months after the effective date of this Standard shall be in compliance with FIPS 201-2.

FIPS 201-2 compliance of PIV components and subsystems is provided in accordance with M-06-18 [OMB0618] and M-11-11 [OMB1111] through products and services from GSA's Interoperability Test Program and Approved Products and Services List, once available. Implementation Guidance to PIV enable federal facilities and information systems, in accordance to M-11-11 will be outlined in the "Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance."

11. Qualifications.

The security provided by the PIV system is dependent on many factors outside the scope of this Standard. Upon adopting this Standard, organizations must be aware that the overall security of the personal identification system relies on—

- + assurance provided by the issuer of an identity credential that the individual in possession of the credential has been correctly identified;
- + protection provided to an identity credential stored within the PIV Card and transmitted between the card and the PIV issuance and usage infrastructure; and
- + protection provided to the identity verification system infrastructure and components throughout the entire lifecycle.

Although it is the intent of this Standard to specify mechanisms and support systems that provide high assurance personal identity verification, conformance to this Standard does not assure that a particular implementation is secure. It is the implementer's responsibility to ensure that components, interfaces, communications, storage media, managerial processes, and services used within the identity verification system are designed and built in a secure manner.

Similarly, the use of a product that conforms to this Standard does not guarantee the security of the overall system in which the product is used. The responsible authority in each department and agency shall ensure that an overall system provides the acceptable level of security.

Because a standard of this nature must be flexible enough to adapt to advancements and innovations in science and technology, NIST has a policy to review this Standard within five years to assess its adequacy.

12. Waivers.

As per the Federal Information Security Management Act of 2002 [FISMA], waivers to Federal Information Processing Standards are not allowed.

13. Where to Obtain Copies.

This publication is available through the Internet by accessing <http://csrc.nist.gov/publications/>.

14. Patents.

Aspects of the implementation of this Standard may be covered by U.S. or foreign patents.

Table of Contents

1. Introduction	1
1.1 Purpose	1
1.2 Scope	1
1.3 Change Management	2
1.3.1 Backward Compatible Change	2
1.3.2 Non-Backward Compatible Change	2
1.3.3 New Features	2
1.3.4 Deprecated and Removed	2
1.3.5 FIPS 201 Version Management	3
1.4 Document Organization	3
2. Common Identification, Security, and Privacy Requirements	5
2.1 Control Objectives	5
2.2 Credentialing Requirements	6
2.3 Biometric Data Collection for Background Investigations	6
2.4 Biometric Data Collection for PIV Card	6
2.5 Biometric Data Use	6
2.6 Chain-of-Trust	7
2.7 PIV Identity Proofing and Registration Requirements	8
2.8 PIV Card Issuance Requirements	10
2.8.1 Special Rule for Pseudonyms	11
2.8.2 Grace Period	11
2.9 PIV Card Maintenance Requirements	12
2.9.1 PIV Card Reissuance Requirements	12
2.9.2 PIV Card Post Issuance Update Requirements	14
2.9.3 PIV Card Verification Data Reset	14
2.9.4 PIV Card Termination Requirements	15
2.10 Derived PIV Credentials Issuance Requirements	16
2.11 PIV Privacy Requirements	16
3. PIV System Overview	18
3.1 Functional Components	18
3.1.1 PIV Front-End Subsystem	19
3.1.2 PIV Card Issuance and Management Subsystem	20
3.1.3 PIV Relying Subsystem	20
3.2 PIV Card Lifecycle Activities	21
4. PIV Front-End Subsystem	23
4.1 PIV Card Physical Characteristics	23
4.1.1 Printed Material	23
4.1.2 Tamper Proofing and Resistance	23
4.1.3 Physical Characteristics and Durability	24
4.1.4 Visual Card Topography	25
4.1.5 Color Representation	39
4.2 PIV Card Logical Characteristics	39
4.2.1 Cardholder Unique Identifier (CHUID)	40
4.2.2 Cryptographic Specifications	41
4.2.3 PIV Biometric Data Specifications	44

4.2.4	PIV Unique Identifiers	45
4.3	PIV Card Activation	45
4.3.1	Activation by Cardholder	46
4.3.2	Activation by Card Management System.....	46
4.4	Card Reader Requirements.....	46
4.4.1	Contact Reader Requirements.....	46
4.4.2	Contactless Reader Requirements.....	46
4.4.3	Reader Resilience and Flexibility	47
4.4.4	Card Activation Device Requirements.....	47
5.	PIV Key Management Requirements.....	48
5.1	Architecture	48
5.2	PKI Certificate	48
5.2.1	X.509 Certificate Contents	48
5.3	X.509 CRL Contents.....	49
5.4	Legacy PKIs	49
5.5	PKI Repository and OCSP Responder(s)	49
5.5.1	Certificate and CRL Distribution	49
5.5.2	OCSP Status Responders	50
6.	PIV Cardholder Authentication.....	51
6.1	PIV Assurance Levels	51
6.1.1	Relationship to OMB's E-Authentication Guidance.....	52
6.2	PIV Card Authentication Mechanisms.....	52
6.2.1	Authentication Using Off-Card Biometric Comparison	52
6.2.2	Authentication Using On-Card Biometric Comparison (OCC-AUTH)	53
6.2.3	Authentication Using PIV Asymmetric Cryptography	54
6.2.4	Authentication with the Symmetric Card Authentication Key (SYM-CAK)	55
6.2.5	Authentication Using the CHUID	56
6.2.6	Authentication Using PIV Visual Credentials (VIS).....	56
6.3	PIV Support of Graduated Assurance Levels for Identity Authentication.....	58
6.3.1	Physical Access	58
6.3.2	Logical Access.....	59

List of Appendices

Appendix A— PIV Validation, Certification, and Accreditation.....	60	
A.1	Accreditation of PIV Card Issuers (PCI)	60
A.2	Application of Risk Management Framework to IT System(s) Supporting PCI.....	61
A.3	Conformance Testing of PIV Card Application and Middleware.....	61
A.4	Cryptographic Testing and Validation.....	61
A.5	FIPS 201 Evaluation Program	61
Appendix B— PIV Object Identifiers and Certificate Extension.....	62	
B.1	PIV Object Identifiers	62
B.2	PIV Certificate Extension.....	62
Appendix C— Glossary of Terms, Acronyms, and Notations.....	64	
C.1	Glossary of Terms	64

C.2 Acronyms	68
C.3 Notations	70
Appendix D— References	71
Appendix E— Revision History.....	75

List of Figures

Figure 3-1. PIV System Notional Model	19
Figure 3-2. PIV Card Lifecycle Activities.....	21
Figure 4-1. Card Front—Printable Areas and Required Data	31
Figure 4-2. Card Front—Optional Data Placement—Example 1.....	32
Figure 4-3. Card Front—Optional Data Placement—Example 2.....	33
Figure 4-4. Card Front—Optional Data Placement—Example 3.....	34
Figure 4-5. Card Front—Optional Data Placement—Example 4.....	35
Figure 4-6. Card Back—Printable Areas and Required Data.....	36
Figure 4-7. Card Back—Optional Data Placement—Example 1	37
Figure 4-8. Card Back—Optional Data Placement—Example 2	38

List of Tables

Table 4-1. Name Examples.....	26
Table 4-2. Color Representation	39
Table 6-1. Relationship Between PIV and E-Authentication Assurance Levels	52
Table 6-2. Authentication for Physical Access.....	58
Table 6-3. Authentication for Logical Access.....	59
Table B-1. PIV Object Identifiers	62

1. Introduction

Authentication of an individual's identity is a fundamental component of physical and logical access control processes. When an individual attempts to access security-sensitive buildings, computer systems, or data, an access control decision must be made. An accurate determination of an individual's identity is needed to make sound access control decisions.

A wide range of mechanisms is employed to authenticate an identity, utilizing various classes of identity credentials. For physical access, an individual's identity has traditionally been authenticated by use of paper or other non-automated, hand-carried credentials, such as driver's licenses and badges. Access authorization to computers and data has traditionally been based on identities authenticated through user-selected passwords. More recently, cryptographic mechanisms and biometric techniques have been used in physical and logical security applications, replacing or supplementing the traditional identity credentials.

The strength of the authentication that is achieved varies, depending upon the type of credential, the process used to issue the credential, and the authentication mechanism used to validate the credential. This document establishes a standard for a Personal Identity Verification (PIV) system based on secure and reliable forms of identity credentials issued by the Federal government to its employees and contractors. These credentials are intended to authenticate individuals who require access to Federally controlled facilities, information systems, and applications. This Standard addresses requirements for initial identity proofing, infrastructures to support interoperability of identity credentials, and accreditation of organizations and processes issuing PIV credentials.

1.1 Purpose

This Standard defines a reliable, government-wide identity credential for use in applications such as access to Federally controlled facilities and information systems. This Standard has been developed within the context and constraints of Federal law, regulations, and policy based on currently available and evolving information processing technology.

This Standard specifies a PIV system within which a common identity credential can be created and later used to verify a claimed identity. The Standard also identifies Federal government-wide requirements for security levels that are dependent on risks to the facility or information being protected.

1.2 Scope

Homeland Security Presidential Directive-12 [HSPD-12], signed by President George W. Bush on August 27, 2004, established the requirements for a common identification standard for identity credentials issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. HSPD-12 directs the Department of Commerce to develop a Federal Information Processing Standards (FIPS) publication to define such a common identity credential. In accordance with HSPD-12, this Standard defines the technical requirements for the identity credential that—

- (a) is issued based on sound criteria for verifying an individual employee's identity;
- (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
- (c) can be rapidly authenticated electronically; and

(d) is issued only by providers whose reliability has been established by an official accreditation process.

This Standard defines authentication mechanisms offering varying degrees of security for both logical and physical access applications. Federal departments and agencies will determine the level of security and authentication mechanisms appropriate for their applications. This Standard does not specify access control policies or requirements for Federal departments and agencies. Therefore, the scope of this Standard is limited to authentication of an individual's identity. Authorization and access control decisions are outside the scope of this Standard. Moreover, requirements for a temporary card used until a new or replacement PIV Card arrives are out of scope of this Standard.

1.3 Change Management

Every revision of this Standard introduces refinements and changes that may impact existing implementations. FIPS 201 and its normative specifications encourage implementation approaches that reduce the high cost of configuration and change management by architecting resilience to change into system processes and components. Nevertheless, changes and modifications are introduced. Because of the importance of this issue, this Change Management section has been added to the Standard.

This section provides change management principles and guidance to implementers of relying systems to manage newly introduced changes and modifications to the previous version of this Standard. Specifically, this section provides a description of the types of changes expected in FIPS 201 revisions.

1.3.1 Backward Compatible Change

A backward compatible change is a change or modification to an existing feature that does not break the relying systems using this feature. For example, changing the Card Authentication certificate from optional to mandatory does not affect the systems using the Card Authentication certificate for authentication (i.e., using the PKI-CAK authentication mechanism).

1.3.2 Non-Backward Compatible Change

A non-backward compatible change is a change or modification to an existing feature such that the modified feature cannot be used with existing relying systems. For example, changing the format of the biometric data would not be compatible with the existing system, because a biometric authentication attempt with the modified format would fail. Similarly, changing the PIV Card Application IDentifier (AID) would introduce a non-backward compatible change. As a result, all systems interacting with the PIV Card would need to be changed to accept the new PIV AID.

1.3.3 New Features

New features are optional or mandatory features that are added to the Standard. New features do not interfere with backward compatibility because they are not part of the existing relying systems. For example, the addition of an optional on-card biometric comparison (OCC) authentication mechanism is a new feature that does not affect the features in current systems. The systems will need to be updated if an agency decides to support the OCC-AUTH authentication mechanism.

1.3.4 Deprecated and Removed

When a feature is to be discontinued or is no longer needed, it is deprecated. In general, a feature that is currently in use by relying systems would only be deprecated if there were a compelling (e.g., security) reason to do so. Deprecated features may continue to be used, but should be phased out in future systems since the feature will likely be removed in the next revision of the Standard. For example, the CHUID

authentication mechanism (Section 6.2.5) has been deprecated, since it provides LITTLE or NO assurance in the identity of the cardholder, and so relying systems should phase out use of this authentication mechanism.²

In the case of deprecated features on PIV Cards, such as the authentication key map, existing PIV Cards with the deprecated features remain valid, however, new PIV Cards should not include the deprecated features.

1.3.5 FIPS 201 Version Management

Subsequent revisions of this Standard may necessitate FIPS 201 version management that introduces new version numbers for FIPS 201 products. Components that may be affected by version management include, for example, PIV Cards, PIV middleware software, and card issuance systems.

New version numbers will be assigned in [SP 800-73], if needed, based on the nature of the change. For example, new mandatory features introduced in a revision of this Standard may necessitate a new PIV Card Application version number so that systems can quickly discover the new mandatory features. Optional features, on the other hand, may be discoverable by an on-card discovery mechanism.

1.4 Document Organization

This Standard describes the minimum requirements for a Federal personal identification system that meets the control and security objectives of [HSPD-12], including identity proofing, registration, and issuance. It provides detailed technical specifications to support the control and security objectives of [HSPD-12] as well as interoperability among Federal departments and agencies. This Standard describes the policies and minimum requirements of a PIV Card that allows interoperability of credentials for physical and logical access. The physical card characteristics, storage media, and data elements that make up identity credentials are specified in this Standard. The interfaces and card architecture for storing and retrieving identity credentials from a smart card are specified in Special Publication 800-73 [SP 800-73], *Interfaces for Personal Identity Verification*. Similarly, the requirements for collection and formatting of biometric information are specified in Special Publication 800-76 [SP 800-76], *Biometric Specifications for Personal Identity Verification*. The requirements for cryptographic algorithms are specified in Special Publication 800-78 [SP 800-78], *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*. The requirements for the accreditation of PIV Card issuers are specified in Special Publication 800-79 [SP 800-79], *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*. The unique organizational codes for Federal agencies are assigned in Special Publication 800-87 [SP 800-87], *Codes for the Identification of Federal and Federally-Assisted Organizations*. The requirements for the PIV Card reader are provided in Special Publication 800-96 [SP 800-96], *PIV Card to Reader Interoperability Guidelines*. The format for encoding the chain-of-trust for import and export is specified in Special Publication 800-156 [SP 800-156], *Representation of PIV Chain-of-Trust for Import and Export*. The requirements for issuing derived PIV credentials are specified in Special Publication 800-157 [SP 800-157], *Guidelines for Derived Personal Identity Verification (PIV) Credentials*.

This Standard contains normative references to other documents, and to the extent described in each citation these documents are included by reference in this Standard. Should normative text in this Standard conflict with normative text in a referenced document the normative text in this Standard prevails for this Standard.

² The CHUID data element has not been deprecated and continues to be mandatory.

All sections in this document are *normative* (i.e., mandatory for compliance) unless specified as *informative* (i.e., non-mandatory). Following is the structure of this document:

- + Section 1, Introduction, provides background information for understanding the scope of this Standard. This section is *informative*.
- + Section 2, Common Identification, Security, and Privacy Requirements, outlines the requirements for identity proofing, registration, and issuance, by establishing the control and security objectives for compliance with [HSPD-12]. This section is *normative*.
- + Section 3, PIV System Overview, serves to provide a PIV system overview. This section is *informative*.
- + Section 4, PIV Front-End Subsystem, provides the requirements for the components of the PIV front-end subsystem. Specifically, this section defines requirements for the PIV Card, logical data elements, biometrics, cryptography, and card readers. This section is *normative*.
- + Section 5, PIV Key Management Requirements, defines the processes and components required for managing a PIV Card's lifecycle. It also provides the requirements and specifications related to this subsystem. This section is *normative*.
- + Section 6, PIV Cardholder Authentication, defines a suite of authentication mechanisms that are supported by the PIV Card, and their applicability in meeting the requirements of graduated levels of identity assurance. This section is *normative*.
- + Appendix A, PIV Validation, Certification, and Accreditation, provides additional information regarding compliance with this document. This appendix is *normative*.
- + Appendix B, PIV Object Identifiers and Certificate Extension, provides additional details for the PIV objects identified in Section 4. This appendix is *normative*.
- + Appendix C, Glossary of Terms, Acronyms, and Notations, describes the vocabulary and textual representations used in the document. This appendix is *informative*.
- + Appendix D, References, lists the specifications and standards referred to in this document. This appendix is *informative*.
- + Appendix E, Revision History, lists changes made to this Standard from its inception. This appendix is *informative*.

2. Common Identification, Security, and Privacy Requirements

This section addresses the fundamental control and security objectives outlined in [HSPD-12], including the identity proofing requirements for Federal employees and contractors.

2.1 Control Objectives

[HSPD-12] established control objectives for secure and reliable identification of Federal employees and contractors. These control objectives, provided in paragraph 3 of the directive, are quoted here:

(3) "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process.

Each agency's PIV implementation shall meet the four control objectives (a) through (d) listed above such that—

- + Credentials are issued 1) to individuals whose identity has been verified and 2) after a proper authority has authorized issuance of the credential.
- + A credential is issued only after National Agency Check with Written Inquiries (NACI) (or equivalent or higher) or Tier 1 or higher federal background investigation is initiated³ and the Federal Bureau of Investigation (FBI) National Criminal History Check (NCHC) portion of the background investigation is completed.
- + An individual is issued a credential only after presenting two identity source documents, at least one of which is a Federal or State government issued picture ID.
- + Fraudulent identity source documents are not accepted as genuine and unaltered.
- + A person suspected or known to the government as being a terrorist is not issued a credential.
- + No substitution occurs in the identity proofing process. More specifically, the individual who appears for identity proofing, and whose fingerprints are checked against databases, is the person to whom the credential is issued.
- + No credential is issued unless requested by proper authority.
- + A credential remains serviceable only up to its expiration date. More precisely, a revocation process exists such that expired or invalidated credentials are swiftly revoked.
- + A single corrupt official in the process may not issue a credential with an incorrect identity or to a person not entitled to the credential.
- + An issued credential is not duplicated or forged, and is not modified by an unauthorized entity.

³ The initiation of a background investigation is defined as the submission of the investigative request to the Office of Personnel Management (OPM), or other Federal background investigation service provider (if authorized).

2.2 Credentialing Requirements

Federal departments and agencies shall use the credentialing guidance issued by the Director of the Office of Personnel Management (OPM)⁴ and OMB⁵.

2.3 Biometric Data Collection for Background Investigations

The following biometric data shall be collected from each PIV applicant:

- + A full set of fingerprints. Biometric identification using fingerprints is the primary input to law enforcement checks. In cases where ten fingerprints are not available, then as many fingers as possible shall be imaged. In cases where obtaining any fingerprints is impossible, agencies shall seek OPM guidance for alternative means of performing the law enforcement checks.

This collection is not necessary for applicants who have a completed and favorably adjudicated NACI (or equivalent or higher) or Tier 1 or higher federal background investigation on record that can be located and referenced.

Fingerprint collection shall conform to the procedural and technical specifications of [SP 800-76].

2.4 Biometric Data Collection for PIV Card

The following biometric data shall be collected from each PIV applicant:

- + Two fingerprints, for off-card comparison. These shall be taken either from the full set of fingerprints collected in Section 2.3, or collected independently.
- + An electronic facial image.

The following biometric data may optionally be collected from a PIV applicant:

- + One or two iris images.
- + Two fingerprints, for on-card comparison. It is recommended that these be different than the fingerprints collected for off-card comparison.

If the biometric data that is collected as specified in this section and in Section 2.3 is collected on separate occasions, then a 1:1 biometric match of the applicant shall be performed at each visit against biometric data collected during a previous visit.

Biometric data collection shall conform to the procedural and technical specifications of [SP 800-76]. The choice of which two fingers is important and may vary between persons. The recommended selection and order is specified in [SP 800-76].

2.5 Biometric Data Use

The full set of fingerprints shall be used for one-to-many identification in the databases of fingerprints maintained by the FBI.

⁴ For example, [SPRINGER MEMO] at http://www.opm.gov/investigate/resources/final_credentialing_standards.pdf and the Federal Investigative Standards.

⁵ For example, [OMB0524] at <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf>.

The two mandatory fingerprints shall be used for preparation of templates to be stored on the PIV Card as described in Section 4.2.3.1. The fingerprints provide an interagency-interoperable authentication mechanism through a match-off-card scheme as described in Section 6.2.1. These fingerprints are also the primary means of authentication during PIV issuance and maintenance processes.

The optional fingerprints may be used for preparation of the fingerprint templates for on-card comparison as described in Section 4.2.3.1. OCC may be used to support card activation as described in Section 4.3.1. OCC may also be used for cardholder authentication (OCC-AUTH) as described in Section 6.2.2.

The electronic iris images may be stored on the PIV Card as described in Section 4.2.3.1. Agencies may choose to collect iris biometrics as a second biometric to support multimodal authentication to improve accuracy, operational suitability, to accommodate user preferences, or as a backup when the fingerprint biometric is unavailable.

The electronic facial image:

- + shall be stored on the PIV Card as described in Section 4.2.3.1;
- + shall be printed on the PIV Card according to Section 4.1.4.1;
- + may be used for generating a visual image on the monitor of a guard workstation for augmenting the visual authentication process defined in Section 6.2.6; and
- + may be used for automated facial authentication in operator-attended PIV issuance, reissuance, and verification data reset processes.

2.6 Chain-of-Trust

A card issuer may optionally maintain, for each PIV Card issued, a documentary chain-of-trust for the identification data it collects. The chain-of-trust is a sequence of related enrollment data records that are created and maintained through the methods of contemporaneous acquisition of data within each enrollment data record, and biometric matching of samples between enrollment data records.⁶

It is recommended that the following data be included in the chain-of-trust:

- + A log of activities that documents who took the action, what action was taken, when and where the action took place, and what data was collected.
- + An enrollment data record that contains the most recent collection of each of the biometric data collected. The enrollment data record describes the circumstances of biometric acquisition including the name and role of the acquiring agent, the office and organization, time, place, and acquisition method. The enrollment data record may also document unavailable biometric data or failed attempts to collect biometric data. The enrollment data record may contain historical biometric data.
- + The most recent unique identifiers (i.e., Federal Agency Smart Credential Number (FASC-N) and Universally Unique IDentifier (UUID)) issued to the individual. The record may contain historical unique identifiers.
- + Information about the authorizing entity who has approved the issuance of a credential.

⁶ For example, ten fingerprints for law enforcement checks may be collected at one time and place, and two fingerprints for PIV Card templates may be collected at a later time and different place, provided that the two fingerprints are verified as among the ten original fingerprints.

- + Current status of the background investigation, including the results of the investigation once completed.
- + The evidence of authorization if the credential is issued under a pseudonym.
- + Any data or any subsequent changes in the data about the cardholder. If the changed data is the cardholder's name, then the issuer should include the evidence of a formal name change.

The biometric data in the chain-of-trust shall be valid for at most 12 years. In order to mitigate ageing effects and thereby maintain operational readiness of a cardholder's PIV Card, agencies may require biometric enrollment more frequently than 12 years.

The chain-of-trust contains personally identifiable information (PII). If implemented, it shall be protected in a manner that protects the individual's privacy and maintains the integrity of the chain-of-trust record both in transit and at rest. A card issuer may import and export a chain-of-trust in the manner and representation described in [SP 800-156].

The chain-of-trust can be applied in several situations to include:

- + **Extended enrollment:** a PIV applicant enrolls a full set of fingerprints for background investigations at one place and time, and two fingerprints for the PIV Card at another place and time. The chain-of-trust would contain identifiers and two enrollment data records, one with a full-set fingerprint transaction, and one with two fingerprint templates. The two fingerprint templates would be matched against the corresponding fingers in the ten-fingerprint data set to link the chain.
- + **Reissuance:** a PIV cardholder loses his/her card. Since the card issuer has biometric enrollment data records, the cardholder can perform a 1:1 biometric match to reconnect to the card issuer's chain-of-trust. The card issuer need not repeat the identity proofing and registration process. The card issuer proceeds to issue a new card as described in Section 2.9.1.
- + **Interagency transfer:** a Federal employee is transferred from one agency to another. When the employee leaves the old agency, he/she surrenders the PIV Card and it is destroyed. When the employee arrives at the new agency and is processed in, the card issuer in the new agency requests the employee's chain-of-trust from the card issuer in the old agency, and receives the chain-of-trust. The employee performs a 1:1 biometric match against the chain-of-trust, and the interaction proceeds as described in Section 2.8.2.

2.7 PIV Identity Proofing and Registration Requirements

Departments and agencies shall follow an identity proofing and registration process that meets the requirements defined below when issuing PIV Cards.

- + The organization shall adopt and use an identity proofing and registration process that is approved in accordance with [SP 800-79].
- + Biometrics shall be captured as specified in Sections 2.3 and 2.4.
- + The process shall begin by locating and referencing a completed and favorably adjudicated NACI (or equivalent or higher) or Tier 1 or higher federal background investigation record. In the absence of a record, the process shall ensure 1) the initiation of a Tier 1 or higher federal background investigation and 2) the completion of the National Agency Check (NAC)⁷ of the background investigation. In cases where

⁷ The NAC is an automated record check.

the NAC results are not received within 5 days of the NAC initiation, the FBI NCHC (fingerprint check) portion of the NAC shall be complete before PIV Card issuance.

- + The applicant shall appear in-person at least once before the issuance of a PIV Card.
- + During identity proofing, the applicant shall be required to provide two forms of identity source documents in original form.⁸ The identity source documents shall be bound to that applicant and shall be neither expired nor cancelled. If the two identity source documents bear different names, evidence of a formal name change shall be provided. The primary identity source document shall be one of the following forms of identification:
 - a U.S. Passport or a U.S. Passport Card;
 - a Permanent Resident Card or an Alien Registration Receipt Card (Form I-551);
 - a foreign passport;
 - an Employment Authorization Document that contains a photograph (Form I-766);
 - a Driver's license or an ID card issued by a state or possession of the United States provided it contains a photograph;
 - a U.S. Military ID card;
 - a U.S. Military dependent's ID card; or
 - a PIV Card.

The secondary identity source document may be from the list above, but cannot be of the same type as the primary identity source document.⁹ The secondary identity source document may also be one of the following:

- a U.S. Social Security Card issued by the Social Security Administration;
- an original or certified copy of a birth certificate issued by a state, county, municipal authority, possession, or outlying possession of the United States bearing an official seal;
- an ID card issued by a federal, state, or local government agency or entity, provided it contains a photograph;
- a voter's registration card;
- a U.S. Coast Guard Merchant Mariner Card;
- a Certificate of U.S. Citizenship (Form N-560 or N-561);
- a Certificate of Naturalization (Form N-550 or N-570);
- a U.S. Citizen ID Card (Form I-197);

⁸ Departments and agencies may choose to accept only a subset of the identity source documents listed in this section. For example, in cases where identity proofing for PIV Card issuance is performed prior to verification of employment authorization, departments and agencies may choose to require the applicant to provide identity source documents that satisfy the requirements of Form I-9, *Employment Eligibility Verification*, in addition to the requirements specified in this section. It is recommended that departments and agencies perform electronic verification of identity source documents, where possible.

⁹ For example, if the primary source document is a foreign passport (e.g., Italy), the secondary source document should not be another foreign passport (e.g., France).

- an Identification Card for Use of Resident Citizen in the United States (Form I-179);
 - a Certification of Birth Abroad or Certification of Report of Birth issued by the Department of State (Form FS-545 or Form DS-1350);
 - a Temporary Resident Card (Form I-688);
 - an Employment Authorization Card (Form I-688A);
 - a Reentry Permit (Form I-327);
 - a Refugee Travel Document (Form I-571);
 - an Employment authorization document issued by Department of Homeland Security (DHS);
 - an Employment Authorization Document issued by DHS with photograph (Form I-688B);
 - a driver's license issued by a Canadian government entity; or
 - a Native American tribal document.
- + The PIV identity proofing, registration, issuance, and reissuance processes shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV Card without the cooperation of another authorized person.

The identity proofing and registration process used when verifying the identity of the applicant shall be accredited by the department or agency as satisfying the requirements above and approved in writing by the head or deputy secretary (or equivalent) of the Federal department or agency.

The requirements for identity proofing and registration also apply to citizens of foreign countries who are working for the Federal government overseas. However, a process for identity proofing and registration must be established using a method approved by the U.S. Department of State's Bureau of Diplomatic Security, except for employees under the command of a U.S. area military commander. These procedures may vary depending on the country.

2.8 PIV Card Issuance Requirements

Departments and agencies shall meet the requirements defined below when issuing PIV Cards. The issuance process used when issuing PIV Cards shall be accredited by the department or agency as satisfying the requirements below and approved in writing by the head or deputy secretary (or equivalent) of the Federal department or agency.

- + PIV Cards are issued after a proper authority has authorized issuance of the credential.
- + The organization shall use an approved PIV credential issuance process in accordance with [SP 800-79].
- + Before issuing the PIV Card, the process shall ensure that a previously completed and favorably adjudicated NACI (or equivalent or higher) or Tier 1 or higher federal background investigation is on record. In the absence of a record, the required federal background investigation shall be initiated.¹⁰ The PIV Card should not be issued before the results of the NAC are complete. However, if the results of the NAC have not been received in 5 days, the PIV Card may be issued based on the FBI NCHC. In the absence of an FBI NCHC

¹⁰ The identity management system (IDMS) should reflect the adjudication status of each PIV cardholder.

(e.g., due to unclassifiable fingerprints) the NAC results are required prior to issuing a PIV Card. The PIV Card shall be terminated if the results of the background investigation so justify.

- + Biometrics used to personalize the PIV Card must be those captured during the identity proofing and registration process.
- + During the issuance process, the issuer shall verify that the individual to whom the PIV Card is to be issued is the same as the intended applicant/recipient as approved by the appropriate authority. Before the card is provided to the applicant, the issuer shall perform a 1:1 biometric match of the applicant against biometrics available on the PIV Card or in the chain-of-trust. The 1:1 biometric match requires either a match of fingerprint(s) or, if unavailable, other optional biometric data that are available. Minimum accuracy requirements for the biometric match are specified in [SP 800-76]. On successful match, the PIV Card shall be released to the applicant. If the match is unsuccessful, or if no biometric data is available, the cardholder shall provide two identity source documents (as specified in Section 2.7), and an attending operator shall inspect these and compare the cardholder with the facial image printed on the PIV Card.
- + The organization shall issue PIV credentials only through systems and providers whose reliability has been established by the agency and so documented and approved in writing (i.e., accredited) in accordance with [SP 800-79].
- + The PIV Card shall be valid for no more than six years.

PIV Cards that contain topographical defects (e.g., scratches, poor color, fading, etc.) or that are not properly printed shall be destroyed. The PIV Card issuer is responsible for the card stock, its management, and its integrity.

2.8.1 Special Rule for Pseudonyms

In limited circumstances Federal employees and contractors are permitted to use pseudonyms during the performance of their official duties with the approval of their employing agency. If an agency determines that use of a pseudonym is necessary to protect an employee or contractor (e.g., from physical harm, severe distress, or harassment),¹¹ the agency may formally authorize the issuance of a PIV Card to the employee or contractor using the agency-approved pseudonym. The issuance of a PIV Card using an authorized pseudonym shall follow the procedures in Section 2.8, PIV Card Issuance Requirements, except that the card issuer must receive satisfactory evidence that the pseudonym is authorized by the agency.

2.8.2 Grace Period

In some instances an individual's status as a Federal employee or contractor will lapse for a brief time period. For example, a Federal employee may leave one Federal agency for another Federal agency and thus occur a short employment lapse period, or an individual who was under contract to a Federal agency may receive a new contract from that agency shortly after the previous contract expired. In these instances, the card issuer may issue a new PIV Card without repeating the identity proofing and

¹¹ See, for example, Section 10.5.7 of the Internal Revenue Service Manual (<http://www.irs.gov/irm/index.html>), which authorizes approval by an employee's supervisor of the use of a pseudonym to protect the employee's personal safety.

registration process if the issuer has access to the applicant's chain-of-trust record and the applicant can be reconnected to the chain-of-trust record.¹²

When issuing a PIV Card under the grace period, the card issuer shall verify that PIV Card issuance has been authorized by a proper authority and that the employee's or contractor's background investigation is valid. Re-investigations shall be performed if required, in accordance with OPM guidance. At the time of issuance, the card issuer shall perform a 1:1 biometric match of the applicant to reconnect to the chain-of-trust. The 1:1 biometric match requires either a match of fingerprint(s) or, if unavailable, other optional biometric data that are available. On successful match, the new PIV Card shall be released to the applicant. If the match is unsuccessful, or if no biometric data is available, the cardholder shall provide two identity source documents (as specified in Section 2.7), and an attending operator shall inspect these and compare the cardholder with the facial image retrieved from the enrollment data record and the facial image printed on the new PIV Card.

2.9 PIV Card Maintenance Requirements

The PIV Card shall be maintained using processes that comply with this section.

The data and credentials held by the PIV Card may need to be updated or invalidated prior to the expiration date of the card. The cardholder may change his or her name, retire, or change jobs; or the employment may be terminated, thus requiring invalidation of a previously issued card. In this regard, procedures for PIV Card maintenance must be integrated into department and agency procedures to ensure effective card maintenance. In order to maintain operational readiness of a cardholder's PIV Card, agencies may require PIV Card update, reissuance, or biometric enrollment more frequently than the maximum PIV Card and biometric lifetimes stated in this Standard. Shorter lifetimes may be specified by agency policy collectively, or on a case-by-case basis as sub-par operation is encountered.

2.9.1 PIV Card Reissuance Requirements

Reissuance is the process by which a new PIV Card is issued to a cardholder without the need to repeat the entire identity proofing and registration procedure. The reissuance process may be used to replace a PIV Card that is nearing expiration, in the event of an employee status or attribute change, or to replace a PIV Card that has been compromised, lost, stolen, or damaged. The cardholder may also apply for reissuance of a PIV Card if one or more logical credentials have been compromised. The entire identity proofing, registration, and issuance process, as described in Sections 2.7 and 2.8, shall be repeated if the issuer does not maintain a chain-of-trust record for the cardholder or if the reissuance process was not started before the old PIV Card expired.

If the expiration date of the new PIV Card is later than the expiration date of the old card, or if any data about the cardholder is being changed, the card issuer shall ensure that a proper authority has authorized the issuance of the new PIV Card. The issuer shall ensure that the proper authority has verified that the employee's or contractor's background investigation is valid before reissuing the card and associated credentials.¹³ If the expiration date of the new PIV Card is later than the expiration date of the old card then re-investigations shall be performed if required, in accordance with OPM guidance.

The issuer shall perform a 1:1 biometric match of the applicant to reconnect to the chain-of-trust. The 1:1 biometric match requires either a match of fingerprint(s) or, if unavailable, other optional biometric data

¹² For the purposes of this section, a lapse is considered to be brief if it is not long enough to require that a new background investigation be performed. OPM currently requires a new background investigation to be performed when there has been a break in service of greater than two years.

¹³ The identity management system (IDMS) should reflect the adjudication status of each PIV cardholder.

that are available (either on the PIV Card or in the chain-of-trust). Minimum accuracy requirements for the biometric match are specified in [SP 800-76]. On successful match, the new PIV Card shall be released to the applicant. If the match is unsuccessful, or if no biometric data is available, the cardholder shall provide two identity source documents (as specified in Section 2.7), and an attending operator shall inspect these and compare the cardholder with the facial image retrieved from the enrollment data record and the facial image printed on the new PIV Card.

The old PIV Card shall be revoked when the new PIV Card is issued:

- + The old PIV Card shall be collected and destroyed, if possible.
- + Any databases maintained by the PIV Card issuer that contain FASC-N or UUID values from the old PIV Card must be updated to reflect the change in status.
- + If the old PIV Card cannot be collected and destroyed, or if the old PIV Card has been compromised or damaged, then the certification authority (CA) shall be informed and the certificates corresponding to the PIV Authentication key and asymmetric Card Authentication key on the old PIV Card shall be revoked. If present, the certificates corresponding to the digital signature key and the key management key shall also be revoked.

In the case of a lost, stolen, or compromised card, normal revocation procedures shall be completed within 18 hours of notification. In certain cases, 18 hours is an unacceptable delay and in those cases emergency procedures must be executed to disseminate the information as rapidly as possible. Departments and agencies are required to have procedures in place to issue emergency notifications in such cases.

If there is any data change about the cardholder, the issuer will record this in the chain-of-trust, if applicable. If the changed data is the cardholder's name, then the issuer shall meet the requirements in Section 2.9.1.1, Special Rule for Name Change by Cardholder.

Previously collected biometric data may be reused with the new PIV Card if the expiration date of the new PIV Card is no later than 12 years after the date that the biometric data was obtained. As biometric authentication accuracy degrades with the time elapsed since initial collection, issuers may elect to refresh the biometric data after reconnecting the applicant to their chain-of-trust. Even if the same biometric data is reused with the new PIV Card, the digital signature must be recomputed with the new FASC-N and UUID.

A new PIV Authentication certificate and a new Card Authentication certificate shall be generated. The corresponding certificates shall be populated with the new FASC-N and UUID. For cardholders who are required to have a digital signature certificate, a new digital signature certificate shall also be generated. Key management key(s) and certificate(s) may be imported to the new PIV Card.

2.9.1.1 Special Rule for Name Change by Cardholder

Name changes frequently occur as a result of marriage, divorce, or as a matter of personal preference. In the event that a cardholder notifies a card issuer that his or her name has changed, and presents the card issuer with evidence of a formal name change, such as a marriage certificate, a divorce decree, judicial recognition of a name change, or other mechanism permitted by State law or regulation, the card issuer shall issue the cardholder a new card following the procedures set out in Section 2.9.1, PIV Card Reissuance Requirements. If the expiration date of the new card is no later than the expiration date of the old PIV Card and no data about the cardholder, other than the cardholder's name, is being changed, then

the new PIV Card may be issued without obtaining the approval of a proper authority and without performing a re-investigation.

2.9.2 PIV Card Post Issuance Update Requirements

A PIV Card post issuance update may be performed without replacing the PIV Card in cases where none of the printed information on the surface of the card is changed. The post issuance update applies to cases where one or more certificates, keys, biometric data objects, or signed data objects are updated. A post issuance update shall not modify the PIV Card expiration date, FASC-N, or UUID.

A PIV Card post issuance update may be done locally (performed with the issuer in physical custody of the PIV Card) or remotely (performed with the PIV Card at a remote location). Post issuance updates shall be performed with issuer security controls equivalent to those applied during PIV Card reissuance. For remote post issuance updates, the following shall apply:

- + Communication between the PIV Card issuer and the PIV Card shall occur only over mutually authenticated secure sessions between tested and validated cryptographic modules (one being the PIV Card).
- + Data transmitted between the PIV Card issuer and PIV Card shall be encrypted and contain data integrity checks.
- + The PIV Card Application will communicate with no end point entity other than the PIV Card issuer during the remote post issuance update.

Post issuance updates to biometric data objects, other than to the digital signature blocks within the biometric data objects, shall satisfy the requirements for verification data reset specified in Section 2.9.3.

If the PIV Authentication key, asymmetric Card Authentication key, the digital signature key, or the key management key, was compromised, the corresponding certificate shall be revoked.

2.9.3 PIV Card Verification Data Reset

The Personal Identification Number (PIN) on a PIV Card may need to be reset if the cardholder has forgotten the PIN or if PIN-based cardholder authentication has been disabled from the usage of an invalid PIN more than the allowed number of retries stipulated by the department or agency.¹⁴ PIN reset may be performed in-person at the issuer's facility, at an unattended kiosk operated by the issuer, or remotely via a general computing platform:

- + When PIN reset is performed in-person at the issuer's facility, before providing the reset PIV Card back to the cardholder, the issuer shall perform a 1:1 biometric match to ensure that the cardholder's biometric matches either the stored biometric on the PIV Card or biometric data stored in the chain-of-trust. In cases where a biometric match is not possible, the cardholder shall provide the PIV Card to be reset and another primary identity source document (as specified in Section 2.7). An attending operator shall inspect these and compare the cardholder with the facial image retrieved from the enrollment data record and the facial image printed on the card.
- + PIN reset at an unattended issuer-operated kiosk shall ensure that the PIV Card is authenticated and that the cardholder's biometric matches either the stored biometric on the PIV Card, through an on-card 1:1 biometric match, or biometric data stored in the chain-of-trust, through an off-card 1:1

¹⁴ Cardholders may change their PINs anytime by providing the current PIN and the new PIN values.

biometric match. If the biometric match or card authentication is unsuccessful, the kiosk shall not reset the PIV Card.

- + Remote PIN reset on a general computing platform (e.g., desktop, laptop) shall only be performed if the following requirements are met:
 - o the cardholder initiates a PIN reset with the issuer operator;
 - o the operator authenticates the owner of the PIV Card through an out-of-band authentication procedure (e.g., pre-registered knowledge tokens); and
 - o the cardholder's biometric matches the stored biometric on the PIV Card through a 1:1 on-card biometric comparison.

The remote PIN reset operation shall satisfy the requirements for remote post issuance updates specified in Section 2.9.2.

Departments and agencies may adopt more stringent procedures for PIN reset (including disallowing PIN reset). PIN reset procedures shall be formally documented by each department and agency.

Verification data other than the PIN may also be reset (i.e., re-enrollment) by the card issuer. Before the reset, the issuer shall perform a 1:1 biometric match of the cardholder to reconnect to the chain-of-trust. The type of biometric used for the match shall not be the same as the type of biometric data that is being reset. For example, if fingerprint templates for on-card comparison are being reset, then a 1:1 iris match could be used to reconnect to the chain-of-trust. If no alternative biometric data is available, the cardholder shall provide the PIV Card to be reset and another primary identity source document (as specified in Section 2.7). An attending operator shall inspect these and compare the cardholder with the facial image retrieved from the enrollment data record and the facial image printed on the PIV Card.

New verification reference data shall be enrolled. The PIV Card's activation methods associated with the verification data shall be reset and the new verification data shall be stored on the card.

Departments and agencies may adopt more stringent procedures for verification data reset (including disallowing verification data reset); such procedures shall be formally documented by each department and agency.

2.9.4 PIV Card Termination Requirements

A PIV card is terminated when the department or agency that issued the card determines that the cardholder is no longer eligible to have a PIV Card. The PIV Card shall be terminated under the following circumstances:

- + a Federal employee separates (voluntarily or involuntarily) from Federal service;
- + a contractor changes positions and no longer needs access to Federal buildings or systems;
- + a cardholder passes away;
- + a determination is made after completion of a cardholder's background investigation that the cardholder should not have a PIV Card; or
- + a cardholder is determined to hold a fraudulent identity.

Similar to the situation in which the card or a credential is compromised, normal termination procedures must be in place as to ensure the following:

- + The PIV Card itself is revoked:
 - o The PIV Card shall be collected and destroyed, if possible.
 - o Any databases maintained by the PIV Card issuer that indicate current valid (or invalid) FASC-N or UUID values must be updated to reflect the change in status.
 - o If the PIV Card cannot be collected and destroyed, the CA shall be informed and the certificates corresponding to the PIV Authentication key and the asymmetric Card Authentication key on the PIV Card shall be revoked. The certificates corresponding to the digital signature and key management keys shall also be revoked, if present.
- + The PII collected from the cardholder is disposed of in accordance with the stated privacy and data retention policies of the department or agency.

If the card cannot be collected, normal termination procedures shall be completed within 18 hours of notification. In certain cases, 18 hours is an unacceptable delay and in those cases emergency procedures must be executed to disseminate the information as rapidly as possible. Departments and agencies are required to have procedures in place to issue emergency notifications in such cases.

2.10 Derived PIV Credentials Issuance Requirements

Valid PIV Cards may be used as the basis for issuing derived PIV credentials in accordance with NIST Special Publication 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials* [SP 800-157]. When a cardholder's PIV Card is terminated as specified in Section 2.9.4, any derived PIV credentials issued to the cardholder shall also be terminated.

2.11 PIV Privacy Requirements

HSPD-12 explicitly states that “protect[ing] personal privacy” is a requirement of the PIV system. As such, all departments and agencies shall implement the PIV system in accordance with the spirit and letter of all privacy controls specified in this Standard, as well as those specified in Federal privacy laws and policies including but not limited to the E-Government Act of 2002 [E-Gov], the Privacy Act of 1974 [PRIVACY], and OMB Memorandum M-03-22 [OMB0322], as applicable.

Departments and agencies may have a wide variety of uses of the PIV system and its components that were not intended or anticipated by the President in issuing [HSPD-12]. In considering whether a proposed use of the PIV system is appropriate, departments and agencies shall consider the aforementioned control objectives and the purpose of this Standard, namely “to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy” [HSPD-12]. No department or agency shall implement a use of the identity credential inconsistent with these control objectives.

To ensure the privacy throughout PIV lifecycle, departments and agencies shall do the following:

- Assign an individual to the role of privacy official.¹⁵ The privacy official is the individual who oversees privacy-related matters in the PIV system and is responsible for implementing the privacy

¹⁵ Privacy official refers to the Senior Agency Official for Privacy (SAOP) or Chief Privacy Officer (CPO).

requirements in the Standard. The individual serving in this role shall not assume any other operational role in the PIV system.

- Conduct a comprehensive Privacy Impact Assessment (PIA) on systems containing PII for the purpose of implementing PIV, consistent with the methodology of [E-Gov] and the requirements of [OMB0322]. Consult with appropriate personnel responsible for privacy issues at the department or agency (e.g., Chief Information Officer) implementing the PIV system.
- Write, publish, and maintain a clear and comprehensive document listing the types of information that will be collected (e.g., transactional information, PII), the purpose of collection, what information may be disclosed to whom during the life of the credential, how the information will be protected, and the complete set of uses of the credential and related information at the department or agency. Provide PIV applicants full disclosure of the intended uses of the information associated with the PIV Card and the related privacy implications.
- Assure that systems that contain PII for the purpose of enabling the implementation of PIV are handled in full compliance with fair information practices as defined in [PRIVACY].
- Maintain appeals procedures for those who are denied a credential or whose credentials are revoked.
- Ensure that only personnel with a legitimate need for access to PII in the PIV system are authorized to access the PII, including but not limited to information and databases maintained for registration and credential issuance.¹⁶
- Coordinate with appropriate department or agency officials to define consequences for violating privacy policies of the PIV system.
- Assure that the technologies used in the department or agency's implementation of the PIV system allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information in the operation of the program.
- Utilize security controls described in [SP 800-53], *Recommended Security Controls for Federal Information Systems*, to accomplish privacy goals, where applicable.
- Ensure that the technologies used to implement PIV sustain and do not erode privacy protections relating to the use, collection, and disclosure of PII. Agencies may choose to deploy PIV Cards with electromagnetically opaque holders or other technology to protect against any unauthorized contactless access to information stored on a PIV Card.

¹⁶ Agencies may refer to NIST SP 800-122 [SP 800-122], *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, for a best practice guideline on protection of PII.

3. PIV System Overview

The PIV system is composed of components and processes that support a common (smart card-based) platform for identity authentication across Federal departments and agencies for access to multiple types of physical and logical access environments. The specifications for the PIV components in this Standard promote uniformity and interoperability among the various PIV system components, across departments and agencies, and across installations. The specifications for processes in this Standard are a set of minimum requirements for the various activities that need to be performed within an operational PIV system. When implemented in accordance with this Standard, the PIV Card supports a suite of authentication mechanisms that can be used consistently across departments and agencies. The authenticated identity information can then be used as a basis for access control in various Federal physical and logical access environments. The following sections briefly discuss the functional components of the PIV system and the lifecycle activities of the PIV Card.

3.1 Functional Components

An operational PIV system can be logically divided into the following three major subsystems:

- **PIV Front-End Subsystem**—PIV Card, card and biometric readers, and PIN input device. The PIV cardholder interacts with these components to gain physical or logical access to the desired Federal resource.
- **PIV Card Issuance and Management Subsystem**—the components responsible for identity proofing and registration, card and key issuance and management, and the various repositories and services (e.g., public key infrastructure (PKI) directory, certificate status servers) required as part of the verification infrastructure.
- **PIV Relying Subsystem**—the physical and logical access control systems, the protected resources, and the authorization data.

The PIV relying subsystem becomes relevant when the PIV Card is used to authenticate a cardholder who is seeking access to a physical or logical resource. Although this Standard does not provide technical specifications for this subsystem, various mechanisms for identification and authentication are defined in Section 6 to provide consistent and secure means for performing the authentication function preceding an access control decision.

Figure 3-1 illustrates a notional model for the operational PIV system, identifying the various system components and the direction of data flow between these components. The boundary shown in the figure is not meant to preclude FIPS 201 requirements on systems outside these boundaries.

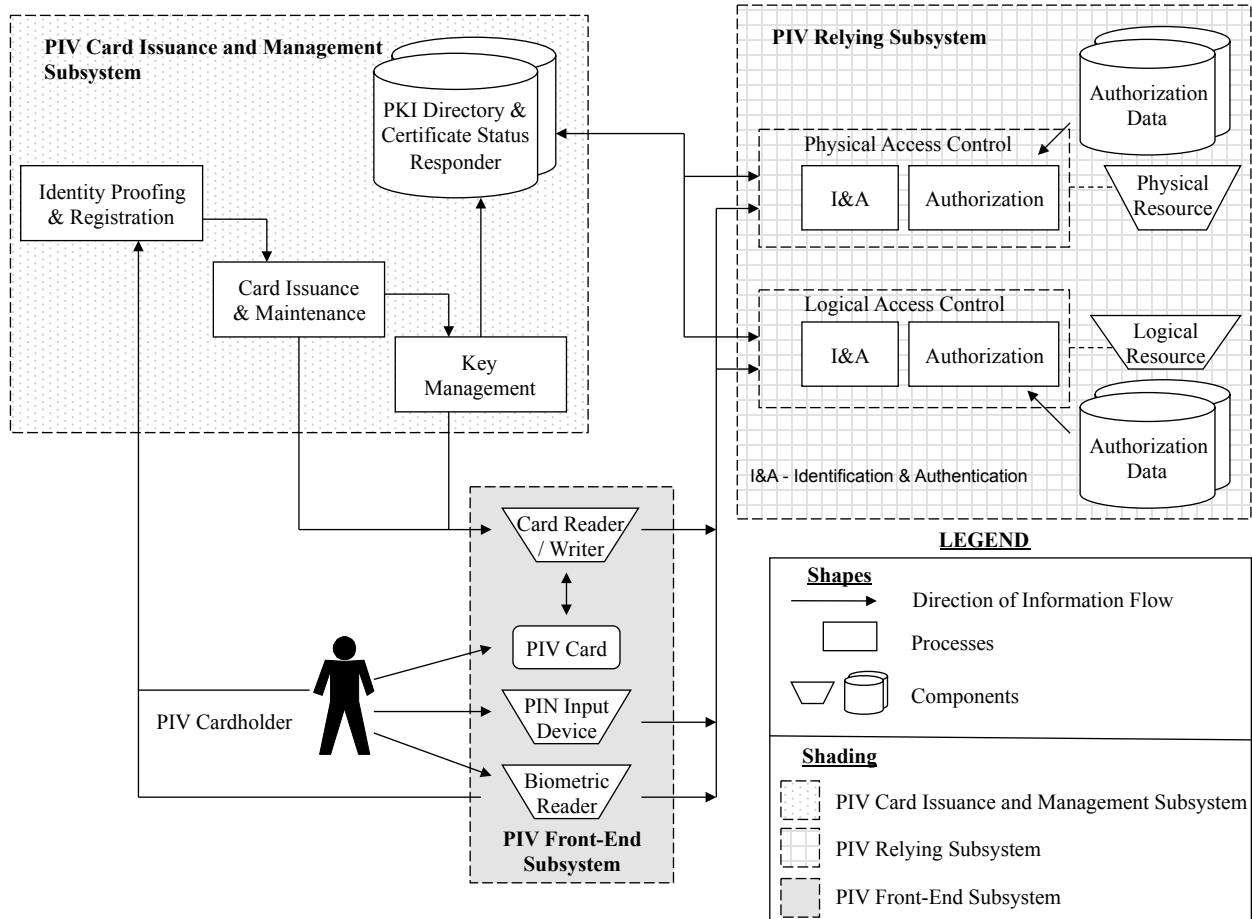


Figure 3-1. PIV System Notional Model

3.1.1 PIV Front-End Subsystem

The PIV Card will be issued to the applicant when all identity proofing, registration, and issuance processes have been completed. The PIV Card has a credit card-size form factor, with one or more embedded integrated circuit chips (ICC) that provide memory capacity and computational capability. The PIV Card is the primary component of the PIV system. The holder uses the PIV Card for authentication to various physical and logical resources.

Card readers are located at access points for controlled resources where a cardholder may wish to gain access (physical and logical) by using the PIV Card. The reader communicates with the PIV Card to retrieve the appropriate information, located in the card’s memory, to relay it to the access control systems for granting or denying access.

Card writers, which are very similar to the card readers, personalize and initialize the information stored on PIV Cards. Card writers may also be used to perform remote PIV Card updates (see Section 2.9.2). The data to be stored on PIV Cards includes personal information, certificates, cryptographic keys, the PIN, and biometric data, and is discussed in further detail in subsequent sections.

PIN input devices can be used along with card readers when a higher level of authentication assurance is required. The cardholder presenting the PIV Card must type in his or her PIN into the PIN input device. For physical access, the PIN is typically entered using a PIN pad device; a keyboard is generally used for

logical access. The input of a PIN provides a “something you know”¹⁷ authentication factor that activates¹⁸ the PIV Card and enables access to other credentials resident on the card that provide additional factors of authentication. A cryptographic key and certificate, for example, provides an additional authentication factor of “something you have” (i.e., the card) through PKI-based authentication.

Biometric readers may be located at secure locations where a cardholder may want to gain access. These readers depend upon the use of biometric data of the cardholder, stored in the memory of the card, and its comparison with a real-time biometric sample. The use of biometrics provides an additional factor of authentication (“something you are”) in addition to entering the PIN (“something you know”) and providing the card (“something you have”) for cryptographic key-based authentication. This provides for a higher level of authentication assurance.

3.1.2 PIV Card Issuance and Management Subsystem

The identity proofing and registration component in Figure 3-1 refers to the process of collecting, storing, and maintaining all information and documentation that is required for verifying and assuring the applicant’s identity. Various types of information are collected from the applicant at the time of registration.

The card issuance and maintenance component deals with the personalization of the physical (visual surface) and logical (contents of the ICC) aspects of the card at the time of issuance and maintenance thereafter. This includes printing photographs, names, and other information on the card and loading the relevant card applications, biometrics, and other data.

The key management component is responsible for the generation of key pairs, the issuance and distribution of digital certificates containing the public keys of the cardholder, and management and dissemination of certificate status information. The key management component is used throughout the lifecycle of PIV Cards—from generation and loading of authentication keys and PKI credentials, to usage of these keys for secure operations, to eventual reissuance or termination of the card. The key management component is also responsible for the provisioning of publicly accessible repositories and services (such as PKI directories and certificate status responders) that provide information to the requesting application about the status of the PKI credentials.

3.1.3 PIV Relying Subsystem

The PIV relying subsystem includes components responsible for determining a particular PIV cardholder’s access to a physical or logical resource. A physical resource is the secured facility (e.g., building, room, parking garage) that the cardholder wishes to access. The logical resource is typically a network or a location on the network (e.g., computer workstation, folder, file, database record, software program) to which the cardholder wants to gain access.

The authorization data component comprises information that defines the privileges (authorizations) possessed by entities requesting to access a particular logical or physical resource. An example of this is an access control list (ACL) associated with a file on a computer system.

The physical and logical access control system grants or denies access to a particular resource and includes an identification and authentication (I&A) component as well as an authorization component.

¹⁷ For more information on the terms “something you know,” “something you have,” and “something you are,” see [SP 800-63].

¹⁸ Alternatively, on-card biometric comparison can be used to activate the PIV Card.

The I&A component interacts with the PIV Card and uses mechanisms discussed in Section 6 to identify and authenticate cardholders. Once authenticated, the I&A component passes information to the authorization component which in turn interacts with the authorization data component to match the cardholder information to the information on record. Access control components typically interface with the card reader, the PIN input device, the biometric reader, supplementary databases, and any certificate status service.

3.2 PIV Card Lifecycle Activities

The PIV Card lifecycle consists of seven activities. The activities that take place during fabrication and pre-personalization of the card at the manufacturer are not considered a part of this lifecycle model. Figure 3-2 presents these PIV activities and depicts the PIV Card request as the initial activity and PIV Card termination as the end of life.

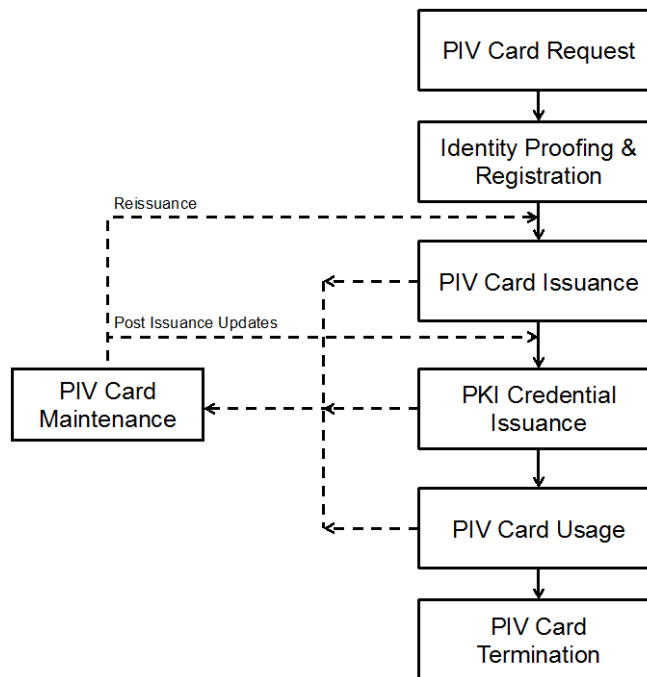


Figure 3-2. PIV Card Lifecycle Activities

Descriptions of the seven card lifecycle activities are as follows:

- **PIV Card Request.** This activity applies to the initiation of a request for the issuance of a PIV Card to an applicant and the validation of this request.
- **Identity Proofing and Registration.** The goal of this activity is to verify the claimed identity of the applicant, verify that the entire set of identity source documents presented at the time of registration is valid, capture biometrics, and optionally create the chain-of-trust record.
- **PIV Card Issuance.** This activity deals with the personalization (physical and logical) of the card and the issuance of the card to the intended applicant.
- **PKI Credential Issuance.** This activity deals with generating logical credentials and loading them onto the PIV Card.

- **PIV Card Usage.** During this activity, the PIV Card is used to perform cardholder authentication for access to a physical or logical resource. Access authorization decisions are made after successful cardholder identification and authentication.
- **PIV Card Maintenance.** This activity deals with the maintenance or update of the physical card and the data stored thereon. Such data includes various card applications, PINs, PKI credentials, and biometrics.
- **PIV Card Termination.** The termination process is used to permanently destroy or invalidate the PIV Card and the data and keys needed for authentication so as to prevent any future use of the card for authentication.

4. PIV Front-End Subsystem

This section identifies the requirements for the components of the PIV front-end subsystem. Section 4.1 provides the physical card specifications. Section 4.2 provides the logical card specifications. Section 4.3 specifies the requirements for card activation. Section 4.4 provides requirements for PIV Card readers.

4.1 PIV Card Physical Characteristics

References to the PIV Card in this section pertain to the physical characteristics only. References to the front of the card apply to the side of the card that contains the electronic contacts; references to the back of the card apply to the opposite side from the front side.

The PIV Card's physical appearance and other characteristics should balance the need to have the PIV Card commonly recognized as a Federal identification card while providing the flexibility to support individual department and agency requirements. Having a common look for PIV Cards is important in meeting the objectives of improved security and interoperability. In support of these objectives, consistent placement of printed components and technology is generally necessary.

The PIV Card shall comply with physical characteristics as described in International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 7810 [ISO7810], ISO/IEC 10373 [ISO10373], ISO/IEC 7816 for contact cards [ISO7816], and ISO/IEC 14443 for contactless cards [ISO14443].

4.1.1 Printed Material

The printed material shall not rub off during the life of the PIV Card, nor shall the printing process deposit debris on the printer rollers during printing and laminating. Printed material shall not interfere with the contact and contactless ICC(s) and related components, nor shall it obstruct access to machine-readable information.

4.1.2 Tamper Proofing and Resistance

The PIV Card shall contain security features that aid in reducing counterfeiting, are resistant to tampering, and provide visual evidence of tampering attempts. At a minimum, a PIV Card shall incorporate one such security feature. Examples of these security features include the following:

- optical varying structures;
- optical varying inks;
- laser etching and engraving;
- holograms;
- holographic images; and
- watermarks.

Incorporation of security features shall—

- be in accordance with durability requirements;

- be free of defects, such as fading and discoloration;
- not obscure printed information; and
- not impede access to machine-readable information.

Departments and agencies may incorporate additional tamper-resistance and anti-counterfeiting methods. As a generally accepted security procedure, Federal departments and agencies are strongly encouraged to periodically review the viability, effectiveness, and currency of employed tamper resistance and anti-counterfeiting methods.

4.1.3 Physical Characteristics and Durability

The following list describes the physical requirements for the PIV Card.

- The PIV Card shall contain a contact and a contactless ICC interface.
- The card body shall be white in accordance with color representation in Section 4.1.5. Only a security feature, as described in Section 4.1.2, may modify the perceived color slightly. Presence of a security feature shall not prevent the recognition of white as the principal card body color by a person with normal vision (corrected or uncorrected) at a working distance of 50 cm to 200 cm.
- The card body structure shall consist of card material(s) that satisfy the card characteristics in [ISO7810] and test methods in American National Standards Institute (ANSI) 322 [ANSI322]. Although the [ANSI322] test methods do not currently specify compliance requirements, the tests shall be used to evaluate card material durability and performance. The [ANSI322] tests minimally shall include card flexure, static stress, plasticizer exposure, impact resistance, card structural integrity, surface abrasion, temperature and humidity-induced dye migration, ultraviolet light exposure, and a laundry test. Cards shall not malfunction or delaminate after hand cleaning with a mild soap and water mixture.
- The card shall be subjected to actual, concentrated, or artificial sunlight to appropriately reflect 2000 hours of southwestern United States' sunlight exposure in accordance with [ISO10373], Section 5.12. Concentrated sunlight exposure shall be performed in accordance with [G90-98] and accelerated exposure in accordance with [G155-00]. After exposure, the card shall be subjected to the [ISO10373] dynamic bending test and shall have no visible cracks or failures. Alternatively, the card may be subjected to the [ANSI322] tests for ultraviolet and daylight fading resistance and subjected to the same [ISO10373] dynamic bending test.
- There are methods by which proper card orientation can be indicated. Section 4.1.4.3, for example, defines Zones 21F and 22F, where card orientation features may be applied.¹⁹ Note: If an agency determines that tactilely discernible markers for PIV Cards imposes an undue burden, the agency must implement policies and procedures to accommodate employees and contractors with disabilities in accordance with Sections 501 and 504 of the Rehabilitation Act.
- The card shall be 27- to 33-mil thick (before lamination) in accordance with [ISO7810].
- The PIV Card shall not be embossed.
- Decals shall not be adhered to the card.

¹⁹ For some individuals, the contact surface for the ICC may be sufficient for determining the orientation of the card.

- Departments and agencies may choose to punch an opening in the card body to enable the card to be oriented by touch or to be worn on a lanyard. Departments and agencies should ensure such alterations are closely coordinated with the card vendor and/or manufacturer to ensure the card material integrity and printing process is not adversely impacted. Departments and agencies are strongly encouraged to ensure such alterations do not—
 - compromise card body durability requirements and characteristics;
 - invalidate card manufacturer warranties or other product claims;
 - alter or interfere with printed information, including the photo; or
 - damage or interfere with machine-readable technology, such as the embedded antenna.
- The card material shall withstand the effects of temperatures required by the application of a polyester laminate on one or both sides of the card by commercial off-the-shelf (COTS) equipment. The thickness added due to a laminate layer shall not interfere with the smart card reader operation. The card material shall allow production of a flat card in accordance with [ISO7810] after lamination of one or both sides of the card.

The PIV Card may be subjected to additional testing.

4.1.4 Visual Card Topography

The information on a PIV Card shall be in visual printed and electronic form. This section covers the placement of visual and printed information. It does not cover information stored in electronic form, such as stored data elements, and other possible machine-readable technologies. Logically stored data elements are discussed in Section 4.2.

As noted in Section 4.1.3, the PIV Card shall contain a contact and a contactless ICC interface. This Standard does not specify whether a single chip is used or multiple chips are used to support the mandated contact and contactless interfaces.

To achieve a common PIV Card appearance, yet provide departments and agencies the flexibility to augment the card with department or agency-specific requirements, the card shall contain mandated and optional printed information and mandated and optional machine-readable technologies. Mandated and optional items shall generally be placed as described and depicted. Printed data shall not interfere with machine-readable technology.

Areas that are marked as reserved should not be used for printing. The reason for the recommended reserved areas is that placement of the embedded contactless ICC module may vary from manufacturer to manufacturer, and there are constraints that prohibit printing over the embedded contactless module. The PIV Card topography provides flexibility for placement of the embedded module, either in the upper right-hand corner or in the lower bottom portion. Printing restrictions apply only to the area where the embedded module is located (i.e., upper right-hand corner, lower bottom portion).

Because technological developments may obviate the need to have a restricted area, or change the size of the restricted area, departments and agencies are encouraged to work closely with card vendors and manufacturers to ensure current printing procedures and methods are applied as well as potential integration of features that may improve tamper resistance and anti-counterfeiting of the PIV Card.




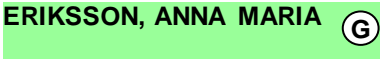

4.1.4.1 Mandatory Items on the Front of the PIV Card

Zone 1F—Photograph. The photograph shall be placed in the upper left corner, as depicted in Figure 4-1, and be a full frontal pose from top of the head to shoulder. A minimum of 300 dots per inch (dpi) resolution shall be used. The background should follow recommendations set forth in [SP 800-76].

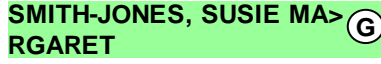
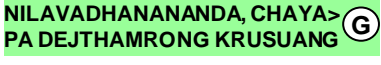
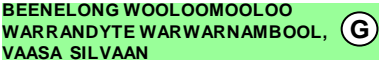
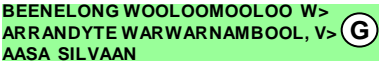
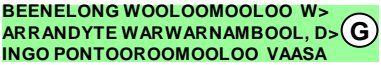
Zone 2F—Name. The full name²⁰ shall be printed directly under the photograph in capital letters. The full name shall be composed of a Primary Identifier (i.e., surnames or family names) and a Secondary Identifier (i.e., pre-names or given names). The printed name shall match the name on the identity source documents provided during identity proofing and registration to the extent possible. The full name shall be printed in the <Primary Identifier>, <Secondary Identifier> format. The entire full name should be printed on available lines of Zone 2F and either identifier could be wrapped. The wrapped identifier shall be indicated with “>” character at the end of the line. The identifiers may be printed on separate lines if each fits on one line. Departments and agencies shall use the largest font size of 7 to 10 points that allows the full name to be printed. The font size 7 point allows space for 3 lines and shall only be used if the full name does not fit on two lines with font size 8 point. Table 4-1 provides examples of separate Primary and Secondary Identifier lines, single line with identifiers, wrapped full names, and full name in three lines. Note that the truncation should only occur if the full name cannot be printed in 7 point font.

Names in the Primary Identifier and the first name in the Secondary Identifier shall not be abbreviated. Other names and conventional prefixes and suffixes, which shall be included in the Secondary Identifier, may be abbreviated. The special character “.” (period) shall indicate such abbreviations, as shown in Figure 4-2. Other uses of special symbols (e.g., “O’BRIEN”) are at the discretion of the issuer.

Table 4-1. Name Examples

<p>Name: John Doe</p> <p>Characteristics: simple full name of individual who does not have a middle name, two lines sufficient with 10 points.</p>	
<p>Name: Anna Maria Eriksson</p> <p>Characteristics: simple full name, two lines sufficient with 10 points.</p>	
<p>Name: Anna Maria Eriksson</p> <p>Characteristics: simple full name with abbreviated middle name, two lines sufficient with 10 points.</p>	
<p>Name: Anna Maria Eriksson</p> <p>Characteristics: simple full name, one line sufficient for full name with 10 points.</p>	
<p>Name: Susie Margaret Smith-Jones</p> <p>Characteristics: longer full name in two lines, sufficient space in 10 points.</p>	

²⁰ Alternatively, an authorized pseudonym as provided under the law as discussed in Section 2.8.1.

<p>Name: Susie Margaret Smith-Jones Characteristics: longer full name wrapped, two lines sufficient with 10 points.</p>	
<p>Name: Chayapa Dejthamrong Krusuang Nilavadhanananda Characteristics: longer full name wrapped, two lines NOT sufficient with 10 points. Reduce the font size to 8 points.</p>	
<p>Name: Vaasa Silvaan Beenelong Wooloomooloo Warrantyte Warwarnambool Characteristics: longer full name, two lines NOT sufficient with 8 point, 7 point allows sufficient space for three lines in Zone 2F.</p>	
<p>Name: Vaasa Silvaan Beenelong Wooloomooloo Warrantyte Warwarnambool Characteristics: same as previous but full name is wrapped.</p>	
<p>Name: Dingo Pontooroomooloo Vaasa Silvaan Beenelong Wooloomooloo Warrantyte Warwarnambool Characteristics: truncated full name, three lines with 7 point NOT sufficient.</p>	

Zone 8F—Employee Affiliation. An employee affiliation shall be printed on the card as depicted in Figure 4-1. Some examples of employee affiliation are “Employee,” “Contractor,” “Active Duty,” and “Civilian.”

Zone 10F—Agency, Department, or Organization. The organizational affiliation shall be printed as depicted in Figure 4-1.

Zone 14F—Card Expiration Date. The card expiration date shall be printed on the card as depicted in Figure 4-1. The card expiration date shall be in a YYYYMMDD format whereby the MMM characters represent the three-letter month abbreviation as follows: JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, and DEC. The Zone 14F expiration date shall be printed in Arial 6 to 9 point bold.

Zone 15F—Color-Coding for Employee Affiliation. Color-coding shall be used for additional identification of employee affiliation as a background color for Zone 2F (name) as depicted in Figures 4-1 and 4-4. The following color scheme shall be used:

- Blue—Foreign National
- White—Government Employee

- Green—Contractor.

Foreign National color-coding has precedence over Government Employee and Contractor color-coding. These colors shall be reserved and shall not be employed for other purposes. Also, these colors shall be printed in accordance to the color specifications provided in Section 4.1.5. Zone 15F may be a solid or patterned line at the department or agency's discretion.

Zone 18F—Affiliation Color Code. The affiliation color code “B” for Blue, “W” for White, or “G” for Green shall be printed in a white circle in Zone 15F as depicted in Figure 4-1. The diameter of the circle shall not be more than 5 mm. Note that the lettering shall correspond to the printed color in Zone 15F.

Zone 19F—Card Expiration Date. The card expiration date shall be printed in a MMMYYYY format in the upper right-hand corner as depicted in Figure 4-1. The Zone 19F expiration date shall be printed in Arial 12pt Bold.

4.1.4.2 Mandatory Items on the Back of the PIV Card

Zone 1B—Agency Card Serial Number. This item shall be printed as depicted in Figure 4-6 and contain the unique serial number from the issuing department or agency. The format shall be at the discretion of the issuing department or agency.

Zone 2B—Issuer Identification Number. This item shall be printed as depicted in Figure 4-6 and consist of six characters for the department code, four characters for the agency code, and a five-digit number that uniquely identifies the issuing facility within the department or agency.

4.1.4.3 Optional Items on the Front of the PIV Card

This section contains a description of the optional information and machine-readable technologies that may be used and their respective placement. The storage capacity of all optional technologies is as prescribed by individual departments and agencies and is not addressed in this Standard. Although the items discussed in this section are optional, if used they shall be placed on the card as designated in the examples provided and as noted.

Zone 3F—Signature. If used, the department or agency shall place the cardholder signature below the photograph and cardholder name as depicted in Figure 4-3. The space for the signature shall not interfere with the contact and contactless placement. Because of card surface space constraints, placement of a signature may limit the size of the optional two-dimensional bar code.

Zone 4F—Agency Specific Text Area. If used, this area can be used for printing agency specific requirements, such as employee status, as shown in Figure 4-2.

Zone 5F—Rank. If used, the cardholder's rank shall be printed in the area as illustrated in Figure 4-2. Data format is at the department or agency's discretion.

Zone 6F—Portable Data File (PDF) Two-Dimensional Bar Code. If used, the PDF bar code placement shall be as depicted in Figure 4-2 (i.e., left side of the card). If Zone 3F (a cardholder signature) is used, the size of the PDF bar code may be affected. The card issuer should confirm that a PDF used in conjunction with a PIV Card containing a cardholder signature will satisfy the anticipated PDF data storage requirements.

Zone 9F—Header. If used, the text “United States Government” shall be placed as depicted in Figure 4-4. Departments and agencies may also choose to use this zone for other department or agency-specific information, such as identifying a Federal emergency responder role, as depicted in Figure 4-2.

Zone 11F—Agency Seal. If used, the seal selected by the issuing department, agency, or organization shall be printed in the area depicted. It shall be printed using the guidelines provided in Figure 4-2 to ensure information printed on the seal is legible and clearly visible.

Zone 12F—Footer. The footer is the location for the *Federal Emergency Response Official* identification label. If used, a department or agency may print “Federal Emergency Response Official” as depicted in Figure 4-2, preferably in white lettering on a red background. Departments and agencies may also use Zone 9F to further identify the Federal emergency responder’s official role. Some examples of official roles are “Law Enforcement,” “Fire Fighter,” and “Emergency Response Team (ERT).”

When Zone 15F indicates Foreign National affiliation and the department or agency does not need to highlight emergency response official status, Zone 12F may be used to denote the country or countries of citizenship. If so used, the department or agency shall print the country name or the three-letter country abbreviation (alpha-3 format) in accordance with ISO 3166-1, Country Codes [ISO3166]. Figure 4-4 illustrates an example of Foreign National color-coding using country abbreviations.

Zone 13F—Issue Date. If used, the card issuance date shall be printed above the Zone 14F expiration date in YYYYMMDD format as depicted in Figure 4-3.

Zone 16F—Photo Border. A border may be used with the photo to further identify employee affiliation, as depicted in Figure 4-3. This border may be used in conjunction with Zone 15F to enable departments and agencies to develop various employee categories. The photo border shall not obscure the photo. The border may be a solid or patterned line. For solid and patterned lines, red shall be reserved for emergency response officials, blue for foreign nationals, and green for contractors. All other colors may be used at the department or agency’s discretion.

Zone 17F—Agency Specific Data. In cases in which other defined optional elements are not used, Zone 17F may be used for other department or agency-specific information, as depicted in Figure 4-5.

Zone 20F—Organizational Affiliation Abbreviation. The organizational affiliation abbreviation may be printed in the upper right-hand corner below the Zone 19F expiration date as shown in Figure 4-2. If printed, the organizational affiliation abbreviation shall be printed in Arial 12pt Bold.

Zone 21F—Edge Ridging or Notched Corner Tactile Marker. If used, this area shall incorporate edge ridging or a notched corner to indicate card orientation as depicted in Figure 4-4. Departments and agencies should ensure such alterations are closely coordinated with the card vendor and/or manufacturer to ensure the card material integrity and printing process is not adversely impacted.

Zone 22F—Laser Engraving Tactile Marker. If used, tactilely discernible marks shall be created using laser engraving to indicate card orientation as depicted in Figure 4-4. There shall be an opening in the lamination foil where laser engraving is performed. Departments and agencies should ensure such alterations are closely coordinated with the card vendor and/or manufacturer to ensure the card material integrity and printing process is not adversely impacted.

4.1.4.4 Optional Items on the Back of the PIV Card

Zone 3B—Magnetic Stripe. If used, the magnetic stripe shall be high coercivity and placed in accordance with [ISO7811], as illustrated in Figure 4-7.

Zone 4B—Return Address. If used, the “return if lost” language shall be generally placed on the back of the card as depicted in Figure 4-7.

Zone 5B—Physical Characteristics of Cardholder. If used, the cardholder physical characteristics (e.g., height, eye color, hair color) shall be printed in the general area illustrated in Figure 4-7.

Zone 6B—Additional Language for Emergency Response Officials. Departments and agencies may choose to provide additional information to identify emergency response officials or to better identify the cardholder’s authorized access. If used, this additional text shall be in the general area depicted and shall not interfere with other printed text or machine-readable components. An example of a printed statement is provided in Figure 4-7.

Zone 7B—Standard Section 499, Title 18 Language. If used, standard Section 499, Title 18, language warning against counterfeiting, altering, or misusing the card shall be printed in the general area depicted in Figure 4-7.

Zone 8B—Linear 3 of 9 Bar Code. If used, a linear 3 of 9 bar code shall be generally placed as depicted in Figure 4-7. It shall be in accordance with Association for Automatic Identification and Mobility (AIM) standards. Beginning and end points of the bar code will be dependent on the embedded contactless module selected. Departments and agencies are encouraged to coordinate placement of the bar code with the card vendor.

Zone 9B—Agency-Specific Text. In cases in which other defined optional elements are not used, Zone 9B may be used for other department or agency-specific information, as depicted in Figure 4-8. For example, emergency response officials may use this area to provide additional details.

Zone 10B—Agency-Specific Text. Zone 10B is similar to Zone 9B in that it is another area for providing department or agency-specific information.

For Zones 9B and 10B, departments and agencies are encouraged to use this area prudently and minimize printed text to that which is absolutely necessary.

In the case of the Department of Defense, the back of the card will have a distinct appearance as depicted in Figure 4-8. This is necessary to display information required by the Geneva Accord and to facilitate legislatively mandated medical entitlements.

- All measurements around the figure are in millimeters and are from the top-left corner .
- All text is to be printed using the Arial font.
- Unless otherwise specified, the font size should be 5pt normal weight for data labels (also referred to as tags) and 6pt bold for actual data.

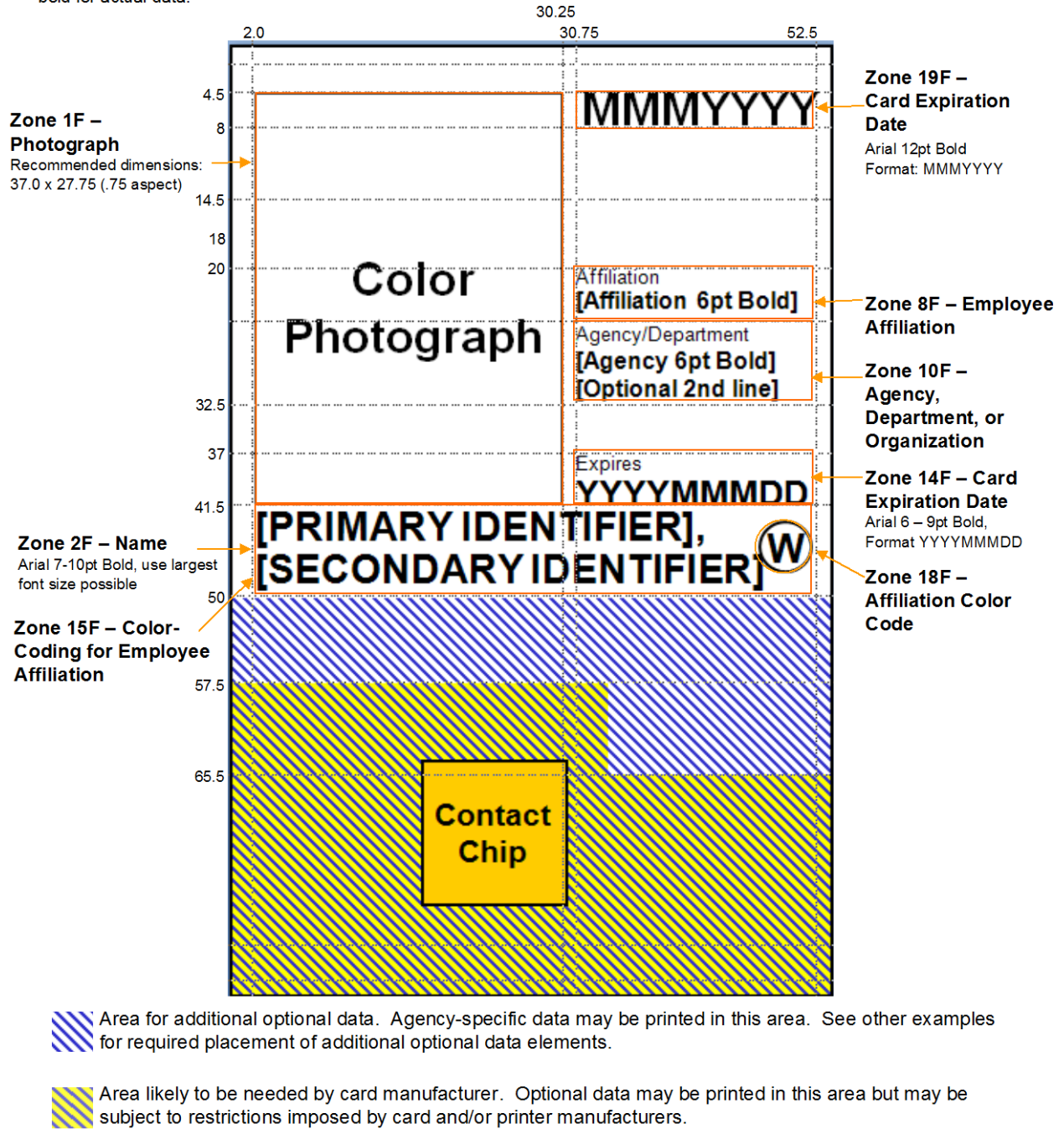


Figure 4-1. Card Front—Printable Areas and Required Data

All measurements around the figure are in millimeters and are from the top-left corner.
 All text is to be printed using the Arial font.
 Unless otherwise specified, the font size should be 5pt normal weight for tags and 6pt bold for data.

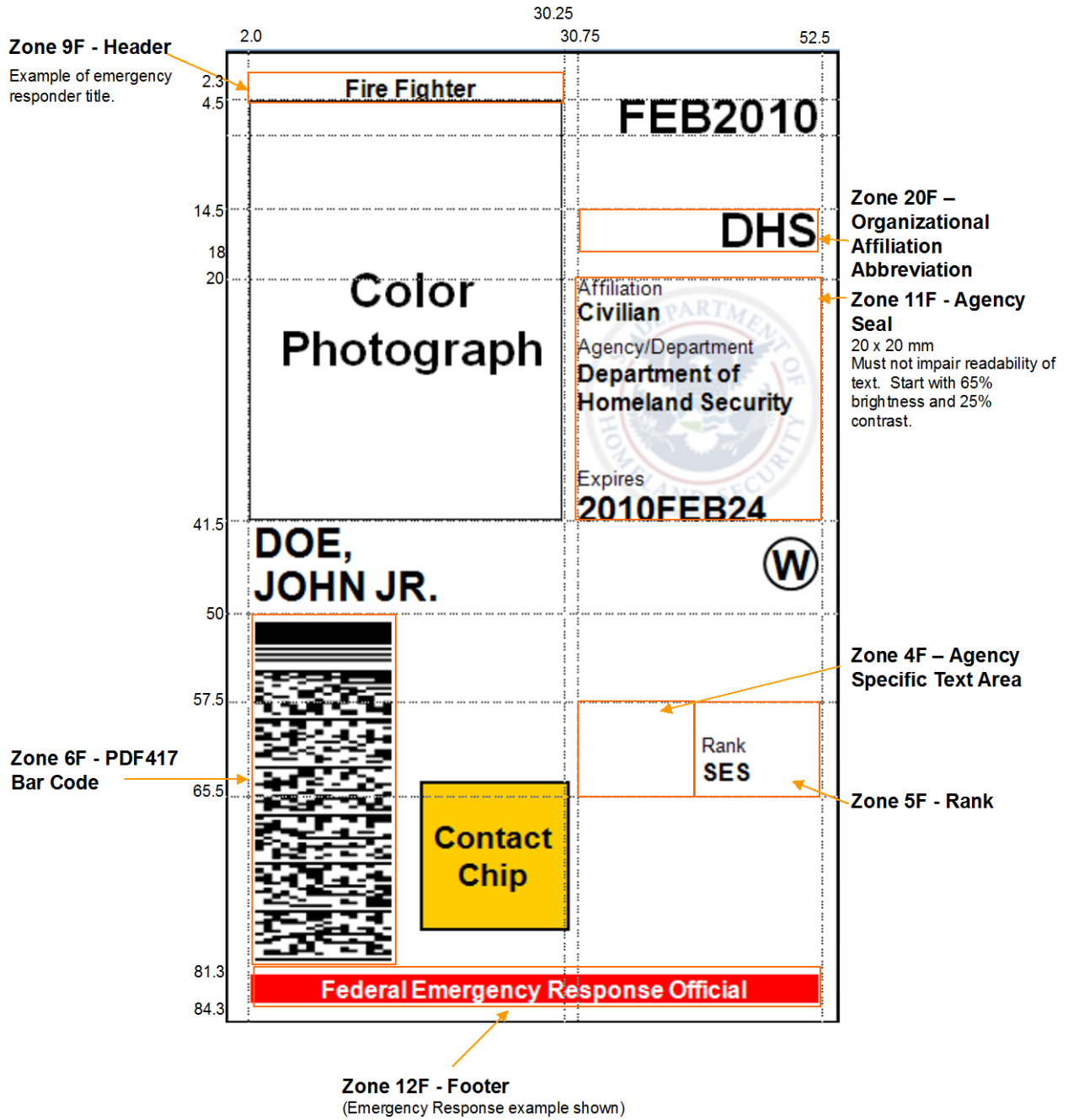


Figure 4-2. Card Front—Optional Data Placement—Example 1

All measurements around the figure are in millimeters and are from the top-left corner.
 All text is to be printed using the Arial font.
 Unless otherwise specified, the font size should be 5pt normal weight for tags and 6pt bold for data.

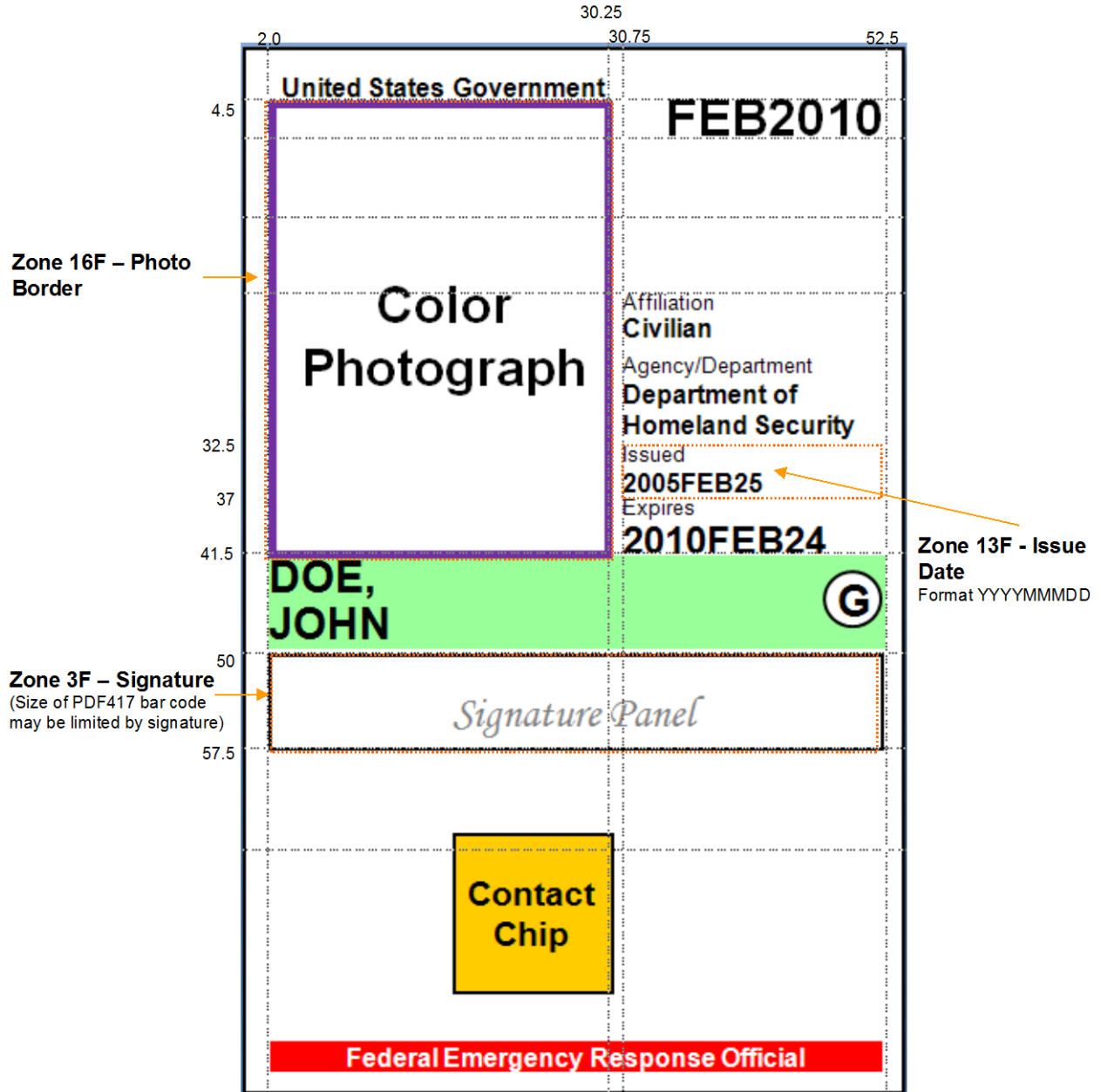


Figure 4-3. Card Front—Optional Data Placement—Example 2

All measurements around the figure are in millimeters and are from the top-left corner.
 All text is to be printed using the Arial font.
 Unless otherwise specified, the font size should be 5pt normal weight for tags and 6pt bold for data.

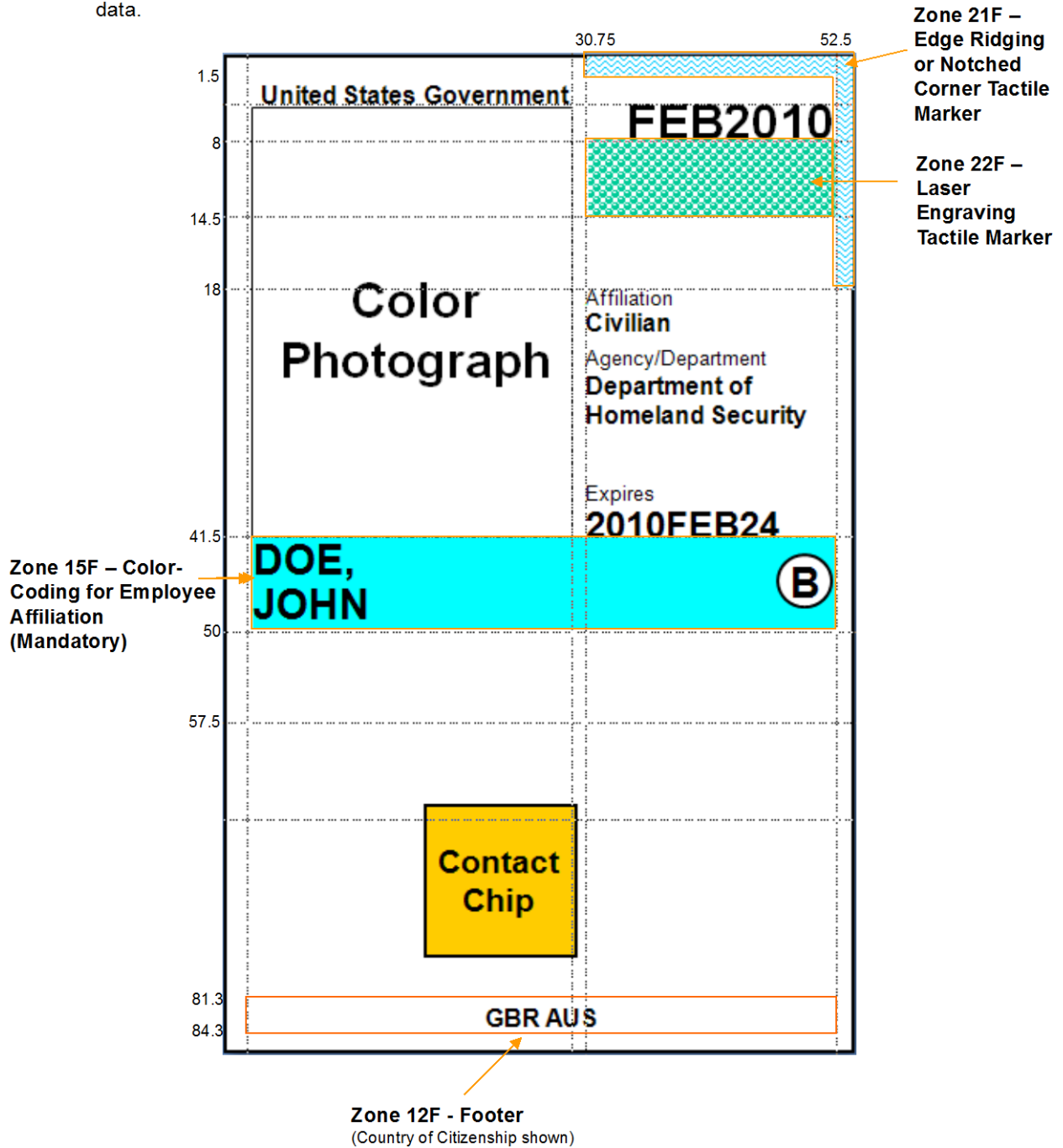


Figure 4-4. Card Front—Optional Data Placement—Example 3

All measurements around the figure are in millimeters and are from the top-left corner.
All text is to be printed using the Arial font.
Unless otherwise specified, the font size should be 5pt normal weight for tags and 6pt bold for data.

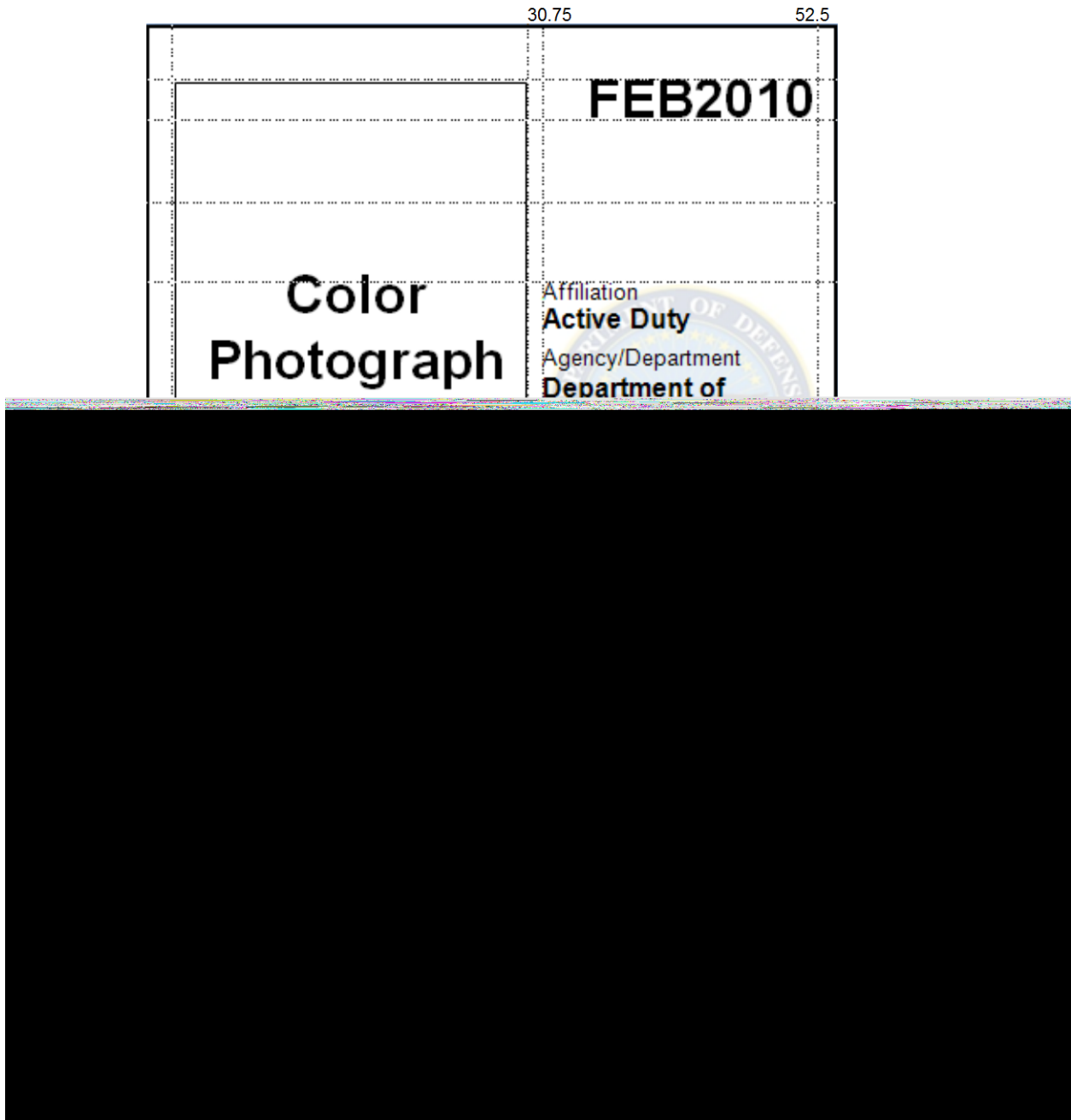
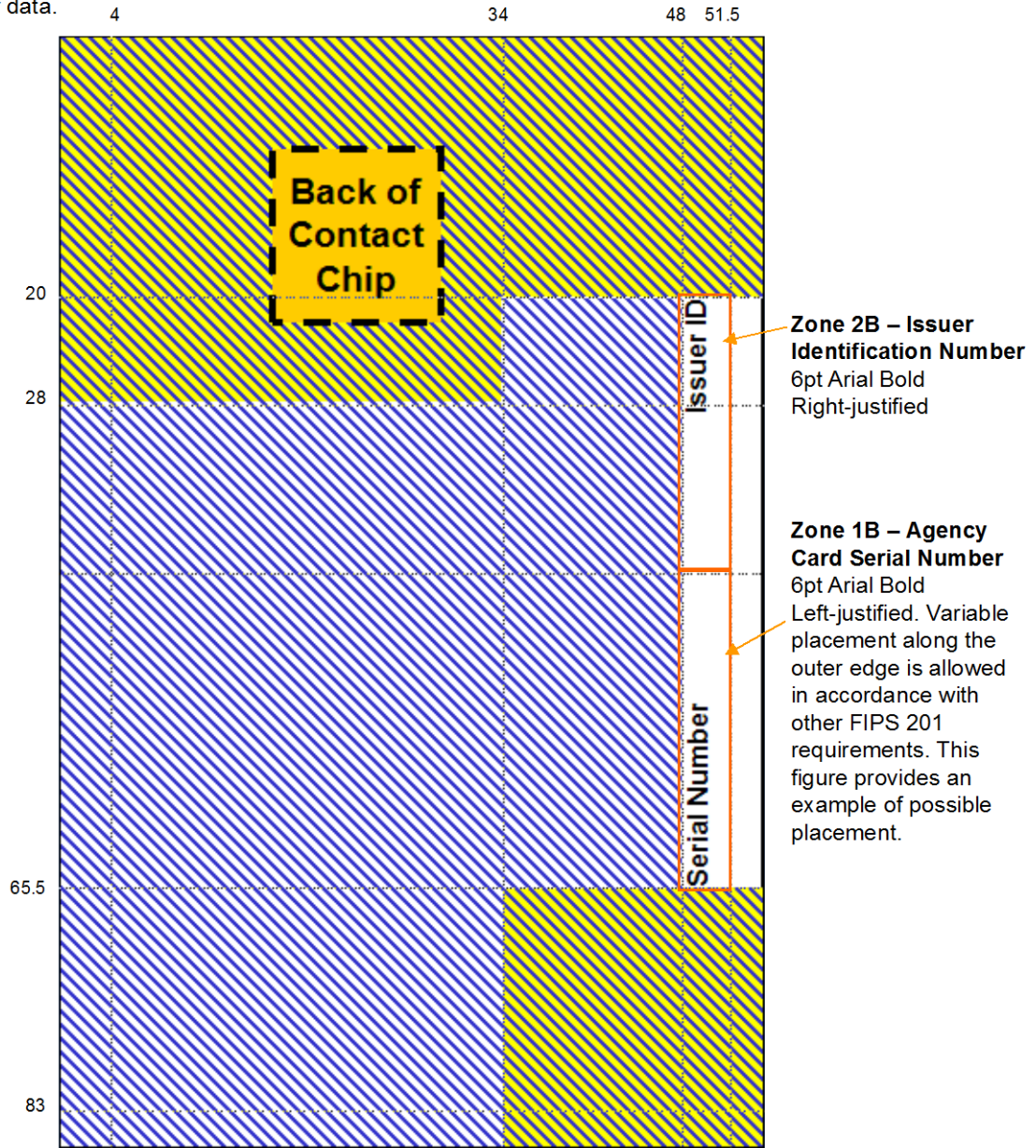



Figure 4-5. Card Front—Optional Data Placement—Example 4

All measurements are in millimeters and are from the top-left corner.
 All text is to be printed using the Arial font.
 Unless otherwise specified, the recommended font size is 5pt normal weight for tags and 6pt bold for data.



 Optional data area. Agency-specific data may be printed in this area. See examples for required placement of optional data elements.


 Optional data area likely to be needed by card manufacturer. Optional data may be printed in this area, but will likely be subject to restrictions imposed by card and/or printer manufacturers.

Figure 4-6. Card Back—Printable Areas and Required Data

All measurements are in millimeters and are from the top-left corner.
 All text is to be printed using the Arial font.
 Unless otherwise specified, the recommended font size is 5pt normal weight for tags and 6pt bold for data.

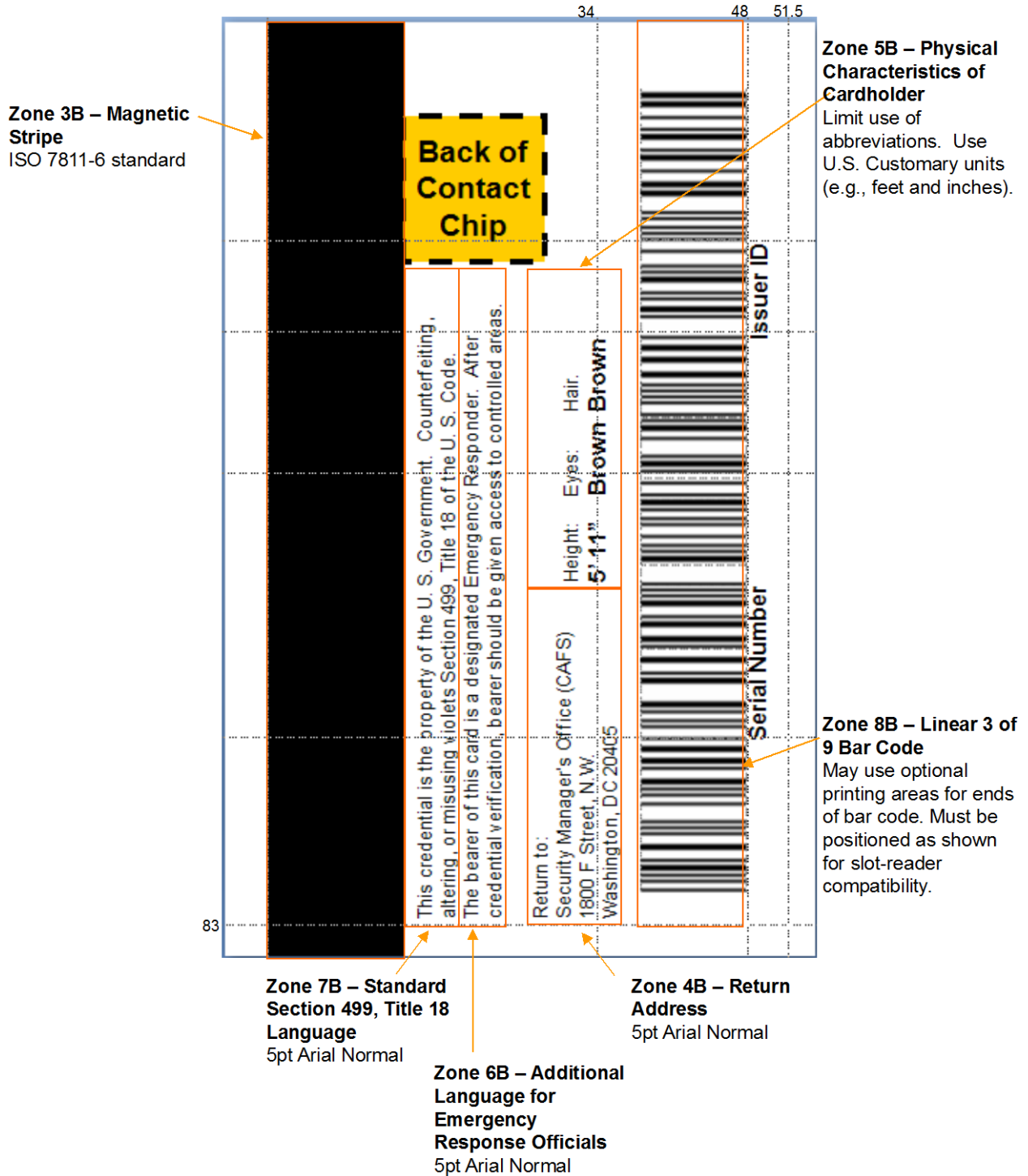


Figure 4-7. Card Back—Optional Data Placement—Example 1

All measurements are in millimeters and are from the top-left corner.
 All text is to be printed using the Arial font.
 Unless otherwise specified, the recommended font size is 5pt normal weight for tags and 6pt bold for data.

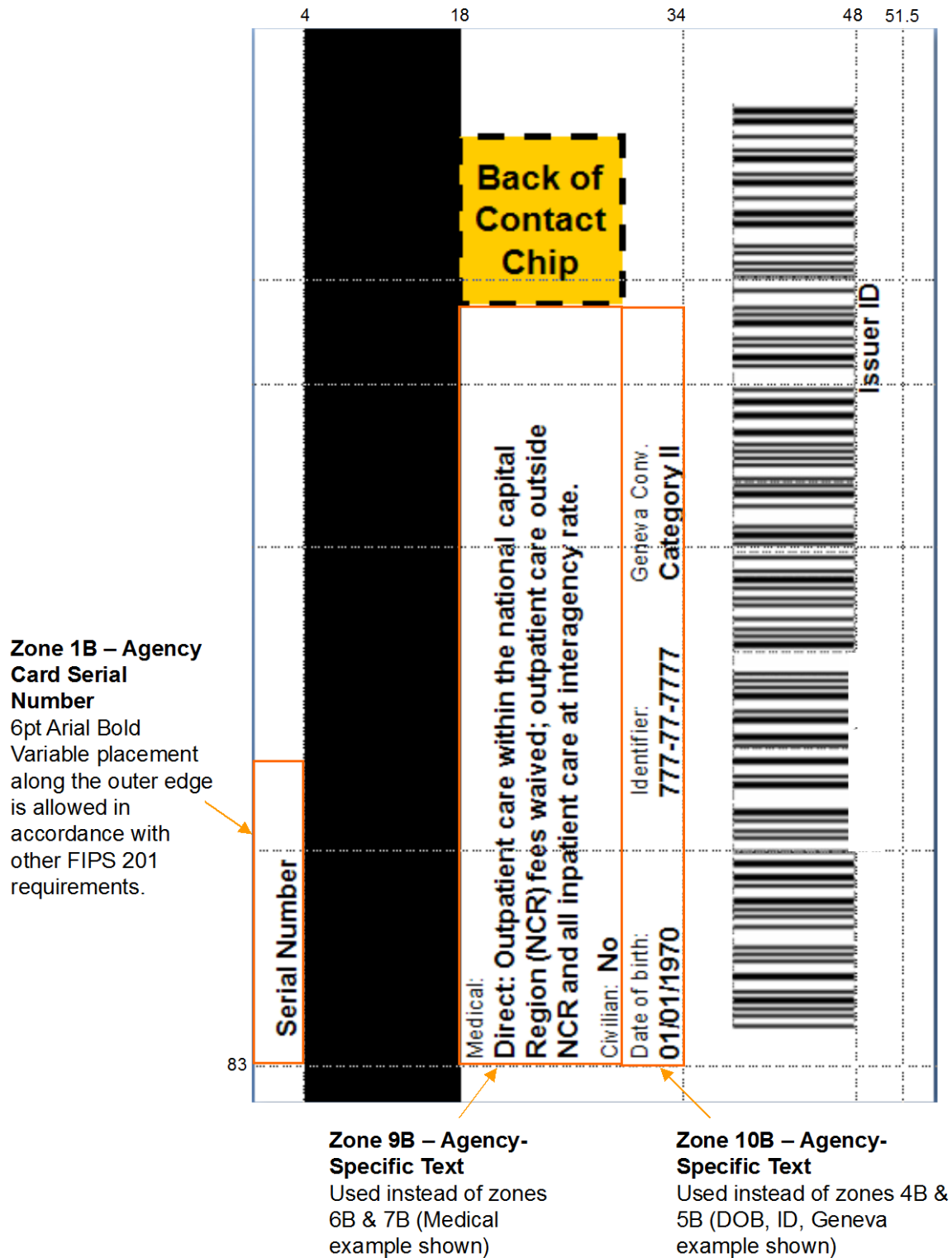


Figure 4-8. Card Back—Optional Data Placement—Example 2

4.1.5 Color Representation

Table 4-2 provides quantitative specifications for colors in three different color systems: sRGB Tristimulus, sRGB ([IEC61966], Color management – default RGB color space), and CMYK (Cyan, Magenta, Yellow and Key or ‘blacK’). Since the card body is white, the white color-coding is achieved by the absence of printing. Note that presence of the security feature, which may overlap colored or printed regions, may modify the perceived color. In the case of colored regions, the effect of overlap shall not prevent the recognition of the principal color by a person with normal vision (corrected or uncorrected) at a working distance of 50 cm to 200 cm.

Table 4-2. Color Representation

Color	Zone	sRGB Tristimulus Value (IEC 61966-2-1)	sRGB Value (IEC 61966-2-1)	CMYK Value {C,M,Y,K}
White	15F	{255, 255, 255}	{255, 255, 255}	{0, 0, 0, 0}
Green	15F	{153, 255, 153}	{203, 255, 203}	{40, 0, 40, 0}
Blue	15F	{0, 255, 255}	{0, 255, 255}	{100, 0, 0, 0}
Red	12F	{253, 27, 20}	{254, 92, 79}	{0, 90, 86, 0}

The colors in Table 4-2 can be mapped to the Pantone²¹ color cue; however, note that this will not produce an exact match. An agency or department may use the following Pantone mappings in cases where Table 4-2 scales are not available.

- Blue—630C
- White—White
- Green—359C
- Red—032C

4.2 PIV Card Logical Characteristics

This section defines logical identity credentials and the requirements for use of these credentials.

To support a variety of authentication mechanisms, the PIV Card shall contain multiple data elements for the purpose of verifying the cardholder's identity at graduated assurance levels. The following mandatory data elements are part of the data model for PIV logical credentials that support authentication mechanisms interoperable across agencies:

- a PIN;
- a CHUID;
- PIV authentication data (one asymmetric private key and corresponding certificate);
- two fingerprint templates;
- an electronic facial image; and

²¹ Pantone is a registered name protected by law.

- card authentication data (one asymmetric private key and corresponding certificate).

This Standard also defines two data elements for the PIV data model that are mandatory if the cardholder has a government-issued email account at the time of credential issuance. These data elements are:

- an asymmetric private key and corresponding certificate for digital signatures; and
- an asymmetric private key and corresponding certificate for key management.

This Standard also defines optional data elements for the PIV data model. These optional data elements include:

- one or two iris images;
- one or two fingerprint templates for on-card comparison;
- a symmetric Card Authentication key for supporting physical access applications; and
- a symmetric PIV Card Application Administration key associated with the card management system.

In addition to the above, other data elements are specified in [SP 800-73].

PIV logical credentials fall into the following three categories:

1. credential elements used to prove the identity of the cardholder to the card (CTC authentication);
2. credential elements used to prove the identity of the card management system to the card (CMTC authentication); and
3. credential elements used by the card to prove the identity of the cardholder to an external entity (CTE authentication) such as a host computer system.

The PIN falls into the first category, the PIV Card Application Administration Key into the second category, and the CHUID, biometric credentials, symmetric keys, and asymmetric keys into the third. The fingerprint templates for on-card comparison fall into the first and third categories.

4.2.1 Cardholder Unique Identifier (CHUID)

The PIV Card shall include the CHUID as defined in [SP 800-73]. The CHUID includes the Federal Agency Smart Credential Number (FASC-N) and the Global Unique Identification Number (GUID), which uniquely identify each card as described in [SP 800-73]. The value of the GUID data element shall be a 16-byte binary representation of a valid Universally Unique Identifier (UUID) [RFC4122]. The CHUID shall also include an expiration date data element in machine-readable format that specifies when the card expires. The expiration date format and encoding rules are as specified in [SP 800-73].

The CHUID shall be accessible from both the contact and contactless interfaces of the PIV Card without card activation. The FASC-N, UUID, and expiration date shall not be modified post-issuance.

This Standard requires inclusion of the asymmetric signature field in the CHUID container. The asymmetric signature data element of the CHUID shall be encoded as a Cryptographic Message Syntax (CMS) external digital signature, as specified in [SP 800-73]. Algorithm and key size requirements for the asymmetric signature and digest algorithm are detailed in [SP 800-78].

For signatures created before October 15, 2015, the public key required to verify the digital signature shall be provided in the *certificates* field of the CMS external digital signature in a content signing certificate, which shall be an X.509 digital signature certificate issued under the id-fpki-common-piv-contentSigning, id-fpki-common-devices, id-fpki-common-devicesHardware, id-fpki-common-hardware, or id-fpki-common-High policy of [COMMON].²² For signatures created on or after October 15, 2015, the public key required to verify the digital signature shall be provided in the *certificates* field of the CMS external digital signature in a content signing certificate, which shall be an X.509 digital signature certificate issued under the id-fpki-common-piv-contentSigning policy of [COMMON]. The content signing certificate shall also include an extended key usage (*extKeyUsage*) extension asserting id-PIV-content-signing. Additional descriptions for the PIV object identifiers are provided in Appendix B. The content signing certificate on a valid PIV Card (one that is neither expired nor revoked) shall not be expired.

4.2.2 Cryptographic Specifications

The PIV Card shall implement the cryptographic operations and support functions as defined in [SP 800-78] and [SP 800-73].

The PIV Card must store private keys and corresponding public key certificates, and perform cryptographic operations using the asymmetric private keys. At a minimum, the PIV Card must store two asymmetric private keys and the corresponding public key certificates, namely the *PIV Authentication key* and the *asymmetric Card Authentication key*. The PIV Card must also store a *digital signature key* and a *key management key*, and the corresponding public key certificates, unless the cardholder does not have a government-issued email account at the time of credential issuance.

The PIV Card may include an asymmetric private key and corresponding public key certificate to establish symmetric keys for use with secure messaging, as specified in [SP 800-73] and [SP 800-78]. Secure messaging enables data and commands transmitted between the card and an external entity to be both integrity protected and encrypted. Secure messaging may be used, for example, to enable the use of on-card biometric comparison as an authentication mechanism.

Once secure messaging has been established, a *virtual contact interface* may be established. Requirements for the virtual contact interface are specified in [SP 800-73]. Any operation that may be performed over the contact interface of the PIV Card may also be performed over the virtual contact interface. With the exception of the *Card Authentication key* and keys used to establish a secure messaging, the cryptographic private key operations shall be performed only through the contact interface or the virtual contact interface.

Symmetric cryptographic operations are not mandated for the contactless interface, but departments and agencies may choose to supplement the basic functionality with storage for a symmetric Card Authentication key and support for a corresponding set of cryptographic operations. For example, if a department or agency wants to utilize Advanced Encryption Standard (AES) based challenge/response for physical access, the PIV Card must contain storage for the AES key and support AES operations through the contactless interface. Algorithms and key sizes for each PIV key type are specified in [SP 800-78].

The PIV Card has both mandatory keys and optional keys:

²² For legacy PKIs, as defined in Section 5.4, the certificates may be issued under a department or agency-specific policy that has been cross-certified with the Federal Bridge CA (FBCA) at the Medium Hardware or High Assurance Level.

- The *PIV Authentication key* is a mandatory asymmetric private key that supports card and cardholder authentication for an interoperable environment.
- The *asymmetric Card Authentication key* is a mandatory private key that supports card authentication for an interoperable environment.
- The *symmetric (secret) Card Authentication key* supports card authentication for physical access, and it is optional.
- The *digital signature key* is an asymmetric private key supporting document signing, and it is mandatory, unless the cardholder does not have a government-issued email account at the time of credential issuance.
- The *key management key* is an asymmetric private key supporting key establishment and transport, and it is mandatory, unless the cardholder does not have a government-issued email account at the time of credential issuance. Optionally, up to twenty retired key management keys may also be stored on the PIV Card.
- The *PIV Card Application Administration Key* is a symmetric key used for personalization and post-issuance activities, and it is optional.
- The PIV Card may include additional key(s) for use with secure messaging. These keys are defined in [SP 800-73] or [SP 800-78].

All PIV cryptographic keys shall be generated within a [FIPS140] validated cryptographic module with overall validation at Level 2 or above. In addition to an overall validation of Level 2, the PIV Card shall provide Level 3 physical security to protect the PIV private keys in storage. The scope of the validation for the PIV Card shall include all cryptographic operations performed over both the contact and contactless interfaces (1) by the PIV Card Application, (2) as part of secure messaging as specified in this section, and (3) as part of remote post issuance updates as specified in Section 2.9.2. Specific algorithm testing requirements for the cryptographic operations performed by the PIV Card Application are specified in [SP 800-78].

Requirements specific to storage and access for each key are detailed below. Where applicable, key management requirements are also specified.

- **PIV Authentication Key.** This key shall be generated on the PIV Card. The PIV Card shall not permit exportation of the PIV Authentication key. The cryptographic operations that use the PIV Authentication key shall be available only through the contact and the virtual contact interfaces of the PIV Card. Private key operations may be performed using an activated PIV Card without explicit user action (e.g., the PIN need not be supplied for each operation).

The PIV Card shall store a corresponding X.509 certificate to support validation of the public key. The X.509 certificate shall include the FASC-N in the subject alternative name extension using the pivFASC-N attribute to support physical access procedures. The X.509 certificate shall also include the UUID value from the GUID data element of the CHUID in the subject alternative name extension. The UUID shall be encoded as a uniform resource identifier (URI), as specified in Section 3 of [RFC4122]. The expiration date of the certificate must be no later than the expiration date of the PIV Card. The PIV Authentication certificate shall include a PIV NACI indicator (background investigation indicator) extension (see Appendix B.2); this non-critical extension indicates the status

of the subject's background investigation at the time of card issuance.²³ Section 5 of this document specifies the certificate format and the key management infrastructure for the PIV Authentication key.

- + **Asymmetric Card Authentication Key.** The asymmetric Card Authentication key may be generated on the PIV Card or imported to the card. The PIV Card shall not permit exportation of the Card Authentication key. Cryptographic operations that use the Card Authentication key shall be available through the contact and the contactless interfaces of the PIV Card. Private key operations may be performed using this key without card activation (e.g., the PIN need not be supplied for operations with this key).

The PIV Card shall store a corresponding X.509 certificate to support validation of the public key. The X.509 certificate shall include the FASC-N in the subject alternative name extension using the pivFASC-N attribute to support physical access procedures. The X.509 certificate shall also include the UUID value from the GUID data element of the CHUID in the subject alternative name extension. The UUID shall be encoded as a URI, as specified in Section 3 of [RFC4122]. The expiration date of the certificate must be no later than the expiration date of the PIV Card. Section 5 of this document specifies the certificate format and the key management infrastructure for asymmetric PIV Card Authentication keys.

- + **Symmetric Card Authentication Key.** The symmetric Card Authentication key may be imported onto the card by the issuer or be generated on the card. If present, the symmetric Card Authentication key shall be unique for each PIV Card and shall meet the algorithm and key size requirements stated in [SP 800-78]. If present, cryptographic operations using this key may be performed without card activation (e.g., the PIN need not be supplied for operations with this key). The cryptographic operations that use the Card Authentication key shall be available through the contact and the contactless interfaces of the PIV Card. This Standard does not specify key management protocols or infrastructure requirements.
- **Digital Signature Key.** The PIV digital signature key shall be generated on the PIV Card. The PIV Card shall not permit exportation of the digital signature key. If present, cryptographic operations using the digital signature key may only be performed using the contact and the virtual contact interfaces of the PIV Card. Private key operations may not be performed without explicit user action, as this Standard requires the cardholder to authenticate to the PIV Card each time it performs a private key computation with the digital signature key.²⁴

The PIV Card shall store a corresponding X.509 certificate to support validation of the public key. The expiration date of the certificate must be no later than the expiration date of the PIV Card. Section 5 of this document specifies the certificate format and the key management infrastructure for PIV digital signature keys.

- **Key Management Key.** This key may be generated on the PIV Card or imported to the card. If present, the cryptographic operations that use the key management key must only be accessible using the contact and the virtual contact interfaces of the PIV Card. Private key operations may be performed using an activated PIV Card without explicit user action (e.g., the PIN need not be supplied for each operation).

The PIV Card shall store a corresponding X.509 certificate to support validation of the public key. Section 5 of this document specifies the certificate format and the key management infrastructure for key management keys.

²³ Other methods to indicate background investigative status will be explored in a future revision of this Standard.

²⁴ [NISTIR7863], *Cardholder Authentication for the PIV Digital Signature Key*, addresses the appropriate use of PIN caching related to digital signatures.

- **PIV Card Application Administration Key.** If present, the PIV Card Application Administration Key shall be imported onto the card by the issuer. If present, the cryptographic operations that use the PIV Card Application Administration Key must only be accessible using the contact interface of the PIV Card.

4.2.3 PIV Biometric Data Specifications

4.2.3.1 Biometric Data Representation

The following biometric data shall be stored on the PIV Card:

- Two fingerprint templates. If no fingerprint images meeting the quality criteria of [SP 800-76] are available, the PIV Card shall nevertheless be populated with fingerprint records as specified in [SP 800-76].
- An electronic facial image.

The following biometric data may also be stored on the PIV Card:

- One or two iris images.
- Fingerprint templates for on-card comparison.²⁵

All biometric data shall be stored in the data elements referenced by [SP 800-73] and in conformance with the preparation and formatting specifications of [SP 800-76].

4.2.3.2 Biometric Data Protection

The integrity of all biometric data, except for fingerprint templates for on-card comparison, shall be protected using digital signatures as follows. The records shall be prepended with a Common Biometric Exchange Formats Framework (CBEFF) header (referred to as CBEFF_HEADER) and appended with the CBEFF signature block (referred to as the CBEFF_SIGNATURE_BLOCK) [CBEFF].

The format for a CBEFF_HEADER is specified in [SP 800-76].

The CBEFF_SIGNATURE_BLOCK contains the digital signature of the biometric data and thus facilitates the verification of integrity of the biometric data. The CBEFF_SIGNATURE_BLOCK shall be encoded as a CMS external digital signature as specified in [SP 800-76]. The algorithm and key size requirements for the digital signature and digest algorithm are detailed in [SP 800-78].

For signatures created before October 15, 2015, the public key required to verify the digital signature shall be contained in a content signing certificate, which shall be issued under the id-fpki-common-piv-contentSigning, id-fpki-common-devices, id-fpki-common-devicesHardware, id-fpki-common-hardware, or id-fpki-common-High policy of [COMMON].²⁶ For signatures created on or after October 15, 2015, the public key required to verify the digital signature shall be contained in a content signing certificate, which shall be issued under the id-fpki-common-piv-contentSigning policy of [COMMON]. The content signing certificate shall also include an extended key usage (*extKeyUsage*) extension asserting id-PIV-content-signing. If the signature on the biometric was generated with a different key than the signature on

²⁵ The on-card and off-card fingerprint reference data are stored separately and, as conformant instances of different formal fingerprint standards, are syntactically different. This is described more fully in [SP 800-76].

²⁶ For legacy PKIs, as defined in Section 5.4, the certificates may be issued under a department or agency-specific policy that has been cross-certified with the Federal Bridge CA (FBCA) at the Medium Hardware or High Assurance Level.

the CHUID, the *certificates* field of the CMS external digital signature shall include the content signing certificate required to verify the signature on the biometric. Otherwise, the *certificates* field shall be omitted. Additional descriptions for the PIV object identifiers are provided in Appendix B. The content signing certificate on a valid PIV Card (one that is neither expired nor revoked) shall not be expired.

4.2.3.3 Biometric Data Access

The PIV biometric data, except for fingerprint templates for on-card comparison, that is stored on the card

- shall be readable through the contact interface and after the presentation of a valid PIN; and
- may optionally be readable through the virtual contact interface and after the presentation of a valid PIN.

On-card biometric comparison may be performed over the contact and the contactless interfaces of the PIV Card to support card activation (Section 4.3.1) and cardholder authentication (Section 6.2.2). The fingerprint templates for on-card comparison shall not be exportable. If implemented, on-card biometric comparison shall be implemented and used in accordance with [SP 800-73] and [SP 800-76].

4.2.4 PIV Unique Identifiers

A cardholder is authenticated through identification and authentication (I&A) using the PIV Card (and its identifier) in authentication mechanisms described in Section 6. The authenticated identity may then be used as the basis for making authorization decisions. Unique identifiers for both authentication and authorization are provided in this Standard in order to uniquely identify the cardholder. The two types of identifiers that serve as identification (of the cardholder) for authentication and authorization purposes, are described as follows:

+ Card identifiers

Each PIV card contains a UUID and a FASC-N that uniquely identify the card and, by correspondence, the cardholder. These two card identifiers are represented in all of the authentication data elements for the purpose of binding the PIV data elements to the same PIV Card.

+ Cardholder Identifiers

Other identifiers may be present in credentials on the PIV Card that identify the cardholder rather than the card. Examples include the subject name and names that may appear in the subjectAltName extension in the PIV Authentication certificate.

4.3 PIV Card Activation

The PIV Card shall be activated²⁷ to perform privileged²⁸ operations such as using the PIV Authentication key, digital signature key, and key management key. The PIV Card shall be activated for privileged operations only after authenticating the cardholder or the appropriate card management system. Cardholder activation is described in Section 4.3.1 and card management system activation is described in Section 4.3.2.

²⁷ Activation in this context refers to the unlocking of the PIV Card Application so privileged operations can be performed.

²⁸ A read of a CHUID or use of the Card Authentication key is not considered a privileged operation.

4.3.1 Activation by Cardholder

PIV Cards shall implement user-based cardholder activation to allow privileged operations using PIV credentials held by the card. At a minimum, the PIV Card shall implement PIN-based cardholder activation in support of interoperability across departments and agencies. Other card activation mechanisms (e.g., OCC card activation), only as specified in [SP 800-73], may be implemented and shall be discoverable. For PIN-based cardholder activation, the cardholder shall supply a numeric PIN. The verification data shall be transmitted to the PIV Card and checked by the card. If the verification data check is successful, the PIV Card is activated. The PIV Card shall include mechanisms to block activation of the card after a number of consecutive failed activation attempts. The number of allowable consecutive failed activation attempts may vary by activation mechanism.

The PIN should not be easily guessable or otherwise individually identifiable in nature (e.g., part of a Social Security Number, phone number). The required PIN length shall be a minimum of six digits.

4.3.2 Activation by Card Management System

PIV Cards may support card activation by the card management system to support card personalization and post-issuance card update. To activate the card for personalization or update, the card management system shall perform a challenge response protocol using cryptographic keys stored on the card in accordance with [SP 800-73]. When cards are personalized, PIV Card Application Administration Keys shall be set to be specific to each PIV Card. That is, each PIV Card shall contain a unique PIV Card Application Administration Key. PIV Card Application Administration Keys shall meet the algorithm and key size requirements stated in [SP 800-78].

4.4 Card Reader Requirements

This section provides minimum requirements for the contact and contactless card readers. Also, this section provides requirements for PIN input devices. Further requirements are specified in [SP 800-96].

4.4.1 Contact Reader Requirements

Contact card readers shall conform to the [ISO7816] standard for the card-to-reader interface. These readers shall conform to the Personal Computer/Smart Card (PC/SC) Specification [PCSC] for the reader-to-host system interface in general desktop computing environment. Specifically, the contact card readers shall conform to the requirements specified in [SP 800-96]. In systems where the readers are not connected to general-purpose desktop computing systems, the reader-to-host system interface is not specified in this Standard.

4.4.2 Contactless Reader Requirements

Contactless card readers shall conform to [ISO14443] standard for the card-to-reader interface and data transmitted over the [ISO14443] link shall conform to [ISO7816]. In cases where these readers are connected to general-purpose desktop computing systems, they shall conform to [PCSC] for the reader-to-host system interface. Specifically, the contactless card readers shall conform to the requirements specified in [SP 800-96]. In systems where the readers are not connected to general-purpose desktop computing systems, the reader-to-host system interface is not specified in this Standard.

4.4.3 Reader Resilience and Flexibility

The international standard ISO/IEC 24727 [ISO24727] enables a high degree of interoperability between electronic credentials and relying subsystems by means of an adaptation layer. To make interoperability among PIV System middleware, card readers, and credentials more resilient and flexible, the Department of Commerce will evaluate ISO/IEC 24727 and propose an optional profile of ISO/IEC 24727 in [SP 800-73]. The profile will explain how profile-conformant middleware, card readers, and PIV Cards can be used interchangeably with middleware, card readers, and PIV Cards currently deployed.

Specifications of the profile will become effective, as an optional means to implement PIV System readers and middleware, when OMB determines that the profile specifications are complete and ready for deployment.

4.4.4 Card Activation Device Requirements

When the PIV Card is used with OCC data or a PIN for physical access, the input device shall be integrated with the PIV Card reader. When the PIV Card is used with OCC data or a PIN for logical access (e.g., to authenticate to a Web site or other server), the input device is not required to be integrated with the PIV Card reader. If the input device is not integrated with the PIV Card reader, the OCC data or the PIN shall be transmitted securely and directly to the PIV Card for card activation.

The specifications for fingerprint capture devices for on-card comparison are given in [SP 800-76].

Malicious code could be introduced into the PIN capture and biometric reader devices for the purpose of compromising or otherwise exploiting the PIV Card. General good practice to mitigate malicious code threats is outside the scope of this document.²⁹

²⁹ See SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* [SP 800-53].

5. PIV Key Management Requirements

PIV Cards consistent with this specification will have two or more asymmetric private keys. To manage the public keys associated with the asymmetric private keys, departments and agencies shall issue and manage X.509 public key certificates as specified below.

5.1 Architecture

The CA that issues certificates to support PIV Card authentication shall participate in the hierarchical PKI for the Common Policy managed by the Federal PKI. Self-signed, self-issued, and CA certificates issued by these CAs shall conform to *Worksheet 1: Self-Signed Certificate Profile*, *Worksheet 2: Self-Issued CA Certificate Profile*, and *Worksheet 3: Cross Certificate Profile*, respectively, in *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program* [PROF]. The requirements for legacy PKIs are defined in Section 5.4.

5.2 PKI Certificate

All certificates issued to support PIV Card authentication shall be issued under the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework* [COMMON]. The requirements in this certificate policy cover identity proofing and the management of CAs and registration authorities. CAs and registration authorities may be operated by departments and agencies, or may be outsourced to PKI service providers. For a list of PKI service providers that have been approved to operate under [COMMON], see <http://www.idmanagement.gov>.

5.2.1 X.509 Certificate Contents

The required contents of X.509 certificates associated with PIV private keys are based on [PROF]. The relationship is described below:

- Certificates containing the public key associated with an asymmetric Card Authentication private key shall conform to *Worksheet 8: Card Authentication Certificate Profile* in [PROF].
- Certificates containing the public key associated with a digital signature private key shall conform to *Worksheet 5: End Entity Signature Certificate Profile* in [PROF] and shall specify either the id-fpki-common-hardware or id-fpki-common-High policy of [COMMON] in the certificate policies extension.
- Certificates containing the public key associated with a PIV Authentication private key shall conform to *Worksheet 9: PIV Authentication Certificate Profile* in [PROF].
- Certificates containing the public key associated with a key management private key shall conform to *Worksheet 6: Key Management Certificate Profile* in [PROF].³⁰
- Requirements for algorithms and key sizes for each type of PIV asymmetric key are given in [SP 800-78].

³⁰ Note that key management certificates may assert the id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-High policy of [COMMON] in the certificate policies extension. Applications / relying systems sensitive to the assurance level may choose not to accept certificates that only assert id-fpki-common-policy.

5.3 X.509 CRL Contents

CAs that issue certificates corresponding to PIV private keys shall issue CRLs as specified in [COMMON]. The contents of X.509 CRLs shall conform to *Worksheet 4: CRL Profile* in [PROF].

5.4 Legacy PKIs

For the purposes of this Standard, legacy PKIs are the PKIs of departments and agencies that have cross-certified with the Federal Bridge CA (FBCA) at the Medium Hardware or High Assurance Level. Legacy PKIs that issue PIV Authentication certificates and Card Authentication certificates shall meet the requirements specified in Sections 5.2.1, 5.3, 5.5, 5.5.1, and 5.5.2, with respect to the PIV Authentication certificates and Card Authentication certificates that they issue. Departments and agencies may assert department or agency-specific policy object identifiers (OIDs) in PIV Authentication Certificates and Card Authentication Certificates in addition to the *id-fpki-common-authentication* policy OID and the *id-fpki-common-cardAuth* policy OID of [COMMON], respectively. This specification imposes no requirements on digital signature or key management certificates issued by legacy PKIs.

5.5 PKI Repository and OCSP Responder(s)

CAs that issue certificates to support PIV Card authentication shall operate repositories and Online Certificate Status Protocol (OCSP) responders that provide certificate status information for the certificates they issue to support high-assurance interagency PIV Card interoperability. Departments and agencies will be responsible for notifying CAs when certificates need to be revoked. CAs shall maintain the status of servers and responders needed for PIV Card and certificate status checking.

The expiration date of the authentication certificates (PIV Authentication certificate and Card Authentication certificate) shall not be after the expiration date of the PIV Card. If the card is revoked, the authentication certificates shall be revoked in cases where the card cannot be collected and destroyed. However, an authentication certificate (and its associated key pair) may be revoked without revoking the PIV Card and may then be replaced. The presence of a valid, unexpired, and unrevoked authentication certificate on a card is proof that the card was issued and is not revoked.

Because an X.509 certificate typically is valid several years, a mechanism to distribute certificate status information is necessary. CRL and OCSP are the two commonly used mechanisms. CAs that issue PIV Authentication, Card Authentication, digital signature, or key management certificates shall maintain a Hypertext Transfer Protocol (HTTP) accessible web server that holds the CRLs for the certificates it issues, as well as any CA certificates issued to or by it, as specified in [PROF]. In addition, every CA that issues PIV Authentication or Card Authentication certificates shall operate an OCSP server that provides certificate status for every authentication certificate the CA issues.

PIV Authentication, Card Authentication, digital signature, and key management certificates shall contain the *crlDistributionPoints* extension needed to locate CRLs. PIV Authentication certificates and Card Authentication certificates shall also contain the *authorityInfoAccess* extension needed to locate the authoritative OCSP responder.

5.5.1 Certificate and CRL Distribution

This Standard requires distribution of CA certificates and CRLs using HTTP. Specific requirements are found in the Shared Service Provider Repository Service Requirements [SSP REP].

Certificates that contain the FASC-N or UUID in the subject alternative name extension, such as PIV Authentication certificates and Card Authentication certificates, shall not be distributed publicly (e.g., via the Lightweight Directory Access Protocol (LDAP) or HTTP accessible from the public Internet). Individual departments and agencies can decide whether other user certificates (digital signature and key management) can be distributed via LDAP. When user certificates are distributed, the requirements in Table IV—End-Entity Certificate Repository Service Requirements of [SSP REP] shall be satisfied.

5.5.2 OCSP Status Responders

OCSP [RFC2560] status responders shall be implemented as a supplementary certificate status mechanism. The OCSP status responders must be updated at least as frequently as CRLs are issued. The definitive OCSP responder for each certificate shall be specified in the *authorityInfoAccess* extension as described in [PROF].

6. PIV Cardholder Authentication

This section defines a suite of authentication mechanisms that are supported by all the PIV Cards, and their applicability in meeting the requirements for a set of graduated levels of identity assurance. This section also defines some authentication mechanisms that make use of credential elements that may optionally be included on PIV Cards. Specific implementation details of authentication mechanisms identified in this section are provided in [SP 800-73]. Moreover, while a wide range of authentication mechanisms is identified in this section, departments and agencies may adopt additional mechanisms that use the identity credentials on the PIV Card. In the context of the PIV Card Application, identity authentication is defined as the process of establishing confidence in the identity of the cardholder presenting a PIV Card. The authenticated identity can then be used to determine the permissions or authorizations granted to that identity for access to various physical and logical resources.

6.1 PIV Assurance Levels

This Standard defines four levels of assurance for identity authentication supported by the PIV Card Application. Each assurance level sets a degree of confidence established in the identity of the holder of the PIV Card. The entity performing the authentication establishes confidence in the identity of the PIV cardholder through the following:

- 1) the rigor of the identity proofing process conducted prior to issuing the PIV Card;
- 2) the security of the PIV Card issuance and maintenance processes; and
- 3) the strength of the technical mechanisms used to verify that the cardholder is the owner of the PIV Card.

Section 2 of this Standard defines requirements for the identity proofing, registration, issuance, and maintenance processes for PIV Cards and establishes a common level of assurance in these processes. The PIV identity proofing, registration, issuance, and maintenance processes meet or exceed the requirements for E-Authentication Level 4 [OMB0404]. The PIV Card contains a number of visual and logical credentials. Depending on the specific PIV data used to authenticate the holder of the PIV Card to an entity that controls access to a resource, varying levels of assurance that the holder of the PIV Card is the owner of the card can be achieved. This is the basis for the following PIV assurance levels defined in this Standard:

- LITTLE or NO Confidence—Little or no assurance in the identity of the cardholder;
- SOME Confidence—A basic degree of assurance in the identity of the cardholder;
- HIGH Confidence—A strong degree of assurance in the identity of the cardholder;
- VERY HIGH Confidence—A very strong degree of assurance in the identity of the cardholder.

Parties responsible for controlling access to Federal resources (both physical and logical) shall determine the appropriate level of identity assurance required for access, based on the harm and impact to individuals and organizations as a result of errors in the authentication of the identity of the PIV cardholder. Once the required level of assurance has been determined, the authentication mechanisms specified within this section may be applied to achieve the required degree of confidence in the identity of the PIV cardholder.

6.1.1 Relationship to OMB’s E-Authentication Guidance

The levels of identity authentication assurance defined within this Standard are closely aligned with Section 2 of OMB’s E-Authentication Guidance for Federal Agencies, M-04-04 [OMB0404]. Specifically, Table 6-1 shows the notional relationship between the PIV assurance levels and the M-04-04 E-Authentication assurance levels.

Table 6-1. Relationship Between PIV and E-Authentication Assurance Levels

PIV Assurance Levels	Comparable OMB E-Authentication Levels	
	Level Number	Description
LITTLE or NO confidence	Level 1	Little or no confidence in the asserted identity’s validity
SOME confidence	Level 2	Some confidence in the asserted identity’s validity
HIGH confidence	Level 3	High confidence in the asserted identity’s validity
VERY HIGH confidence	Level 4	Very high confidence in the asserted identity’s validity

[OMB0404] addresses “four levels of identity assurance for electronic transactions requiring authentication” and prescribes a methodology for determining the level of identity assurance required based on the risks and potential impacts of errors in identity authentication. In the context of the PIV Card, owners of logical resources shall apply the methodology defined in [OMB0404] to identify the level of identity authentication assurance required for their electronic transaction. Parties that are responsible for access to physical resources may use a methodology similar to that defined in [OMB0404] to determine the PIV assurance level required for access to their physical resource; they may also use other applicable methodologies to determine the required level of identity assurance for their application.

6.2 PIV Card Authentication Mechanisms

The following subsections define the basic types of authentication mechanisms that are supported by the credential set hosted by the PIV Card Application. PIV Cards can be used for identity authentication in environments that are equipped with card readers as well as those that lack card readers. Card readers, when present, can be contact readers or contactless readers. The usage environment affects the PIV authentication mechanisms that may be applied to a particular situation.

6.2.1 Authentication Using Off-Card Biometric Comparison

The PIV Card Application hosts the signed fingerprint templates and, optionally, the signed iris images. Either biometric can be read from the card following cardholder-to-card (CTC) authentication using a PIN supplied by the cardholder. These PIV biometrics are designed to support a cardholder-to-external system (CTE) authentication mechanism through a match-off-card scheme. The following subsections define two authentication schemes that make use of the PIV biometrics.³¹

Some characteristics of the PIV Biometrics authentication mechanisms (described below) are as follows:

³¹ As noted in Section 4.2.3.1, neither the fingerprint templates nor the iris images are guaranteed to be present on a PIV Card, since it may not be possible to collect fingerprints from some cardholders and iris images collection is optional. When biometric authentication cannot be performed, PKI-AUTH is the recommended alternate authentication mechanism.

- Strong resistance to use of unaltered card by non-owner since PIN and cardholder biometric are required.
- Digital signature on biometric, which is checked to further strengthen the mechanism.
- Slower mechanism, because it requires two interactions (e.g., presentation of PIN and biometric) with the cardholder.
- Does not provide protection against use of a revoked card.
- Applicable with contact card readers, and contactless card readers that support the virtual contact interface.

6.2.1.1 Unattended Authentication Using PIV Biometric (BIO)

The following steps shall be performed for unattended authentication of the PIV biometric:

- The CHUID or another data element³² is read from the card and is checked to ensure the card has not expired and that it is from a trusted source.
 - The cardholder is prompted to submit a PIN, activating the PIV Card.
 - The PIV biometric is read from the card.
 - The signature on the biometric is verified to ensure the biometric is intact and comes from a trusted source. Note that the signature verification may require retrieval of the content signing certificate from the CHUID if the signature on the biometric was generated with the same key as the signature on the CHUID.
 - The cardholder is prompted to submit a live biometric sample.
 - If the biometric sample matches the biometric read from the card, the cardholder is authenticated to be the owner of the card.
 - The FASC-N (or UUID) in the CHUID or other data element is compared with the FASC-N (or UUID) in the Signed Attributes field of the external digital signature on the biometric.
- + A unique identifier within the CHUID or other data element is used as input to the authorization check to determine whether the cardholder should be granted access.

6.2.1.2 Attended Authentication of PIV Biometric (BIO-A)

In this higher assurance variant, an attendant (e.g., security guard) supervises the use of the PIV Card and the submission of the biometric by the cardholder. Otherwise, the steps for this authentication mechanism are the same as for the unattended biometric (BIO) authentication mechanism.

6.2.2 Authentication Using On-Card Biometric Comparison (OCC-AUTH)

The PIV Card Application may host the optional on-card biometric comparison algorithm. In this case, on-card biometric comparison data is stored on the card, which cannot be read, but could be used for identity verification. A live-scan biometric is supplied to the card to perform cardholder-to-card (CTC)

³² The PIV Authentication certificate or Card Authentication PIV certificate may be leveraged instead of the CHUID to verify that the card is not expired.

authentication and the card responds with an indication of the success of the on-card biometric comparison. The response includes information that allows the reader to authenticate the card. The cardholder PIN is not required for this operation. The PIV Card shall include a mechanism to block this authentication mechanism after a number of consecutive failed authentication attempts as stipulated by the department or agency. As with authentication using the PIV biometrics, if agencies choose to implement on-card biometric comparison, it shall be implemented as defined in [SP 800-73] and [SP 800-76].

Some of the characteristics of the on-card biometric comparison authentication mechanism are as follows:

- Highly resistant to credential forgery.
- Strong resistance to use of unaltered card by non-owner.
- Applicable with contact and contactless card readers.

6.2.3 Authentication Using PIV Asymmetric Cryptography

The PIV Card contains two mandatory asymmetric authentication private keys and corresponding certificates to support cardholder-to-external system (CTE) authentication, as described in Section 4. The following subsections shall be used to perform authentication using the authentication keys.

6.2.3.1 Authentication with the PIV Authentication Certificate Credential (PKI-AUTH)

The following steps shall be performed for PKI-AUTH:

- The PIV Authentication certificate is read from the PIV Card Application.
- The relying system validates the PIV Authentication certificate from the PIV Card Application using standards-compliant PKI path validation³³ to ensure that it is neither expired nor revoked and that it is from a trusted source.
- The cardholder is prompted to submit a PIN, which is used to activate the card. (If implemented, other card activation mechanisms, as specified in [SP 800-73], may be used to activate the card.)
- The relying system issues a challenge string to the card and requests an asymmetric operation in response.
- The card responds to the previously issued challenge by signing it using the PIV Authentication private key.
- The relying system verifies that the card's response is the expected response to the issued challenge.
- A unique identifier from the PIV Authentication certificate is extracted and passed as input to the access control decision.

Some of the characteristics of the PKI-based authentication mechanism are as follows:

- Requires the use of certificate status checking infrastructure.
- Highly resistant to credential forgery.

³³ Path validation should be configured to specify which policy OIDs are trusted. The policy OID for the PIV Authentication certificate is id-fpki-common-authentication.

- Strong resistance to use of unaltered card by non-owner since card activation is required.
- Provides protection against use of a revoked card.
- Applicable with contact card readers, and contactless card readers that support the virtual contact interface.

6.2.3.2 Authentication with the Card Authentication Certificate Credential (PKI-CAK)

The following steps shall be performed for PKI-CAK:

- The Card Authentication certificate is read from the PIV Card Application.
- The relying system validates the Card Authentication certificate from the PIV Card Application using standards-compliant PKI path validation³⁴ to ensure that it is neither expired nor revoked and that it is from a trusted source.
- The relying system issues a challenge string to the card and requests an asymmetric operation in response.
- The card responds to the previously issued challenge by signing it using the Card Authentication private key.
- The relying system verifies that the card's response is the expected response to the issued challenge.
- A unique identifier from the Card Authentication certificate is extracted and passed as input to the access control decision.

Some of the characteristics of the PKI-CAK authentication mechanism are as follows:

- Requires the use of certificate status checking infrastructure.
- Highly resistant to credential forgery.
- Low resistance to use of unaltered card by non-owner of card.
- Applicable with contact and contactless readers.

6.2.4 Authentication with the Symmetric Card Authentication Key (SYM-CAK)

The PIV Card Application may host the optional symmetric Card Authentication key. In this case, the symmetric Card Authentication key shall be used for PIV cardholder authentication using the following steps:

- The CHUID, PIV Authentication certificate, or Card Authentication certificate data element is read from the PIV Card and is checked to ensure the card has not expired.
- The digital signature on the data element is checked to ensure that it was signed by a trusted source and is unaltered.
- The reader issues a challenge string to the card and requests a response.

³⁴ Path validation should be configured to specify which policy OIDs are trusted. The policy OID for the Card Authentication certificate is id-fpki-common-cardAuth.

- The card responds to the previously issued challenge by encrypting the challenge using the symmetric Card Authentication key.
- The response is validated as the expected response to the issued challenge.
- A unique identifier within the data element is used as input to the authorization check to determine whether the cardholder should be granted access.

Some of the characteristics of the symmetric Card Authentication key authentication mechanism are as follows:

- Resistant to credential forgery.
- Does not provide protection against use of a revoked card.
- Low resistance to use of unaltered card by non-owner of card.
- Applicable with contact and contactless readers.

6.2.5 Authentication Using the CHUID

The PIV Card provides a mandatory data element called the CHUID. As described in Section 4.2.1, the CHUID contains numerous data elements.

The CHUID shall be used for PIV cardholder authentication using the following steps:

- The CHUID is read electronically from the PIV Card.
- The digital signature on the CHUID is checked to ensure the CHUID was signed by a trusted source and is unaltered.
- The expiration date on the CHUID is checked to ensure that the card has not expired.
- A unique identifier within the CHUID is used as input to the authorization check to determine whether the cardholder should be granted access.

Some characteristics of the CHUID-based authentication mechanism are as follows:

- Can be used for rapid authentication for high volume access control.
- Low resistance to use of unaltered card by non-owner of card.
- Does not provide protection against use of a revoked card.
- Applicable with contact and contactless readers.

As the CHUID authentication mechanism provides LITTLE or NO assurance in the identity of the cardholder, use of the CHUID authentication mechanism is deprecated. It is expected that the CHUID authentication mechanism will be removed from this Standard at the next five-year revision.

6.2.6 Authentication Using PIV Visual Credentials (VIS)

Visual authentication of a PIV cardholder shall be used only to support access control to physical facilities and resources.

The PIV Card has several mandatory topographical features on the front and back that support visual identification and authentication, as follows:

- Zone 1F – Photograph;
- Zone 2F – Name;
- Zone 8F – Employee Affiliation;
- Zone 10F – Agency, Department, or Organization;
- Zones 14F and 19F – Card Expiration Date;
- Zone 15F – Color-Coding for Employee Affiliation;
- Zone 1B – Agency Card Serial Number (back of card);
- Zone 2B – Issuer Identification Number (back of card).

The PIV Card may also bear optional components, some of which are:

- Zone 11F – Agency Seal;
- Zone 5B – Physical Characteristics of Cardholder (back of card);
- Zone 3F – Signature.

When a cardholder attempts to pass through an access control point for a Federally controlled facility, a human guard shall perform visual identity verification of the cardholder, and determine whether the identified individual should be allowed through the control point. The following steps shall be applied in the visual authentication process:

- The guard at the access control entry point determines whether the PIV Card appears to be genuine and has not been altered in any way.
- The guard compares the cardholder’s facial features with the picture on the card to ensure that they match.
- The guard checks the expiration date on the card to ensure that the card has not expired.
- The guard compares the cardholder’s physical characteristic descriptions to those of the cardholder. (Optional)
- The guard collects the cardholder’s signature and compares it with the signature on the card. (Optional)
- One or more of the other data elements on the card (e.g., name, employee affiliation, agency card serial number, issuer identification, agency name) are used to determine whether the cardholder should be granted access.

Some characteristics of the visual authentication mechanism are as follows:

- Human inspection of card, which is not amenable for rapid or high volume access control and is susceptible to human error.

- Some resistance to use of unaltered card by non-owner of card.
- Low resistance to tampering and forgery.
- Does not provide protection against use of a revoked card.
- Applicable in environments with and without card readers.

6.3 PIV Support of Graduated Assurance Levels for Identity Authentication

The PIV Card supports a set of authentication mechanisms that can be used to implement graduated assurance levels for identity authentication. The following subsections specify which basic PIV authentication mechanisms may be used to support the various levels of identity authentication assurance as defined in Section 6.1. Two or more complementing authentication mechanisms may be applied in unison to achieve a higher degree of assurance of the identity of the PIV cardholder. For example, PKI-AUTH and BIO may be applied in unison to achieve a higher degree of assurance in cardholder identity.

Adequately designed and implemented relying systems can achieve the PIV Card authentication assurance levels stated in Tables 6-2 (physical access) and 6-3 (logical access). Less adequately designed or implemented relying systems may only achieve lower authentication assurance levels. The design of components of relying systems, including card readers, biometric readers, cryptographic modules, and key management systems, involves many factors not fully specified by FIPS 201, such as correctness of the functional mechanism, physical protection of the mechanism, and environmental conditions at the authentication point. Additional standards and best practice guidelines apply to the design and implementation of relying systems, e.g., [FIPS140] and [SP 800-116].

6.3.1 Physical Access

The PIV Card may be used to authenticate the identity of the cardholder in a physical access control environment. For example, a Federal facility may have physical entry doors that have human guards at checkpoints, or may have electronic access control points. The PIV-supported authentication mechanisms for physical access control systems are summarized in Table 6-2. An authentication mechanism that is suitable for a higher assurance level can also be applied to meet the requirements for a lower assurance level. Moreover, the authentication mechanisms in Table 6-2 can be combined to achieve higher assurance levels.³⁵

Table 6-2. Authentication for Physical Access

PIV Assurance Level Required by Application/Resource	Applicable PIV Authentication Mechanism
LITTLE or NO confidence	VIS, CHUID
SOME confidence	PKI-CAK, SYM-CAK
HIGH confidence	BIO
VERY HIGH confidence	BIO-A, OCC-AUTH, PKI-AUTH

³⁵ Combinations of authentication mechanisms are specified in [SP 800-116].

6.3.2 Logical Access

The PIV Card may be used to authenticate the cardholder in support of decisions concerning access to logical information resources. For example, a cardholder may log in to his or her department or agency network using the PIV Card; the identity established through this authentication process can be used for determining access to file systems, databases, and other services available on the network.

Table 6-3 describes the authentication mechanisms defined for this Standard to support logical access control. An authentication mechanism that is suitable for a higher assurance level can also be applied to meet the requirements for a lower assurance level.

Table 6-3. Authentication for Logical Access

PIV Assurance Level Required by Application/Resource	Applicable PIV Authentication Mechanism	
	Local Workstation Environment	Remote/Network System Environment
LITTLE or NO confidence	CHUID	
SOME confidence	PKI-CAK	PKI-CAK
HIGH confidence	BIO	
VERY HIGH confidence	BIO-A, OCC-AUTH, PKI-AUTH	PKI-AUTH

Appendix A—PIV Validation, Certification, and Accreditation

This appendix provides compliance requirements for PIV validation, certification, and accreditation, and is normative.

A.1 Accreditation of PIV Card Issuers (PCI)

[HSPD-12] requires that all cards be issued by providers whose reliability has been established by an official accreditation process. The accreditation of the PIV Card issuer shall be reviewed through a third-party assessment to enhance the trustworthiness of the credential. To facilitate consistent independent validation of the PCI, NIST developed a set of attributes as the basis of reliability assessment of PIV Card issuers in SP 800-79 and published this document in July 2005. Subsequent lessons learned in implementation experience (in credential management and PIV Card issuance) of various agencies together with the evolution of PCI organizations motivated NIST to develop a new accreditation methodology that is objective, efficient, and will result in consistent and repeatable accreditation decisions and published the substantial revision as SP 800-79-1 in June 2008 [SP 800-79]. The new PCI accreditation methodology is built on a foundation of four major accreditation topics, 13 accreditation focus areas, and a total of 79 control requirements distributed under the various accreditation focus areas. Associated with each control requirement is a set of assessment methods, the exercise of the latter will result in outcomes that form the basis for accreditation decisions.

The four major accreditation topics identified in [SP 800-79] are:

- organizational preparedness;
- security management and data protection;
- infrastructure elements; and
- (PIV) processes.

The entire spectrum of activities in the PCI accreditation methodology is divided into the following four phases:

- initiation phase;
- assessment phase;
- accreditation phase; and
- monitoring phase.

The initiation phase involves communicating the goals of the assessment/accreditation to the key personnel of the PCI organization and the review of documents such as the PCI operations plan. In the assessment phase, the appropriate assessment methods stipulated in the methodology for each PCI control are carried out and the individual results recorded. The accreditation phase involves aggregating the results of assessment, arriving at an accreditation decision, and issuing the appropriate notification – the authorization to operate (ATO) or the denial of authorization to operate (DATO), that is consistent with the accreditation decision.

A.2 Application of Risk Management Framework to IT System(s) Supporting PCI

The accreditation of the capability and reliability of a PCI using the methodology outlined in [SP 800-79] depends upon adequate security for the information systems that are used for PCI functions. The assurance that such a security exists in a PCI is obtained through evidence of the application of the Risk Management Framework guidelines specified in [SP 800-37]. The methodology in [SP 800-37] in turn was created pursuant to a mandate in Appendix III of Office of Management and Budget (OMB) Circular A-130. An Information system authorization decision together with evidence of security control monitoring compliant with [SP 800-37] guidelines signifies that a PCI organization's official accepts responsibility for the security (in terms of confidentiality, integrity, and availability of information) of the information systems that will be involved in carrying out the PCI functions. Hence evidence of successful application of Risk Management Framework consistent with [SP 800-37] guidelines is mandatory for issuing PCI accreditation using [SP 800-79].

A.3 Conformance Testing of PIV Card Application and Middleware

Assurance of conformance of the PIV Card Application and PIV Middleware interfaces to this Standard and its associated technical specifications is needed in order to meet the security and interoperability goals of [HSPD-12]. To facilitate this, NIST has established the NIST Personal Identity Verification Program (NPIVP). Under this program NIST has developed test procedures in SP 800-85A, *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73 compliance)*, and an associated toolkit for conformance testing of PIV Card Applications and PIV Middleware [SP 800-85A]. Commercial products under these two categories are tested by the set of accredited test laboratories, accredited under the National Voluntary Laboratory Accreditation Program (NVLAP) program, using the NIST supplied test procedures and toolkit. The outcomes of the test results are validated by NIST, which then issues validation certificates. Information about NPIVP is available at <http://csrc.nist.gov/groups/SNS/piv/npivp>.

A.4 Cryptographic Testing and Validation

All on-card cryptographic modules hosting the PIV Card Application and cryptographic modules of card issuance and maintenance systems shall be validated to [FIPS140] with an overall Security Level 2 (or higher). The facilities for [FIPS140] testing are the Cryptographic and Security Testing laboratories accredited by the NVLAP program of NIST. Vendors wanting to supply cryptographic modules can select any of the accredited laboratories. The tests conducted by these laboratories for all vendor submissions are validated and a validation certificate for each vendor module is issued by the Cryptographic Module Validation Program (CMVP), a joint program run by NIST and the Communications Security Establishment (CSE) of the Government of Canada. The details of the CMVP and NVLAP programs and the list of testing laboratories can be found at the CMVP Web site at <http://csrc.nist.gov/groups/STM/cmvp/index.html>.

A.5 FIPS 201 Evaluation Program

In order to evaluate the conformance of different families of products that support the PIV processes to this Standard and its associated technical specifications, the Office of Governmentwide Policy under GSA set up the FIPS 201 Evaluation Program. The product families currently include card personalization products, card readers, products involved in credential enrollment functions such as fingerprint and facial image capture equipment, biometric fingerprint template generators, etc. Products evaluated and approved under this program are placed on the FIPS 201 Approved Products List to enable procurement of conformant products by implementing agencies. The details of the program are available at <http://fips201ep.cio.gov/>.

Appendix B—PIV Object Identifiers and Certificate Extension

This normative appendix provides additional details for the PIV objects identified in Section 4.

B.1 PIV Object Identifiers

Table B-1 lists details for PIV object identifiers.

Table B-1. PIV Object Identifiers

ID	Object Identifier	Description
PIV eContent Types		
id-PIV-CHUIDSecurityObject	2.16.840.1.101.3.6.1	The associated content is the concatenated contents of the CHUID, excluding the authentication key map ³⁶ and the asymmetric signature field.
id-PIV-biometricObject	2.16.840.1.101.3.6.2	The associated content is the concatenated CBEFF_HEADER + STD_BIOMETRIC_RECORD.
PIV Attributes		
pivCardholder-Name	2.16.840.1.101.3.6.3	The attribute value is of type DirectoryString and specifies the PIV cardholder's name.
pivCardholder-DN	2.16.840.1.101.3.6.4	The attribute value is an X.501 type Name and specifies the DN associated with the PIV cardholder in the PIV certificate(s).
pivSigner-DN	2.16.840.1.101.3.6.5	The attribute value is an X.501 type Name and specifies the subject name that appears in the PKI certificate for the entity that signed the biometric or CHUID.
pivFASC-N	2.16.840.1.101.3.6.6	The pivFASC-N OID may appear as a name type in the otherName field of the subjectAltName extension of X.509 certificates or a signed attribute in CMS external signatures. Where used as a name type, the syntax is OCTET STRING. Where used as an attribute, the attribute value is of type OCTET STRING. In each case, the value specifies the FASC-N of the PIV Card.
PIV Extended Key Usage		
id-PIV-content-signing	2.16.840.1.101.3.6.7	This specifies that the public key may be used to verify signatures on CHUIDs and PIV biometrics.
id-PIV-cardAuth	2.16.840.1.101.3.6.8	This specifies that the public key is used to authenticate the PIV Card rather than the PIV cardholder.

The OIDs for certificate policies are specified in [COMMON].

B.2 PIV Certificate Extension

The PIV NACI indicator (background investigation indicator) extension indicates whether the subject's background investigation was incomplete at the time of credential issuance. The PIV NACI indicator (background investigation indicator) extension is always non-critical, and shall appear in all PIV

³⁶ The authentication key map was deprecated in SP 800-73-2 and was removed from SP 800-73-3.

Authentication certificates and Card Authentication certificates. The value of this extension is asserted as follows:

- TRUE if, at the time of credential issuance, (1) the FBI National Criminal History Fingerprint Check has completed, and (2) a background investigation has been initiated but has not completed.
- FALSE if, at the time of credential issuance, the subject's background investigation has been completed and successfully adjudicated.

The PIV NACI indicator (background investigation indicator) extension is identified by the id-piv-NACI object identifier. The syntax for this extension is defined by the following ASN.1 module.

```
PIV-Cert-Extensions { 2 16 840 1 101 3 6 10 1 }

DEFINITIONS EXPLICIT TAGS ::=

BEGIN

-- EXPORTS ALL --

-- IMPORTS NONE --

id-piv-NACI OBJECT IDENTIFIER ::= { 2 16 840 1 101 3 6 9 1 }

NACI-indicator ::= BOOLEAN

END
```

Appendix C—Glossary of Terms, Acronyms, and Notations

This informative appendix describes the vocabulary and textual representations used in the document.

C.1 Glossary of Terms

The following terms are used throughout this Standard.

Access Control: The process of granting or denying specific requests: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances).

Applicant: An individual applying for a PIV Card/credential. The applicant may be a current or prospective Federal hire, a Federal employee, a government affiliate, or a contractor.³⁷

Application: A hardware/software system implemented to satisfy a particular set of requirements. In this context, an application incorporates a system used to satisfy a subset of requirements related to the verification or identification of an end user's identity so that the end user's identifier can be used to facilitate the end user's interaction with the system.

Architecture: A highly structured specification of an acceptable approach within a framework for solving a specific problem. An architecture contains descriptions of all the components of a selected, acceptable solution while allowing certain details of specific components to be variable to satisfy related constraints (e.g., costs, local environment, user acceptability).

Asymmetric Keys: Two related keys, a public key and a private key, that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.

Authentication: The process of establishing confidence of authenticity; in this case, in the validity of a person's identity and the PIV Card.

Biometric: A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris image samples are all examples of biometrics.

Biometric Information: The stored electronic information pertaining to a biometric. This information can be in terms of raw or compressed pixels or in terms of some characteristic (e.g., patterns).

Capture: The method of taking a biometric sample from an end user. [INCITS/M1-040211]

Cardholder: An individual possessing an issued PIV Card.

Card Management System: The card management system manages the lifecycle of a PIV Card Application.

Certificate Revocation List: A list of revoked public key certificates created and digitally signed by a certification authority. [RFC5280]

³⁷ See Page 2 of [OMB0524] for further details of individuals who are eligible to be issued PIV Cards.

Certification: The process of verifying the correctness of a statement or claim and issuing a certificate as to its correctness.

Certification Authority: A trusted entity that issues and revokes public key certificates.

Chain-of-trust: The chain-of-trust is a sequence of related enrollment data sets that is created and maintained by PIV Card issuers.

Comparison: The process of comparing a biometric with a previously stored reference. See also “Identification” and “Identity Verification”. [INCITS/M1-040211]

Component: An element of a large system, such as an identity card, issuer, card reader, or identity verification support, within the PIV system.

Conformance Testing: A process established by NIST within its responsibilities of developing, promulgating, and supporting FIPS for testing specific characteristics of components, products, and services, as well as people and organizations for compliance with a FIPS.

Credential: Evidence attesting to one’s right to credit or authority; in this Standard, it is the PIV Card and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual.

Cryptographic Key (Key): A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm.

E-Authentication Assurance Level: A measure of trust or confidence in an authentication mechanism defined in [OMB0404] and [SP 800-63], in terms of four levels:

- Level 1: LITTLE OR NO confidence
- Level 2: SOME confidence
- Level 3: HIGH confidence
- Level 4: VERY HIGH confidence

Enrollment Data Set: A record including information about a biometric enrollment: name and role of the acquiring agent, office and organization, time, place, and acquisition method.

Federal Agency Smart Credential Number (FASC-N): As required by FIPS 201, one of the primary identifiers on the PIV Card for physical access control. The FASC-N is a fixed length (25 byte) data object, specified in [SP 800-73], and included in several data objects on a PIV Card.

Federal Information Processing Standards (FIPS): A standard for adoption and use by Federal departments and agencies that has been developed within the Information Technology Laboratory and published by NIST, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology to achieve a common level of quality or some level of interoperability.

Hash Function: A function that maps a bit string of arbitrary length to a fixed length bit string. Secure hash functions [FIPS180] satisfy the following properties:

1. **One-Way.** It is computationally infeasible to find any input that maps to any pre-specified output.

2. **Collision Resistant.** It is computationally infeasible to find any two distinct inputs that map to the same output.

Identification: The process of discovering the identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items.

Identifier: Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers.

Identity: The set of physical and behavioral characteristics by which an individual is uniquely recognizable.

Identity Proofing: The process of providing sufficient information (e.g., identity history, credentials, documents) to establish an identity.

Identity Management System (IDMS): Identity management system comprised of one or more systems or applications that manages the identity verification, validation, and issuance process.

Identity Registration: The process of making a person's identity known to the PIV system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system.

Identity Verification: The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the PIV Card or system and associated with the identity being claimed.

Interoperability: For the purposes of this Standard, interoperability allows any government facility or information system, regardless of the issuer, to verify a cardholder's identity using the credentials on the PIV Card.

Issuer: The organization that is issuing the PIV Card to an applicant. Typically this is an organization for which the applicant is working.

Key: See "Cryptographic Key."

Match/Matching: The process of comparing biometric information against a previously stored biometric data and scoring the level of similarity.

Model: A very detailed description or scaled representation of one component of a larger system that can be created, operated, and analyzed to predict actual operational characteristics of the final produced component.

Off-Card: Refers to data that is not stored within the PIV Card or to a computation that is not performed by the Integrated Circuit Chip (ICC) of the PIV Card.

On-Card: Refers to data that is stored within the PIV Card or to a computation that is performed by the Integrated Circuit Chip (ICC) of the PIV Card.

On-Card Comparison: Comparison of fingerprint data transmitted to the card with reference data previously stored on the card.

Online Certificate Status Protocol (OCSP): An online protocol used to determine the status of a public key certificate. [RFC2560]

Path Validation: The process of verifying the binding between the subject identifier and subject public key in a certificate, based on the public key of a trust anchor, through the validation of a chain of certificates that begins with a certificate issued by the trust anchor and ends with the target certificate. Successful path validation provides strong evidence that the information in the target certificate is trustworthy.

Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity, such as name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. [OMB0716]

Personal Identification Number (PIN): A secret that a cardholder memorizes and uses to authenticate his or her identity.

Personal Identity Verification (PIV) Card: A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains a PIV Card Application which stores identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

PIV Assurance Level: A degree of confidence established in the identity of the holder of the PIV Card.

Private Key: The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.

Pseudonyms: a name assigned by a Federal department or agency through a formal process to a Federal employee for the purpose of the employee's protection (i.e., the employee might be placed at risk if his or her actual name were known) or for other purposes.

Public Key: The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.

Public Key Infrastructure (PKI): A support service to the PIV system that provides the cryptographic keys needed to perform digital signature-based identity verification and to protect communications and storage of sensitive verification system data within identity cards and the verification system.

PKI-Card Authentication Key (PKI-CAK): A PIV authentication mechanism that is implemented by an asymmetric key challenge/response protocol using the Card Authentication key of the PIV Card and a contact or contactless reader.

PKI-PIV Authentication Key (PKI-AUTH): A PIV authentication mechanism that is implemented by an asymmetric key challenge/response protocol using the PIV Authentication key of the PIV Card and a contact reader, or a contactless card reader that supports the virtual contact interface.

Recommendation: A special publication of the ITL stipulating specific characteristics of technology to use or procedures to follow to achieve a common level of quality or level of interoperability.

Registration: See "Identity Registration."

Symmetric Key: A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code.

Validation: The process of demonstrating that the system under consideration meets in all respects the specification of that system. [INCITS/M1-040211]

Verification: See “Identity Verification.”

C.2 Acronyms

The following acronyms and abbreviations are used throughout this Standard:

ACL	Access Control List
AES	Advanced Encryption Standard
AID	Application IDentifier
AIM	Association for Automatic Identification and Mobility
ANSI	American National Standards Institute
ASN.1	Abstract Syntax Notation One
ASTM	American Society for Testing and Materials
ATO	Authorization to Operate
CA	Certification Authority
CAK	Card Authentication Key
CBEFF	Common Biometric Exchange Formats Framework
CHUID	Cardholder Unique Identifier
cm	Centimeter
CMS	Cryptographic Message Syntax
CMTC	Card Management System to the Card
CMVP	Cryptographic Module Validation Program
COTS	Commercial Off-the-Shelf
CRL	Certificate Revocation List
CSE	Communications Security Establishment
CTC	Cardholder to Card
CTE	Cardholder to External System
DATO	Denial of Authorization to Operate
DHS	Department of Homeland Security
DN	Distinguished Name
DOB	Date of Birth
dpi	Dots Per Inch
ERT	Emergency Response Team
FASC-N	Federal Agency Smart Credential Number
FBCA	Federal Bridge Certification Authority
FBI	Federal Bureau of Investigation
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FIPS PUB	FIPS Publication
FISMA	Federal Information Security Management Act

GSA	U.S. General Services Administration
GUID	Global Unique Identification Number
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
I&A	Identification and Authentication
IAB	Interagency Advisory Board
ICAMSC	Identity, Credential, and Access Management Subcommittee
ICC	Integrated Circuit Chip
ID	Identification
IDMS	Identity Management System
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
INCITS	International Committee for Information Technology Standards
ISO	International Organization for Standardization
IT	Information Technology
ITL	Information Technology Laboratory
LDAP	Lightweight Directory Access Protocol
mm	Millimeter
MWR	Morale, Welfare, and Recreation
NAC	National Agency Check
NACI	National Agency Check with Written Inquiries
NCHC	National Criminal History Check
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NPIVP	NIST Personal Identity Verification Program
NVLAP	National Voluntary Laboratory Accreditation Program
OCC	On-Card Biometric Comparison
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PCI	PIV Card Issuer
PC/SC	Personal Computer/Smart Card
PDF	Portable Data File
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RFC	Request for Comments
SES	Senior Executive Service
SP	Special Publication

SSP	Shared Service Provider
TSA	Transportation Security Administration
URI	Uniform Resource Identifier
U.S.C.	United States Code
UUID	Universally Unique Identifier

C.3 Notations

This Standard uses the following typographical conventions in text:

- ASN.1 data types are represented in *italics*. For example, *SignedData* and *SignerInfo* are data types defined for digital signatures.
- Letters or words in CAPITALS separated with underscore represent CBEFF-compliant data structures. For example, CBEFF_HEADER is a header field in the CBEFF structure.

Appendix D—References

- [ANSI322] ANSI INCITS 322 Information Technology, *Card Durability Test Methods*, ANSI, 2002.
- [CBEFF] NISTIR 6529-A, *Common Biometric Exchange Formats Framework (CBEFF)*, NIST, 2003.
- [COMMON] X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 1.21, December 18, 2012, or as amended. Available at <http://idmanagement.gov/documents/common-policy-framework-certificate-policy>.
- [E-Gov] *E-Government Act of 2002*, U.S. Public Law 107-347, 2002.
- [FIPS140] FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*, NIST, May 25, 2001, or as amended. Available at <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.
- [FIPS180] FIPS Publication 180-4, *Secure Hash Standard (SHS)*, March 2012, or as amended. Available at <http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf>.
- [FISMA] *Federal Information Security Management Act of 2002*. Available at <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>.
- [G155-00] ASTM G155-00, *Standard Practice for Operating Xenon Arc Light Apparatus for Exposure of Non-metallic Materials*, Vol. 14.04, ASTM, July 2000.
- [G90-98] ASTM G90-98, *Standard Practice for Performing Accelerated Outdoor Weathering of Non-metallic Materials Using Concentrated Natural Sunlight*, Vol. 14.04, ASTM, 2003.
- [HSPD-12] HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004.
- [IEC61966] IEC 61966-2-1:1999, *Multimedia systems and equipment - Colour measurement and management - Part 2-1: Colour management - Default RGB colour space – sRGB*, October 1999.
- [INCITS/M1-040211] ANSI/INCITS M1-040211, *Biometric Profile—Interoperability and Data Interchange—Biometrics-Based Verification and Identification of Transportation Workers*, ANSI, April 2004.
- [ISO10373] ISO/IEC 10373, *Identification Cards—Test Methods*. Part 1—*Standard for General Characteristic Test of Identification Cards*, ISO, 1998. Part 3—*Standard for Integrated Circuit Cards with Contacts and Related Interface Devices*, ISO, 2001. Part 6—*Standard for Proximity Card Support in Identification Cards*, ISO, 2001.
- [ISO14443] ISO/IEC 14443-1:2000, *Identification Cards—Contactless Integrated Circuit(s) Cards—Proximity Cards*, ISO, 2000.
- [ISO3166] ISO 3166-1:2006. *Codes for the representation of names of countries and their subdivisions—Part 1: Country codes*.

[ISO7810] ISO/IEC 7810:2003, *Identification Cards—Physical Characteristics*, ISO, 2003.

[ISO7811] ISO/IEC 7811, *Identification cards -- Recording technique. Part 6—Magnetic stripe -- High coercivity*, ISO, 2008. Part 7—*Magnetic stripe -- High coercivity, high density*, ISO, 2004.

[ISO7816] ISO/IEC 7816, *Identification Cards—Integrated Circuits with Contacts*, Parts 1-6, ISO.

[ISO24727] ISO/IEC 24727, *Identification cards -- Integrated circuit card programming interfaces. Part 1—Architecture*, ISO, 2007. Part 2—*Generic card interface*, ISO, 2008. Part 3—*Application interface*, ISO 2008. Part 4—*Application programming interface (API) administration*, ISO, 2008. Part 5—*Testing procedures*, ISO, 2011. Part 6—*Registration authority procedures for the authentication protocols for interoperability*, ISO, 2010.

[NISTIR7863] NISTIR 7863, *Cardholder Authentication for the PIV Digital Signature Key*, NIST.

[OMB0322] OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, OMB, September 26, 2003.

[OMB0404] OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, OMB, December 2003.

[OMB0524] OMB Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, OMB, August 2005.

[OMB0618] OMB Memorandum M-06-18, *Acquisition of Products and Services for Implementation of HSPD-12*, June 2006.

[OMB0716] OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, OMB, May 2007.

[OMB1111] OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors*, February 2011.

[PCSC] Personal Computer/Smart Card Workgroup Specifications. Available at <http://www.pcscworkgroup.com>.

[PRIVACY] *Privacy Act of 1974*, U.S. Public Law 93-579, 1974.

[PROF] *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Provider (SSP) Program*, Version 1.5, January 7, 2008 or as amended. Available at <http://idmanagement.gov/sites/default/files/documents/CertCRLprofileForCP.pdf>.

[RFC2560] RFC 2560, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*, Internet Engineering Task Force (IETF), June 1999. Available at <http://www.ietf.org/rfc/rfc2560.txt>.

[RFC4122] RFC 4122, *A Universally Unique Identifier (UUID) URN Namespace*, Internet Engineering Task Force (IETF), July 2005. Available at <http://www.ietf.org/rfc/rfc4122.txt>.

[RFC5280] RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, IETF, May 2008. Available at <http://www.ietf.org/rfc/rfc5280.txt>.

[RFC5652] RFC 5652, *Cryptographic Message Syntax (CMS)*, IETF, September 2009. Available at <http://www.ietf.org/rfc/rfc5652.txt>.

[SP 800-37] NIST Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, NIST, February 2010 or as amended.

[SP 800-53] NIST Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, NIST, August 2009 or as amended.

[SP 800-59] NIST Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, NIST, August 2003 or as amended.

[SP 800-63] NIST Special Publication 800-63-1, *Electronic Authentication Guideline*, NIST, December 2011 or as amended.

[SP 800-73] NIST Special Publication 800-73-3, *Interfaces for Personal Identity Verification*, NIST, February 2010 or as amended.

[SP 800-76] NIST Special Publication 800-76-2, *Biometric Specifications for Personal Identity Verification*, NIST, July 2013 or as amended.

[SP 800-78] NIST Special Publication 800-78-3, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, NIST, December 2010 or as amended.

[SP 800-79] NIST Special Publication 800-79-1, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*, NIST, June 2008 or as amended.

[SP 800-85A] NIST Special Publication 800-85A-2, *PIV Card Application and Middleware Interface Test Guidelines (SP800-73-3 compliance)*, NIST, July 2010 or as amended.

[SP 800-87] NIST Special Publication 800-87 Revision 1, *Codes for the Identification of Federal and Federally-Assisted Organizations*, NIST, April 2008 or as amended.

[SP 800-96] NIST Special Publication 800-96, *PIV Card to Reader Interoperability Guidelines*, NIST, September 2006 or as amended.

[SP 800-116] NIST Special Publication 800-116, *A Recommendation for the use of PIV Credentials in Physical Access Control Systems (PACS)*, NIST, November 2008 or as amended.

[SP 800-122] NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, NIST, April 2010 or as amended.

[SP 800-156] NIST Special Publication 800-156, *Representation of PIV Chain-of-Trust for Import and Export*, NIST.

[SP 800-157] NIST Special Publication 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, NIST.

[SPRINGER MEMO] Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12, July 31, 2008.

[SSP REP] Shared Service Provider Repository Service Requirements, December 13, 2011, or as amended. Available at <http://idmanagement.gov/documents/shared-service-provider-repository-service-requirements>.

Appendix E—Revision History

The Revision History provides an overview of the changes to FIPS 201 since its initial release.

Version	Release Date	Updates
FIPS 201	February 2005	Initial Release
FIPS 201-1	March 2006	Added the requirement for electronically distinguishable from identity credentials issued to individuals who have a completed investigation (NACI Indicator).
FIPS 201-1 Change Notice 1	March 2006	Added clarification for variable placement of Agency Card Serial Number along the outer edge of the back of the PIV Card is allowed. Also, updated ASN.1 encoding for NACI Indicator (background investigation indicator).
FIPS 201-2	August 2013	<p>This version represents the 5-year review of FIPS 201 and change request inputs received from agencies. Following are the highlights of changes made in this version.</p> <p>Modified the requirement for accreditation of PIV Card issuer to include an independent review.</p> <p>Incorporated references to credentialing guidance and requirements issued by OPM and OMB.</p> <p>Made the facial image data element on the PIV Card mandatory.</p> <p>Added the option to collect and store iris biometric data on the PIV Card.</p> <p>Added option to use electronic facial image for authentication in operator-attended environments.</p> <p>Incorporated the content from Form I-9 that is relevant to FIPS 201.</p> <p>Introduced the concept of a “chain-of-trust” optionally maintained by a PIV Card issuer.</p> <p>Changed the maximum life of PIV Card from 5 years to 6 years.</p> <p>Added requirements for issuing a PIV Card to an individual under a pseudonymous identity.</p> <p>Added requirements for issuing a PIV Card to an individual within grace period.</p> <p>Added requirements for post-issuance updates.</p> <p>Added option to allow for remote PIN resets.</p> <p>Introduced the ability to issue derived PIV credentials.</p> <p>The employee affiliation color-coding and the large expiration date in the upper right-hand corner of the card are now mandatory.</p> <p>Made all four asymmetric keys and certificates mandatory.</p> <p>Introduced the concept of a virtual contact interface over which all functionality of the PIV Card is accessible.</p> <p>Added a mandatory UUID as a unique identifier for the PIV Card in addition to the FASC-N.</p> <p>Added optional on-card biometric comparison as a means of performing card activation and as a PIV authentication mechanism.</p>

		<p>Removed direct requirement to distribute certificates and CRLs via LDAP.</p> <p>Updated authentication mechanisms to enable variations in implementations.</p> <p>Require signature verification and certification path validation in the CHUID, BIO, and BIO-A authentication mechanisms.</p> <p>The VIS and CHUID authentication mechanisms have been downgraded to indicate that they provide LITTLE or NO assurance in the identity of the cardholder.</p> <p>Deprecated the use of the CHUID authentication mechanism. The CHUID data element has not been deprecated and continues to be mandatory.</p>
--	--	--

SOLICITATION PROVISIONS
(Acquisition of Leasehold Interests in Real Property)

1. 552.270 1 INSTRUCTIONS TO OFFERORS - ACQUISITION OF LEASEHOLD INTERESTS
IN REAL PROPERTY (JUN 2011)

(a) Definitions. As used in this provision --

"Discussions" are negotiations that occur after establishment of the competitive range that may, at the Contracting Officer's discretion, result in the offeror being allowed to revise its proposal.

"In writing, writing or written" means any worded or numbered expression that can be read, reproduced, and later communicated, and includes electronically transmitted and stored information.

"Proposal modification" is a change made to a proposal before the solicitation's closing date and time, or made in response to an amendment, or made to correct a mistake at any time before award.

"Proposal revision" is a change to a proposal made after the solicitation closing date, at the request of or as allowed by a Contracting Officer as the result of negotiations.

"Time," if stated as a number of days, is calculated using calendar days, unless otherwise specified, and will include Saturdays, Sundays, and legal holidays. However, if the last day falls on a Saturday, Sunday, or legal holiday, then the period shall include the next working day.

(b) Amendments to solicitations. If this solicitation is amended, all terms and conditions that are not amended remain unchanged. Offerors shall acknowledge receipt of any amendment to this solicitation by the date and time specified in the amendment(s).

(c) Submission, modification, revision, and withdrawal of proposals.

(1) Unless other methods (e.g., electronic commerce or facsimile) are permitted in the solicitation, proposals and modifications to proposals shall be submitted in paper media in sealed envelopes or packages. Offers must be:

(i) Submitted on the forms prescribed and furnished by the Government as a part of this solicitation or on copies of those forms, and

(ii) Signed. The person signing an offer must initial each erasure or change appearing on any offer form. If the offeror is a partnership, the names of the partners composing the firm must be included with the offer.

(2) Late proposals and revisions.

(i) The Government will not consider any proposal received at the office designated in the solicitation after the exact time specified for receipt of offers unless it is received before the Government makes award and it meets at least one of the following conditions:

(A) It was sent by registered or certified mail not later than the fifth calendar day before the date specified for receipt of offers (e.g., an offer submitted in response to a solicitation requiring receipt of offers by the 20th of the month must have been mailed by the 15th).

(B) It was sent by mail (or telegram or facsimile, if authorized) or hand-carried (including delivery by a commercial carrier) if it is determined by the Government that the late receipt was due primarily to Government mishandling after receipt at the Government installation.

(C) It was sent by U.S. Postal Service Express Mail Next Day Service-Post Office to Addressee, not later than 5:00 p.m. at the place of mailing two working days prior to the date specified for receipt of proposals. The term "working days" excludes weekends and U.S. Federal holidays.

(D) It was transmitted through an electronic commerce method authorized by the solicitation and was received at the initial point of entry to the Government infrastructure not later than 5:00 p.m. one working day prior to the date specified for receipt of proposals.

(E) There is acceptable evidence to establish that it was received at the activity designated for receipt of offers and was under the Government's control prior to the time set for receipt of offers, and that the Contracting Officer determines that accepting the late offer would not unduly delay the procurement.

(F) It is the only proposal received.

(ii) Any modification or revision of a proposal or response to request for information, including any final proposal revision, is subject to the same conditions as in paragraphs (c)(2)(i)(A) through (c)(2)(i)(E) of this provision.

(iii) The only acceptable evidence to establish the date of mailing of a late proposal or modification or revision sent either by registered or certified mail is the U.S. or Canadian Postal Service postmark both on the envelope or wrapper and on the original receipt from the U.S. or Canadian Postal Service. Both postmarks must show a legible date or the proposal, response to a request for information, or modification or revision shall be processed as if mailed late. "Postmark" means a printed, stamped, or otherwise placed impression (exclusive of a postage meter machine impression) that is readily identifiable without further action as having been supplied and affixed by employees of the U.S. or Canadian Postal Service on the date of mailing. Therefore, offerors or respondents should request the postal clerk to place a legible hand cancellation bull's eye postmark on both the receipt and the envelope or wrapper.

(iv) Acceptable evidence to establish the time of receipt at the Government installation includes the time/date stamp of that installation on the proposal wrapper, other documentary evidence of receipt maintained by the installation, or oral testimony or statements of Government personnel.

(v) The only acceptable evidence to establish the date of mailing of a late offer, modification or revision, or withdrawal sent by Express Mail Next Day Service-Post Office to Addressee is the date entered by the post office receiving clerk on the "Express Mail Next Day Service-Post Office to Addressee" label and the postmark on both the envelope or wrapper and on the original receipt from the U.S. Postal Service. "Postmark" has the same meaning as defined in paragraph (c)(2)(iii) of this provision, excluding postmarks of the Canadian Postal Service. Therefore, offerors or respondents should request the postal clerk to place a legible hand cancellation bull's eye postmark on both the receipt and the envelope or wrapper.

(vi) Notwithstanding paragraph (c)(2)(i) of this provision, a late modification or revision of an otherwise successful proposal that makes its terms more favorable to the Government will be considered at any time it is received and may be accepted.

(vii) An offeror may withdraw its proposal by written notice or telegram (including mailgram) received at any time before award. If the solicitation authorizes facsimile proposals, an offeror may withdraw its proposal via facsimile received at any time before award, subject to the conditions specified in the provision entitled "Facsimile Proposals." Proposals may be withdrawn in person by an offeror or an authorized representative, if the representative's identity is made known and the representative signs a receipt for the proposal before award.

(viii) If an emergency or unanticipated event interrupts normal Government processes so that proposals cannot be received at the office designated for receipt of proposals by the exact time specified in the solicitation, and urgent Government requirements preclude amendment of the solicitation or other notice of an extension of the closing date, the time specified for receipt of proposals will be deemed to be extended to the same time of day specified in the solicitation on the first work day on which normal Government processes resume. If no time is specified in the solicitation, the time for receipt is 4:30 p.m., local time, for the designated Government office.

(3) Any information given to a prospective offeror concerning this solicitation will be furnished promptly to all other prospective offerors, if that information is necessary in submitting offers or if the lack of it would be prejudicial to any other prospective offeror.

(4) Offerors may submit modifications to their proposals at any time before the solicitation closing date and time, and may submit modifications in response to an amendment, or to correct a mistake at any time before award.

(5) Offerors may submit revised proposals only if requested or allowed by the Contracting Officer.

(6) The Government will construe an offer to be in full and complete compliance with this solicitation unless the offer describes any deviation in the offer.

(7) Offerors may submit proposals that depart from stated requirements. Such a proposal shall clearly identify why the acceptance of the proposal would be advantageous to the Government. The proposal must clearly identify and explicitly define any deviations from the terms and conditions of the solicitation, as well as the comparative advantage to the Government. The Government reserves the right to amend the solicitation to allow all offerors an opportunity to submit revised proposals based on the revised requirements.

(d) Restriction on disclosure and use of data. An offeror that includes in its proposal data that it does not want disclosed to the public for any purpose, or used by the Government except for evaluation purposes, must meet both of the following conditions:

(1) Mark the title page with the following legend:

This proposal includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed --in whole or in part --for any purpose other than to evaluate this proposal. If, however, a lease is awarded to this offeror as a result of --or in connection with --the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained in sheets *[insert numbers or other identification of sheets]*.

(2) Mark each sheet of data it wishes to restrict with the following legend:

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.

(e) *Lease award.*

(1) The Government intends to award a lease resulting from this solicitation to the responsible offeror whose proposal represents the best value after evaluation in accordance with the factors and subfactors in the solicitation.

(2) The Government may reject any or all proposals if such action is in the Government's interest.

(3) The Government may waive informalities and minor irregularities in proposals received.

(4) The Government intends to evaluate proposals and award a lease after conducting discussions with offerors whose proposals have been determined to be within the competitive range. If the Contracting Officer determines that the number of proposals that would otherwise be in the competitive range exceeds the number at which an efficient competition can be conducted, the Contracting Officer may limit the number of proposals in the competitive range to the greatest number that will permit an efficient competition among the most highly rated proposals. Therefore, the offeror's initial proposal should contain the offeror's best terms from a price and technical standpoint.

(5) Exchanges with offerors after receipt of a proposal do not constitute a rejection or counteroffer by the Government.

(6) The Government may determine that a proposal is unacceptable if the prices proposed are materially unbalanced between line items or subline items. Unbalanced pricing exists when, despite an acceptable total evaluated price, the price of one or more contract line items is significantly overstated or understated as indicated by the application of cost or price analysis techniques. A proposal may be rejected if the Contracting Officer determines that the lack of balance poses an unacceptable risk to the Government.

(7)) The execution and delivery of the Lease contract by the Government establishes a valid award and contract.

(8) The Government may disclose the following information in postaward debriefings to other offerors:

- (i) The overall evaluated cost or price and technical rating of the successful offeror;
- (ii) The overall ranking of all offerors, when any ranking was developed by the agency during source selection; and
- (iii) A summary of the rationale for award.

(f) *Paperwork collection.* The information collection requirements contained in this solicitation/contract are either required by regulation or approved by the Office of Management and Budget pursuant to the Paperwork Reduction Act and assigned OMB Control No. 3090-0163.

2. 52.222_24 _ PREAWARD ON-SITE EQUAL OPPORTUNITY COMPLIANCE EVALUATION (FEB 1999)

If a contract in the amount of \$10 million or more will result from this solicitation, the prospective Contractor and its known first-tier subcontractors with anticipated subcontracts of \$10 million or more shall be subject to a preaward compliance evaluation by the Office of Federal Contract Compliance Programs (OFCCP), unless, within the preceding 24 months, OFCCP has conducted an evaluation and found the prospective Contractor and subcontractors to be in compliance with Executive Order 11246.

3. 552.270_3 _ PARTIES TO EXECUTE LEASE (JUN 2011)

(a) If the lessor is an individual, that individual shall sign the lease. A lease with an individual doing business as a firm shall be signed by that individual, and the signature shall be followed by the individual's typed, stamped, or printed name and the words, "an individual doing business as

_____ [insert name of firm]."

(b) If the Lessor is a corporation, the lease must be signed in the corporate name, followed by the signature and title of the officer or other person signing the lease on its behalf, duly attested, and, evidence of this authority to so act shall be furnished.

(c) If the Lessor is a corporation, the lease must be signed in the corporate name, followed by the signature and title of the officer or other person signing the lease on its behalf, duly attested, and, if requested by the Government, evidence of this authority to so act shall be furnished.

d) If the Lessor is a joint venture, the lease must be signed by each participant in the joint venture in the manner prescribed in paragraphs (a) through (c) of this provision for each type of participant. When a corporation is participating in the joint venture, the corporation shall provide evidence that the corporation is authorized to participate in the joint venture.

(e) If the lease is executed by an attorney, agent, or trustee on behalf of the Lessor, an authenticated copy of the power of attorney, or other evidence to act on behalf of the Lessor, must accompany the lease.

4. 52.233_2 _ SERVICE OF PROTEST (SEP 2006) (VARIATION)

(Applies to leases over \$150,000 average net annual rental, including option periods.)

(a) Protests, as defined in section 33.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), shall be served on the Contracting Officer by obtaining written and dated acknowledgment of receipt from the Contracting Officer at the address shown elsewhere in this solicitation.

(b) The copy of any protest shall be received in the office designated above within one day of filing a protest with the GAO.

5. 52.215-5 - FACSIMILE PROPOSALS (OCT 1997)

(a) Definition. "Facsimile proposal," as used in this provision, means a proposal, revision or modification of a proposal, or withdrawal of a proposal that is transmitted to and received by the Government via facsimile machine.

(b) Offerors may submit facsimile proposals as responses to this solicitation. Facsimile proposals are subject to the same rules as paper proposals.

- (c) The telephone number of receiving facsimile equipment is: [insert telephone number].
- (d) If any portion of a facsimile proposal received by the Contracting Officer is unreadable to the degree that conformance to the essential requirements of the solicitation cannot be ascertained from the document--
 - (1) The Contracting Officer immediately shall notify the offeror and permit the offeror to resubmit the proposal;
 - (2) The method and time for resubmission shall be prescribed by the Contracting Officer after consultation with the offeror; and
 - (3) The resubmission shall be considered as if it were received at the date and time of the original unreadable submission for the purpose of determining timeliness, provided the offeror complies with the time and format requirements for resubmission prescribed by the Contracting Officer.
- (e) The Government reserves the right to make award solely on the facsimile proposal. However, if requested to do so by the Contracting Officer, the apparently successful offeror promptly shall submit the complete original signed proposal.

6. FLOOD PLAINS (JUN 2012)

A Lease will not be awarded for any offered Property located within a 100-year floodplain unless the Government has determined that there is no practicable alternative. An Offeror may offer less than its entire site in order to exclude a portion of the site that falls within a floodplain, so long as the portion offered meets all the requirements of this RLP. If an Offeror intends that the offered Property that will become the Premises for purposes of this Lease will be something other than the entire site as recorded in tax or other property records the Offeror shall clearly demarcate the offered Property on its site plan/map submissions and shall propose an adjustment to property taxes on an appropriate pro rata basis. For such an offer, the LCO may, in his or her sole discretion, determine that the offered Property does not adequately avoid development in a 100-year floodplain.

GENERAL CLAUSES
(Acquisition of Leasehold Interests in Real Property)

CATEGORY	CLAUSE NO.	48 CFR REF.	CLAUSE TITLE
GENERAL	1		SUBLETTING AND ASSIGNMENT
	2	552.270-11	SUCCESSORS BOUND
	3	552.270-23	SUBORDINATION, NON-DISTURBANCE AND ATTORNMEN
	4	552.270-24	STATEMENT OF LEASE
	5	552.270-25	SUBSTITUTION OF TENANT AGENCY
	6	552.270-26	NO WAIVER
	7		INTEGRATED AGREEMENT
	8	552.270-28	MUTUALITY OF OBLIGATION
PERFORMANCE	9		DELIVERY AND CONDITION
	10		DEFAULT BY LESSOR
	11	552.270-19	PROGRESSIVE OCCUPANCY
	12		MAINTENANCE OF THE PROPERTY, RIGHT TO INSPECT
	13		FIRE AND CASUALTY DAMAGE
	14		COMPLIANCE WITH APPLICABLE LAW
	15	552.270-12	ALTERATIONS
	16		ACCEPTANCE OF SPACE AND CERTIFICATE OF OCCUPANCY
PAYMENT	17	52.204-7	SYSTEM FOR AWARD MANAGEMENT
	18	52.204-13	SYSTEM FOR AWARD MANAGEMENT
	19	552.270-31	MAINTENANCE
	20	52.232-23	PROMPT PAYMENT
	21		ASSIGNMENT OF CLAIMS
	22	52.232-33	PAYMENT
STANDARDS OF CONDUCT	23	52.203-13	PAYMENT BY ELECTRONIC FUNDS TRANSFER—SYSTEM FOR AWARD MANAGEMENT
	24	52.203-13	CONTRACTOR CODE OF BUSINESS ETHICS AND CONDUCT
	25	552.270-32	COVENANT AGAINST CONTINGENT FEES
	26	52-203-7	ANTI-KICKBACK PROCEDURES
	27	52-223-6	DRUG-FREE WORKPLACE
	28	52.203-14	DISPLAY OF HOTLINE POSTER(S)
ADJUSTMENTS	29	552.270-30	PRICE ADJUSTMENT FOR ILLEGAL OR IMPROPER ACTIVITY
	30	52.215-10	PRICE REDUCTION FOR DEFECTIVE COST OR PRICING DATA
	31	552.270-13	PROPOSALS FOR ADJUSTMENT
	32		CHANGES
AUDITS	33	552.215-70	EXAMINATION OF RECORDS BY GSA
	34	52.215-2	AUDIT AND RECORDS—NEGOTIATION

INITIALS: LESSOR _____ & _____
 GOVERNMENT

DISPUTES	34	52.233-1	DISPUTES
LABOR STANDARDS	35	52.222-26	EQUAL OPPORTUNITY
	36	52.222-21	PROHIBITION OF SEGREGATED FACILITIES
	37	52.219-28	POST-AWARD SMALL BUSINESS PROGRAM
	38	52.222-35	REREPRESENTATION
	39	52.222-36	EQUAL OPPORTUNITY FOR VETERANS
	40	52.222-37	EQUAL OPPORTUNITY FOR WORKERS WITH DISABILITIES
	40	52.222-37	EMPLOYMENT REPORTS ON VETERANS
SUBCONTRACTING	41	52.209-6	PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, OR PROPOSED FOR DEBARMENT
	42	52.215-12	SUBCONTRACTOR CERTIFIED COST OR PRICING DATA
	43	52.219-8	UTILIZATION OF SMALL BUSINESS CONCERNS
	44	52.219-9	SMALL BUSINESS SUBCONTRACTING PLAN
	45	52.219-16	LIQUIDATED DAMAGES—SUBCONTRACTING PLAN
	46	52.204-10	REPORTING EXECUTIVE COMPENSATION AND FIRST-TIER SUBCONTRACT AWARDS
	47	552.219-73	GOALS FOR SUBCONTRACTING PLAN

The information collection requirements contained in this solicitation/contract that are not required by regulation have been approved by the Office of Management and Budget (OMB) pursuant to the Paperwork Reduction Act and assigned the OMB Control Number 3090-0163.

INITIALS: _____ & _____
LESSOR GOVERNMENT

GENERAL CLAUSES
(Acquisition of Leasehold Interests in Real Property)

1. SUBLETTING AND ASSIGNMENT (JAN 2011)

The Government may sublet any part of the premises but shall not be relieved from any obligations under this lease by reason of any such subletting. The Government may at any time assign this lease, and be relieved from all obligations to Lessor under this lease excepting only unpaid rent and other liabilities, if any, that have accrued to the date of said assignment. Any subletting or assignment shall be subject to prior written consent of Lessor, which shall not be unreasonably withheld.

2. 552.270-11 SUCCESSORS BOUND (SEP 1999)

This lease shall bind, and inure to the benefit of, the parties and their respective heirs, executors, administrators, successors, and assigns.

3. 552.270-23 SUBORDINATION, NON-DISTURBANCE AND ATTORNMENT (SEP 1999)

(a) Lessor warrants that it holds such title to or other interest in the premises and other property as is necessary to the Government's access to the premises and full use and enjoyment thereof in accordance with the provisions of this lease. Government agrees, in consideration of the warranties and conditions set forth in this clause, that this lease is subject and subordinate to any and all recorded mortgages, deeds of trust and other liens now or hereafter existing or imposed upon the premises, and to any renewal, modification or extension thereof. It is the intention of the parties that this provision shall be self-operative and that no further instrument shall be required to effect the present or subsequent subordination of this lease. Government agrees, however, within twenty (20) business days next following the Contracting Officer's receipt of a written demand, to execute such instruments as Lessor may reasonably request to evidence further the subordination of this lease to any existing or future mortgage, deed of trust or other security interest pertaining to the premises, and to any water, sewer or access easement necessary or desirable to serve the premises or adjoining property owned in whole or in part by Lessor if such easement does not interfere with the full enjoyment of any right granted the Government under this lease.

(b) No such subordination, to either existing or future mortgages, deeds of trust or other lien or security instrument shall operate to affect adversely any right of the Government under this lease so long as the Government is not in default under this lease. Lessor will include in any future mortgage, deed of trust or other security instrument to which this lease becomes subordinate, or in a separate non-disturbance agreement, a provision to the foregoing effect. Lessor warrants that the holders of all notes or other obligations secured by existing mortgages, deeds of trust or other security instruments have consented to the provisions of this clause, and agrees to provide true copies of all such consents to the Contracting Officer promptly upon demand.

(c) In the event of any sale of the premises or any portion thereof by foreclosure of the lien of any such mortgage, deed of trust or other security instrument, or the giving of a deed in lieu of foreclosure, the Government will be deemed to have attorned to any purchaser, purchasers, transferee or transferees of the premises or any portion thereof and its or their successors and assigns, and any such purchasers and transferees will be deemed to have assumed all obligations of the Lessor under this lease, so as to establish direct privity of estate and contract between Government and such purchasers or transferees, with the same force, effect and relative priority in time and right as if the lease had initially been entered into between such purchasers or transferees and the Government; provided, further, that the Contracting Officer and such purchasers or transferees shall, with reasonable promptness following any such sale or deed delivery in lieu of foreclosure, execute all such revisions to this lease, or other writings, as shall be necessary to document the foregoing relationship.

(d) None of the foregoing provisions may be deemed or construed to imply a waiver of the Government's rights as a sovereign.

INITIALS: _____ & _____
LESSOR GOVERNMENT

4. 552.270-24 STATEMENT OF LEASE (SEP 1999)

(a) The Contracting Officer will, within thirty (30) days next following the Contracting Officer's receipt of a joint written request from Lessor and a prospective lender or purchaser of the building, execute and deliver to Lessor a letter stating that the same is issued subject to the conditions stated in this clause and, if such is the case, that (1) the lease is in full force and effect; (2) the date to which the rent and other charges have been paid in advance, if any; and (3) whether any notice of default has been issued.

(b) Letters issued pursuant to this clause are subject to the following conditions:

(1) That they are based solely upon a reasonably diligent review of the Contracting Officer's lease file as of the date of issuance;

(2) That the Government shall not be held liable because of any defect in or condition of the premises or building;

(3) That the Contracting Officer does not warrant or represent that the premises or building comply with applicable Federal, State and local law; and

(4) That the Lessor, and each prospective lender and purchaser are deemed to have constructive notice of such facts as would be ascertainable by reasonable pre-purchase and pre-commitment inspection of the Premises and Building and by inquiry to appropriate Federal, State and local Government officials.

5. 552.270-25 SUBSTITUTION OF TENANT AGENCY (SEP 1999)

The Government may, at any time and from time to time, substitute any Government agency or agencies for the Government agency or agencies, if any, named in the lease.

6. 552.270-26 NO WAIVER (SEP 1999)

No failure by either party to insist upon the strict performance of any provision of this lease or to exercise any right or remedy consequent upon a breach thereof, and no acceptance of full or partial rent or other performance by either party during the continuance of any such breach shall constitute a waiver of any such breach of such provision.

7. INTEGRATED AGREEMENT (JUN 2012)

This Lease, upon execution, contains the entire agreement of the parties and no prior written or oral agreement, express or implied, shall be admissible to contradict the provisions of the Lease. Except as expressly attached to and made a part of the Lease, neither the Request for Lease Proposals nor any pre-award communications by either party shall be incorporated in the Lease.

8. 552.270-28 MUTUALITY OF OBLIGATION (SEP 1999)

The obligations and covenants of the Lessor, and the Government's obligation to pay rent and other Government obligations and covenants, arising under or related to this Lease, are interdependent. The Government may, upon issuance of and delivery to Lessor of a final decision asserting a claim against Lessor, set off such claim, in whole or in part, as against any payment or payments then or thereafter due the Lessor under this lease. No setoff pursuant to this clause shall constitute a breach by the Government of this lease.

9. DELIVERY AND CONDITION (JAN 2011)

(a) Unless the Government elects to have the space occupied in increments, the space must be delivered ready for occupancy as a complete unit.

INITIALS: _____ & _____
LESSOR GOVERNMENT

(b) The Government may elect to accept the Space notwithstanding the Lessor's failure to deliver the Space substantially complete; if the Government so elects, it may reduce the rent payments.

10. DEFAULT BY LESSOR (APR 2012)

(a) The following conditions shall constitute default by the Lessor, and shall give rise to the following rights and remedies for the Government:

(1) Prior to Acceptance of the Premises. Failure by the Lessor to diligently perform all obligations required for Acceptance of the Space within the times specified, without excuse, shall constitute a default by the Lessor. Subject to provision of notice of default to the Lessor, and provision of a reasonable opportunity for the Lessor to cure its default, the Government may terminate the Lease on account of the Lessor's default.

(2) After Acceptance of the Premises. Failure by the Lessor to perform any service, to provide any item, or satisfy any requirement of this Lease, without excuse, shall constitute a default by the Lessor. Subject to provision of notice of default to the Lessor, and provision of a reasonable opportunity for the Lessor to cure its default, the Government may perform the service, provide the item, or obtain satisfaction of the requirement by its own employees or contractors. If the Government elects to take such action, the Government may deduct from rental payments its costs incurred in connection with taking the action. Alternatively, the Government may reduce the rent by an amount reasonably calculated to approximate the cost or value of the service not performed, item not provided, or requirement not satisfied, such reduction effective as of the date of the commencement of the default condition.

(3) Grounds for Termination. The Government may terminate the Lease if:

(i) The Lessor's default persists notwithstanding provision of notice and reasonable opportunity to cure by the Government, or

(ii) The Lessor fails to take such actions as are necessary to prevent the recurrence of default conditions,

and such conditions (i) or (ii) substantially impair the safe and healthful occupancy of the Premises, or render the Space unusable for its intended purposes.

(4) Excuse. Failure by the Lessor to timely deliver the Space or perform any service, provide any item, or satisfy any requirement of this Lease shall not be excused if its failure in performance arises from:

(i) Circumstances within the Lessor's control;

(ii) Circumstances about which the Lessor had actual or constructive knowledge prior to the Lease Award Date that could reasonably be expected to affect the Lessor's capability to perform, regardless of the Government's knowledge of such matters;

(iii) The condition of the Property;

(iv) The acts or omissions of the Lessor, its employees, agents or contractors; or

(v) The Lessor's inability to obtain sufficient financial resources to perform its obligations.

(5) The rights and remedies specified in this clause are in addition to any and all remedies to which the Government may be entitled as a matter of law.

INITIALS: _____ & _____
LESSOR GOVERNMENT

it as a tenant under this lease, provided that nothing in this Lease shall be construed as a waiver of the sovereign immunity of the Government. This Lease shall be governed by Federal law.

15. 552.270-12 ALTERATIONS (SEP 1999)

The Government shall have the right during the existence of this lease to make alterations, attach fixtures, and erect structures or signs in or upon the premises hereby leased, which fixtures, additions or structures so placed in, on, upon, or attached to the said premises shall be and remain the property of the Government and may be removed or otherwise disposed of by the Government. If the lease contemplates that the Government is the sole occupant of the building, for purposes of this clause, the leased premises include the land on which the building is sited and the building itself. Otherwise, the Government shall have the right to tie into or make any physical connection with any structure located on the property as is reasonably necessary for appropriate utilization of the leased space.

16. ACCEPTANCE OF SPACE AND CERTIFICATE OF OCCUPANCY (APR 2015)

(a) Ten (10) working days prior to the completion of the Space, the Lessor shall issue written notice to the Government to schedule the inspection of the Space for acceptance. The Government shall accept the Space only if the construction of building shell and TIs conforming to this Lease and the approved DIDs is substantially complete, and a Certificate of Occupancy has been issued as set forth below.

(b) The Space shall be considered substantially complete only if the Space may be used for its intended purpose and completion of remaining work will not unreasonably interfere with the Government's enjoyment of the Space. Acceptance shall be final and binding upon the Government with respect to conformance of the completed TIs to the approved DIDs, with the exception of items identified on a punchlist generated as a result of the inspection, concealed conditions, latent defects, or fraud, but shall not relieve the Lessor of any other Lease requirements.

(c) The Lessor shall provide a valid Certificate of Occupancy, issued by the local jurisdiction, for the intended use of the Government. If the local jurisdiction does not issue Certificates of Occupancy or if the Certificate of Occupancy is not available, the Lessor may satisfy this condition by providing a report prepared by a licensed fire protection engineer that indicates that the Space and Building are compliant with all applicable local codes and ordinances and all fire protection and life safety-related requirements of this Lease to ensure an acceptable level of safety is provided. Under such circumstances, the Government shall only accept the Space without a Certificate of Occupancy if a licensed fire protection engineer determines that the offered space is compliant with all applicable local codes and ordinances and fire protection and life safety-related requirements of this Lease.

17. 52.204-7 SYSTEM FOR AWARD MANAGEMENT (JUL 2013)

This clause is incorporated by reference.

18. 52.204-13 SYSTEM FOR AWARD MANAGEMENT MAINTENANCE (JUL 2013)

This clause is incorporated by reference.

19. 552.270-31 PROMPT PAYMENT (JUN 2011)

The Government will make payments under the terms and conditions specified in this clause. Payment shall be considered as being made on the day a check is dated or an electronic funds transfer is made. All days referred to in this clause are calendar days, unless otherwise specified.

(a) *Payment due date* —

(1) *Rental payments.* Rent shall be paid monthly in arrears and will be due on the first workday of each month, and only as provided for by the lease.

INITIALS: _____ & _____
LESSOR GOVERNMENT

(i) When the date for commencement of rent falls on the 15th day of the month or earlier, the initial monthly rental payment under this contract shall become due on the first workday of the month following the month in which the commencement of the rent is effective.

(ii) When the date for commencement of rent falls after the 15th day of the month, the initial monthly rental payment under this contract shall become due on the first workday of the second month following the month in which the commencement of the rent is effective.

(2) *Other payments.* The due date for making payments other than rent shall be the later of the following two events:

(i) The 30th day after the designated billing office has received a proper invoice from the Contractor.

(ii) The 30th day after Government acceptance of the work or service. However, if the designated billing office fails to annotate the invoice with the actual date of receipt, the invoice payment due date shall be deemed to be the 30th day after the Contractor's invoice is dated, provided a proper invoice is received and there is no disagreement over quantity, quality, or Contractor compliance with contract requirements.

(b) *Invoice and inspection requirements for payments other than rent.*

(1) The Contractor shall prepare and submit an invoice to the designated billing office after completion of the work. A proper invoice shall include the following items:

(i) Name and address of the Contractor.

(ii) Invoice date.

(iii) Lease number.

(iv) Government's order number or other authorization.

(v) Description, price, and quantity of work or services delivered.

(vi) Name and address of Contractor official to whom payment is to be sent (must be the same as that in the remittance address in the lease or the order).

(vii) Name (where practicable), title, phone number, and mailing address of person to be notified in the event of a defective invoice.

(2) The Government will inspect and determine the acceptability of the work performed or services delivered within seven days after the receipt of a proper invoice or notification of completion of the work or services unless a different period is specified at the time the order is placed. If actual acceptance occurs later, for the purpose of determining the payment due date and calculation of interest, acceptance will be deemed to occur on the last day of the seven day inspection period. If the work or service is rejected for failure to conform to the technical requirements of the contract, the seven days will be counted beginning with receipt of a new invoice or notification. In either case, the Contractor is not entitled to any payment or interest unless actual acceptance by the Government occurs.

(c) *Interest Penalty.*

(1) An interest penalty shall be paid automatically by the Government, without request from the Contractor, if payment is not made by the due date.

(2) The interest penalty shall be at the rate established by the Secretary of the Treasury under Section 12 of the Contract Disputes Act of 1978 (41 U.S.C. 611) that is in effect on the day after the due date. This rate is referred to as the "Renegotiation Board Interest Rate," and it is published in the **Federal Register**

INITIALS: _____ & _____
LESSOR GOVERNMENT

semiannually on or about January 1 and July 1. The interest penalty shall accrue daily on the payment amount approved by the Government and be compounded in 30-day increments inclusive from the first day after the due date through the payment date.

(3) Interest penalties will not continue to accrue after the filing of a claim for such penalties under the clause at 52.233-1, Disputes, or for more than one year. Interest penalties of less than \$1.00 need not be paid.

(4) Interest penalties are not required on payment delays due to disagreement between the Government and Contractor over the payment amount or other issues involving contract compliance or on amounts temporarily withheld or retained in accordance with the terms of the contract. Claims involving disputes, and any interest that may be payable, will be resolved in accordance with the clause at 52.233-1, Disputes.

(d) *Overpayments.* If the Lessor becomes aware of a duplicate payment or that the Government has otherwise overpaid on a payment, the Contractor shall—

(1) Return the overpayment amount to the payment office cited in the contract along with a description of the overpayment including the—

(i) Circumstances of the overpayment (e.g., duplicate payment, erroneous payment, liquidation errors, date(s) of overpayment);

(ii) Affected lease number; (iii) Affected lease line item or sub-line item, if applicable; and

(iii) Lessor point of contact.

(2) Provide a copy of the remittance and supporting documentation to the Contracting Officer.

20. 52.232-23 ASSIGNMENT OF CLAIMS (MAY 2014)

(Applicable to leases over the micro-purchase threshold.)

(a) The Contractor, under the Assignment of Claims Act, as amended, [31 U.S.C. 3727](#), [41 U.S.C.6305](#) (hereafter referred to as “the Act”), may assign its rights to be paid amounts due or to become due as a result of the performance of this contract to a bank, trust company, or other financing institution, including any Federal lending agency. The assignee under such an assignment may thereafter further assign or reassign its right under the original assignment to any type of financing institution described in the preceding sentence.

(b) Any assignment or reassignment authorized under the Act and this clause shall cover all unpaid amounts payable under this contract, and shall not be made to more than one party, except that an assignment or reassignment may be made to one party as agent or trustee for two or more parties participating in the financing of this contract.

(c) The Contractor shall not furnish or disclose to any assignee under this contract any classified document (including this contract) or information related to work under this contract until the Contracting Officer authorizes such action in writing.

21. PAYMENT (MAY 2011)

(a) When space is offered and accepted, the amount of American National Standards Institute/Building Owners and Managers Association Office Area (ABOA) square footage delivered will be confirmed by:

(1) The Government’s measurement of plans submitted by the successful Offeror as approved by the Government, and an inspection of the space to verify that the delivered space is in conformance with such

INITIALS: _____ & _____
LESSOR GOVERNMENT

plans or

(2) A mutual on-site measurement of the space, if the Contracting Officer determines that it is necessary.

(b)(b) Payment will not be made for space which is in excess of the amount of ABOA square footage stated in the lease.

(c) If it is determined that the amount of ABOA square footage actually delivered is less than the amount agreed to in the lease, the lease will be modified to reflect the amount of ABOA space delivered and the annual rental will be adjusted as follows:

ABOA square feet not delivered multiplied by one plus the common area factor (CAF), multiplied by the rate per rentable square foot (RSF). That is: $(1+CAF) \times \text{Rate per RSF} = \text{Reduction in Annual Rent}$

22. 52.232-33 PAYMENT BY ELECTRONIC FUNDS TRANSFER—SYSTEM FOR AWARD MANAGEMENT (JUL 2013)

This clause is incorporated by reference.

23. 52.203-13 CONTRACTOR CODE OF BUSINESS ETHICS AND CONDUCT (OCT 2015)

(Applicable to leases over \$5.5 million total contract value and performance period is 120 days or more.)

This clause is incorporated by reference.

24. 552.270-32 COVENANT AGAINST CONTINGENT FEES (JUN 2011)

(Applicable to leases over the Simplified Lease Acquisition Threshold.)

(a) The Contractor warrants that no person or agency has been employed or retained to solicit or obtain this contract upon an agreement or understanding for a contingent fee, except a bona fide employee or agency. For breach or violation of this warranty, the Government shall have the right to annul this contract without liability or, in its discretion, to deduct from the contract price or consideration, or otherwise recover the full amount of the contingent fee.

(b) *Bona fide agency*, as used in this clause, means an established commercial or selling agency (including licensed real estate agents or brokers), maintained by a Contractor for the purpose of securing business, that neither exerts nor proposes to exert improper influence to solicit or obtain Government contracts nor holds itself out as being able to obtain any Government contract or contracts through improper influence.

(1) *Bona fide employee*, as used in this clause, means a person, employed by a Contractor and subject to the Contractor’s supervision and control as to time, place, and manner of performance, who neither exerts nor proposes to exert improper influence to solicit or obtain Government contracts nor holds out as being able to obtain any Government contract or contracts through improper influence.

(2) *Contingent fee*, as used in this clause, means any commission, percentage, brokerage, or other fee that is contingent upon the success that a person or concern has in securing a Government contract.

(3) *Improper influence*, as used in this clause, means any influence that induces or tends to induce a *Government* employee or officer to give consideration or to act regarding a Government contract on any basis other than the merits of the matter.

25. 52.203-7 ANTI-KICKBACK PROCEDURES (MAY 2014)

(Applicable to leases over the Simplified Lease Acquisition Threshold.)

This clause is incorporated by reference.

INITIALS: _____ & _____
LESSOR GOVERNMENT

26. 52.223-6 DRUG-FREE WORKPLACE (MAY 2001)

(Applicable to leases over the Simplified Lease Acquisition Threshold, as well as to leases of any value awarded to an individual.)

This clause is incorporated by reference.

27. 52.203-14 DISPLAY OF HOTLINE POSTER(S) (OCT 2015)

(Applicable to leases over \$5.5 Million total contract value and performance period is 120 days or more.)

(a) Definition.

“United States,” as used in this clause, means the 50 States, the District of Columbia, and outlying areas.

(b) Display of fraud hotline poster(s). Except as provided in paragraph (c)—

(1) During contract performance in the United States, the Contractor shall prominently display in common work areas within business segments performing work under this contract and at contract work sites—

(i) Any agency fraud hotline poster or Department of Homeland Security (DHS) fraud hotline poster identified in paragraph (b)(3) of this clause; and

(ii) Any DHS fraud hotline poster subsequently identified by the Contracting Officer.

(2) Additionally, if the Contractor maintains a company website as a method of providing information to employees, the Contractor shall display an electronic version of the poster(s) at the website.

(3) Any required posters may be obtained as follows:

Poster(s)	Obtain from
GSA Office of Inspector General “FRAUDNET HOTLINE	Contracting Officer

(Contracting Officer shall insert—

(i) Appropriate agency name(s) and/or title of applicable Department of Homeland Security fraud hotline poster); and

(ii) The website(s) or other contact information for obtaining the poster(s).)

(c) If the Contractor has implemented a business ethics and conduct awareness program, including a reporting mechanism, such as a hotline poster, then the Contractor need not display any agency fraud hotline posters as required in paragraph (b) of this clause, other than any required DHS posters.

(d) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (d), in all subcontracts that exceed \$5.5 million, except when the subcontract—

(1) Is for the acquisition of a commercial item; or

(2) Is performed entirely outside the United States.

28. 552.270-30 PRICE ADJUSTMENT FOR ILLEGAL OR IMPROPER ACTIVITY (JUN 2011)

(Applicable to leases over the Simplified Lease Acquisition Threshold.)

INITIALS: _____ & _____
LESSOR GOVERNMENT

(a) If the head of the contracting activity (HCA) or his or her designee determines that there was a violation of subsection 27(a) of the Office of Federal Procurement Policy Act, as amended (41 U.S.C. 423), as implemented in the Federal Acquisition Regulation, the Government, at its election, may—

- (1) Reduce the monthly rental under this lease by five percent of the amount of the rental for each month of the remaining term of the lease, including any option periods, and recover five percent of the rental already paid;
- (2) Reduce payments for alterations not included in monthly rental payments by five percent of the amount of the alterations agreement; or
- (3) Reduce the payments for violations by a Lessor’s subcontractor by an amount not to exceed the amount of profit or fee reflected in the subcontract at the time the subcontract was placed.

(b) Prior to making a determination as set forth above, the HCA or designee shall provide to the Lessor a written notice of the action being considered and the basis thereof. The Lessor shall have a period determined by the agency head or designee, but not less than 30 calendar days after receipt of such notice, to submit in person, in writing, or through a representative, information and argument in opposition to the proposed reduction. The agency head or designee may, upon good cause shown, determine to deduct less than the above amounts from payments.

(c) The rights and remedies of the Government specified herein are not exclusive, and are in addition to any other rights and remedies provided by law or under this lease.

29. 52.215-10 PRICE REDUCTION FOR DEFECTIVE COST OR PRICING DATA (AUG 2011)

(Applicable when cost or pricing data are required for work or services over \$750,000.)
This clause is incorporated by reference.

30. 552.270-13 PROPOSALS FOR ADJUSTMENT (SEP 1999)

(a) The Contracting Officer may, from time to time during the term of this lease, require changes to be made in the work or services to be performed and in the terms or conditions of this lease. Such changes will be required under the Changes clause.

(b) If the Contracting Officer makes a change within the general scope of the lease, the Lessor shall submit, in a timely manner, an itemized cost proposal for the work to be accomplished or services to be performed when the cost exceeds \$100,000. The proposal, including all subcontractor work, will contain at least the following detail—

- (1) Material quantities and unit costs;
- (2) Labor costs (identified with specific item or material to be placed or operation to be performed);
- (3) Equipment costs;
- (4) Worker's compensation and public liability insurance;
- (5) Overhead;
- (6) Profit; and
- (7) Employment taxes under FICA and FUTA.

(c) The following Federal Acquisition Regulation (FAR) provisions also apply to all proposals exceeding \$500,000 in cost—

INITIALS: _____ & _____
LESSOR GOVERNMENT

(1) The Lessor shall provide cost or pricing data including subcontractor cost or pricing data (48 CFR 15.403-4) and

(2) The Lessor's representative, all Contractors, and subcontractors whose portion of the work exceeds \$500,000 must sign and return the "Certificate of Current Cost or Pricing Data" (48 CFR 15.406-2).

(d) Lessors shall also refer to 48 CFR Part 31, Contract Cost Principles, for information on which costs are allowable, reasonable, and allocable in Government work.

31. CHANGES (MAR 2013)

(a) The LCO may at any time, by written order, direct changes to the Tenant Improvements within the Space, Building Security Requirements, or the services required under the Lease.

(b) If any such change causes an increase or decrease in Lessor's costs or time required for performance of its obligations under this Lease, whether or not changed by the order, the Lessor shall be entitled to an amendment to the Lease providing for one or more of the following:

- (1) An adjustment of the delivery date;
- (2) An equitable adjustment in the rental rate;
- (3) A lump sum equitable adjustment; or
- (4) A change to the operating cost base, if applicable.

(c) The Lessor shall assert its right to an amendment under this clause within 30 days from the date of receipt of the change order and shall submit a proposal for adjustment. Failure to agree to any adjustment shall be a dispute under the Disputes clause. However, the pendency of an adjustment or existence of a dispute shall not excuse the Lessor from proceeding with the change as directed.

(d) Absent a written change order from the LCO, or from a Government official to whom the LCO has explicitly and in writing delegated the authority to direct changes, the Government shall not be liable to Lessor under this clause.

32. 552.215-70 EXAMINATION OF RECORDS BY GSA (FEB 1996)

The Contractor agrees that the Administrator of General Services or any duly authorized representative shall, until the expiration of 3 years after final payment under this contract, or of the time periods for the particular records specified in Subpart 4.7 of the Federal Acquisition Regulation (48 CFR 4.7), whichever expires earlier, have access to and the right to examine any books, documents, papers, and records of the Contractor involving transactions related to this contract or compliance with any clauses thereunder. The Contractor further agrees to include in all its subcontracts hereunder a provision to the effect that the subcontractor agrees that the Administrator of General Services or any duly authorized representatives shall, until the expiration of 3 years after final payment under the subcontract, or of the time periods for the particular records specified in Subpart 4.7 of the Federal Acquisition Regulation (48 CFR 4.7), whichever expires earlier, have access to and the right to examine any books, documents, papers, and records of such subcontractor involving transactions related to the subcontract or compliance with any clauses thereunder. The term "subcontract" as used in this clause excludes (a) purchase orders not exceeding \$100,000 and (b) subcontracts or purchase orders for public utility services at rates established for uniform applicability to the general public.

33. 52.215-2 AUDIT AND RECORDS—NEGOTIATION (OCT 2010)

(Applicable to leases over the Simplified Lease Acquisition Threshold.)
This clause is incorporated by reference.

INITIALS: _____ & _____
LESSOR GOVERNMENT

34. 52.233-1 DISPUTES (MAY 2014)

This clause is incorporated by reference.

35. 52.222-26 EQUAL OPPORTUNITY (APR 2015)

This clause is incorporated by reference.

36. 52.222-21 PROHIBITION OF SEGREGATED FACILITIES (APR 2015)

This clause is incorporated by reference.

37. 52.219-28 POST-AWARD SMALL BUSINESS PROGRAM REREPRESENTATION (JUL 2013)

(Applicable to leases exceeding the micro-purchase threshold.)

This clause is incorporated by reference.

38. 52.222-35 EQUAL OPPORTUNITY FOR VETERANS (OCT 2015)

(Applicable to leases \$150,000 or more, total contract value.)

(a) Definitions. As used in this clause—

“Active duty wartime or campaign badge veteran,” “Armed Forces service medal veteran,” “disabled veteran,” “protected veteran,” “qualified disabled veteran,” and “recently separated veteran” have the meanings given at FAR [22.1301](#).

(b) Equal opportunity clause. The Contractor shall abide by the requirements of the equal opportunity clause at 41 CFR 60-300.5(a), as of March 24, 2014. This clause prohibits discrimination against qualified protected veterans, and requires affirmative action by the Contractor to employ and advance in employment qualified protected veterans.

(c) Subcontracts. The Contractor shall insert the terms of this clause in subcontracts of \$150,000 or more unless exempted by rules, regulations, or orders of the Secretary of Labor. The Contractor shall act as specified by the Director, Office of Federal Contract Compliance Programs, to enforce the terms, including action for noncompliance. Such necessary changes in language may be made as shall be appropriate to identify properly the parties and their undertakings.

39. 52.222-36 EQUAL OPPORTUNITY FOR WORKERS WITH DISABILITIES (JUL 2014)

(Applicable to leases over \$15,000 total contract value.)

(a) *Equal opportunity clause.* The Contractor shall abide by the requirements of the equal opportunity clause at 41 CFR 60-741.5(a), as of March 24, 2014. This clause prohibits discrimination against qualified individuals on the basis of disability, and requires affirmative action by the Contractor to employ and advance in employment qualified individuals with disabilities.

(b) *Subcontracts.* The Contractor shall include the terms of this clause in every subcontract or purchase order in excess of \$15,000 unless exempted by rules, regulations, or orders of the Secretary, so that such provisions will be binding upon each subcontractor or vendor. The Contractor shall act as specified by the Director, Office of Federal Contract Compliance Programs of the U.S. Department of Labor, to enforce the terms, including action for noncompliance. Such necessary changes in language may be made as shall be appropriate to identify properly the parties and their undertakings.

40. 52.222-37 EMPLOYMENT REPORTS ON VETERANS (FEB 2016)

(Applicable to leases \$150,000 or more, total contract value.)

This clause is incorporated by reference.

INITIALS: _____ & _____
LESSOR GOVERNMENT

41. 52.209-6 PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, OR PROPOSED FOR DEBARMENT (OCT 2015)

(Applicable to leases over \$35,000 total contract value.)

This clause is incorporated by reference.

42. 52.215-12 SUBCONTRACTOR CERTIFIED COST OR PRICING DATA (OCT 2010)

(Applicable if over \$750,000 total contract value.)

This clause is incorporated by reference.

43. 52.219-8 UTILIZATION OF SMALL BUSINESS CONCERNS (OCT 2014)

(Applicable to leases over the Simplified Lease Acquisition Threshold.)

This clause is incorporated by reference.

44. 52.219-9 SMALL BUSINESS SUBCONTRACTING PLAN (OCT 2015) ALTERNATE III (OCT 2015)

(Applicable to leases over \$700,000 total contract value.)

This clause is incorporated by reference.

45. 52.219-16 LIQUIDATED DAMAGES—SUBCONTRACTING PLAN (JAN 1999)

(Applicable to leases over \$700,000 total contract value.)

This clause is incorporated by reference.

46. 52.204-10 REPORTING EXECUTIVE COMPENSATION AND FIRST-TIER SUBCONTRACT AWARDS (OCT 2015)

(Applicable if over \$30,000 total contract value.)

This clause is incorporated by reference.

47. 52.219-73 GOALS FOR SUBCONTRACTING PLAN (JUN 2005), ALTERNATE I (SEP 1999)

(Applicable if over \$700,000 total contract value.)

This clause is incorporated by reference.

INITIALS: _____ & _____
LESSOR GOVERNMENT

PROPOSAL TO LEASE SPACE

OMB Control Number: 3090-0086
Expiration Date: 12/31/2022

Paperwork Reduction Act Statement - This information collection meets the requirements of 44 U.S.C. § 3507, as amended by section 2 of the Paperwork Reduction Act of 1995. You do not need to answer these questions unless we display a valid Office of Management and Budget (OMB) control number. The OMB control number for this collection is 3090-0086. We estimate that it will take 2.3 hours to read the instructions, gather the facts, and answer the questions. Send only comments relating to our time estimate, including suggestions for reducing this burden, or any other aspects of this collection of information to: U.S. General Services Administration, Regulatory Secretariat Division (M1V1CB), 1800 F Street, NW, Washington, DC 20405.

In Response to Request for Lease
 Proposals (RLP) Number -->

DATED

SECTION I - DESCRIPTION OF PREMISES

1. BUILDING DESCRIPTION	a. Building Name	b. Building Street Address			
c. City	d. State	e. 9-Digit ZIP Code	f. Congressional District		
2a. FLOORS OFFERED	2b. TOTAL NUMBER OF FLOORS IN BUILDING	3. TOTAL RENTABLE SPACE IN OFFERED BUILDING			
		a. GENERAL PURPOSE <i>(Office)</i>	b. WAREHOUSE	c. OTHER	
		SQUARE FEET	SQUARE FEET	SQUARE FEET	
4. LIVE FLOOR LOAD POUNDS PER SQUARE FOOT	5. MEASUREMENT METHOD <input type="checkbox"/> ANSI/BOMA <input type="checkbox"/> OTHER	6. YEAR OF LAST MAJOR RENOVATION <i>(if applicable)</i>	7. BUILDING AGE	8. SITE SIZE	
				_____ SQUARE FEET ACRES	

SECTION II - SPACE OFFERED AND RATES

9. ANSI/BOMA OFFICE AREA SQUARE FEET (ABOA)	10. RENTABLE SQUARE FEET (RSF)	11. COMMON AREA FACTOR (CAF)
---	--------------------------------	------------------------------

"Tenant Improvements" are all alterations for the Government-demised area above the building shell buildout, excluding costs identified as tenant improvements in the Security Unit Price List. Building Specific Amortized Capital (BSAC) is the sum of costs identified as such in the Security Unit Price List. Neither the Tenant Improvements as stated in Block 12, nor the BSAC as stated in Block 13, are to be included in the shell rent. It is expected that the tenant buildout will be fully amortized at the end of the firm term, and the rent will be reduced accordingly. Any desired rent increases or decreases beyond the firm term of the lease should be reflected in the shell rate and fully explained as part of this written proposal. If Tenant improvements or BSAC improvements are to be amortized beyond the firm term, those calculations must be itemized as part of this written proposal. The Offeror may attach additional pages as necessary.

					Number of years each cost per square foot is in effect. State any changes for any rent component.	
	a. BUILD-OUT COSTS PER CATEGORY	b. AMORTIZATION TERM	c. AMORTIZATION INTEREST RATE (%)	d. ANNUAL RENT \$ PER RSF	e. ANNUAL RENT \$ PER ABOA SQUARE FOOT	f. NUMBER OF YEARS RATE IS EFFECTIVE
12. TENANT IMPROVEMENTS <i>(per RLP requirements)</i>						
13. BSAC <i>(per RLP requirements detailed on Security Unit Price List)</i>						
14. SHELL BUILD-OUT <i>(per RLP requirements)</i>						
15. TOTAL BUILD-OUT COSTS						
16. SHELL RENT <i>(Including real estate taxes. Refer to Line 28 on GSA 1217)</i>						
17. OPERATING COSTS <i>(Refer to Line 27 on GSA 1217)</i>						
18. TOTAL RATE/SQUARE FOOT						
19. TOTAL ANNUAL RENT						
	a. PER SQUARE FOOT RATE	b. FOR YEARS	c. PER SQUARE FOOT RATE	d. FOR YEARS	e. PER SQUARE FOOT RATE	f. FOR YEARS
20. STEP RENT <i>(SHELL RATES)</i>	_____ /RSF /ABOA	Thru	_____ /RSF /ABOA	Thru	_____ /RSF /ABOA	Thru

21. PARKING	<p>a. Number of parking spaces for the future building/facility which are under the control of the Offeror: _____ Surface _____ Structured</p> <p>b. Number of auto parking spaces required by local code: _____ Surface _____ Structured</p> <p>c. Number of auto parking spaces for Employee/Visitor Use (per RLP): _____ Surface _____ Structured</p> <p>d. Number of parking spaces (auto and truck) for Official Government Vehicles (per RLP): _____ Surface _____ Structured</p> <p>e. Does the rental rate offered above include RLP - required parking costs? <input type="checkbox"/> YES <input type="checkbox"/> NO</p> <p>If NO, complete the following: Annual cost per space: _____ Surface _____ Structured</p>
-------------	---

SECTION III - LEASE TERMS AND CONDITIONS

22. INITIAL LEASE TERM <i>(Full Term)</i>			23. RENEWAL OPTIONS			
a. Number of Years	b. Years Firm	c. Number of Days Notice for Government to Terminate Lease:	a. Shell Rate/RSF/Year	b. Years Each	c. Number of Options	d. Number of Days Notice to Exercise Option

24. OFFER GOOD UNTIL AWARD 26. COMMISSIONS <i>(if applicable)</i> , ATTACH COMMISSION AGREEMENT	25. Space will be altered and delivered in accordance with the Government's specifications and requirements in accordance with the Request for Lease Proposals (RLP) and the lease.
--	---

a. Tenant Representative Commission:	b. Owner's Representative Commission:	c. Schedule of Commission Payments:
%	%	% at lease award and % at lease occupancy

27. OFFEROR'S TENANT IMPROVEMENT FEE SCHEDULE

***Block 27 fees only applicable for Tenant Improvement (TI) subject to post-award pricing;**

N/A for turnkey pricing.

a. Architectural/Engineering fees will be *(choose one)*:

1. _____ per ABOA SF

2. _____ % of Total TI construction costs.

3. _____ flat fee

b. Lessor's Project Management Fee will be _____ percent of Total TI construction costs.

c. If other fees are applicable, state as per ABOA square foot in the space below, or if using a percentage, the basis for determining the fee.

The Government will add the cost of the proposed TI fees to the net present value of the offered rental rate as described in the RLP's Present Value Price Evaluation paragraph. This schedule will be applicable for Tenant Improvements.

29. FREE RENT INCLUDED IN OFFER

1. _____ months free rent (includes shell, operating, TI and BSAC rent)

2. Other rental concessions structured as follows:

3. None

28. ADDITIONAL FINANCIAL ASPECTS OF THE LEASE

Adjustment for Vacant Premises: _____ per ABOA SF

HVAC Overtime Rate: _____ per hour per *(choose one)*

zone floor space

For rates based on a "per zone" basis, provide the following:

Number of zones in offered space: _____

Areas requiring 24 hour HVAC (LAN, etc.) _____ per ABOA SF*

***Only applies when the Government requires separate reimbursement for 24 hour HVAC as described under Section 1 of the Lease. Otherwise, include this cost in the operating rent, as described under Section 6 of the Lease.**

Building's Normal Hours of HVAC Operation:

Monday - Friday _____ AM to _____ PM

Saturday _____ AM to _____ PM

Sunday _____ AM to _____ PM

Percent of Government Occupancy: _____ %

Current Year Taxes: _____

Based on fully assessed value? YES NO

Is the offered space part of multiple tax bills? YES NO

If so, provide tax ID numbers and square footage for each in the blank space below the question on total land costs. Attach the legal description of the offered property.

If a site is offered, state the total land costs: _____

30. LIST OF ATTACHMENTS SUBMITTED WITH THIS OFFER *(See RLP requirements)*

31. ADDITIONAL REMARKS OR CONDITIONS WITH RESPECT TO THIS OFFER

SECTION IV - OWNER IDENTIFICATION AND CERTIFICATION

32. RECORDED OWNER

a. Name	b. Address	c. City	d. State	e. ZIP Code + 4	f. DUNS Number
---------	------------	---------	----------	-----------------	----------------

33. BY SUBMITTING THIS OFFER, THE OFFEROR AGREES UPON ACCEPTANCE OF THIS PROPOSAL BY HEREIN SPECIFIED DATE. TO LEASE TO THE UNITED STATES OF AMERICA, THE PREMISES DESCRIBED, UPON THE TERMS AND CONDITIONS AS SPECIFIED HEREIN, IN FULL COMPLIANCE WITH AND ACCEPTANCE OF THE AFOREMENTIONED RLP, WITH ATTACHMENTS.

I have read the RLP with attachments in its entirety and am requesting no deviations.

34. Offeror's Interest in Property

Owner Agent Other

35. OFFEROR Check if same as Recorded Owner

a. Name	b. Address	c. City	d. State	e. ZIP Code + 4
f. Title	g. E-Mail Address		h. Telephone Number	
i. Offeror's Signature			j. Date Signed	

LEASE PROPOSAL DATA

In Response to Request for Lease Proposals (RLP) Number _____

DATE: _____

Offeror's Interest in the Property

1. Fee owner Other: _____

Attach evidence of Offeror's interest in property (e.g., deed) and representative's authority to bind Offeror.

Flood Plains:

2. The Property is in a base (100-year) flood plain in a 500-year flood plain not in a flood plain.

(See RLP Section 2, Flood Plains.)

Seismic Safety: The Building

RLP does not contain seismic requirements. No documentation required.

RLP contains seismic requirements. The Building:

3. Fully meets seismic requirements or meets an exemption under the RLP
 Does not meet seismic requirements, but will be retrofitted to meet seismic requirements
 Will be constructed to meet seismic requirements
 Will not meet seismic requirements

(See RLP Section 2, Seismic Safety.) Attach appropriate documentation.

Historic Preference: The Building is a

- Historic property within a historic district.
 Non-historic developed site or non-historic undeveloped site within a historic district.
 Historic property outside of a historic district.
 None of the above.

(See RLP Section 2, Historic Preference.) Attach appropriate documentation.

Asbestos-Containing Material (ACM): The Property

5. Contains no ACM, or contains ACM in a stable, solid matrix that is not damaged or subject to damage.
 Contains ACM not in a stable, solid matrix.

(See RLP Section 2, Asbestos.)

Fire/Life Safety:

6. The Property Meets Does not meet Lease fire/life safety standards.

(See RLP Section 2, Fire Protection and Life Safety.)

Accessibility:

7. The Property Meets Does not meet Lease accessibility standards.

(See RLP Section 2, Accessibility.)

ENERGY STAR®: The Building

- Has received the ENERGY STAR® Label within the past twelve months. Date (MM-DD-YYYY): _____
 Has not received the ENERGY STAR® Label within the past twelve months; the Offeror has evaluated energy savings measures and
 Determined that none are cost effective. Determined that the following are cost effective *(Attach additional pages):*

(See RLP Section 2, Energy Independence and Security Act.)

9. Waiver of Price Evaluation Preference. A HUBZone small business concern (SBC) Offeror may elect to waive the price evaluation preference provided in Section 4 of the RLP. In such a case, no price evaluation preference shall apply to the evaluation of the HUBZone SBC, and the performance of work requirements set forth in Section 1 of the Lease shall not be applicable to a lease awarded to the HUBZone SBC Offeror under this solicitation. A HUBZone SBC desiring to waive the price evaluation preference should so indicate below.

I am a HUBZone SBC Offeror and I elect to waive the price evaluation preference. *(See RLP and Lease documents for more information.)*

LESSOR'S ANNUAL COST STATEMENT

Important - Read attached "Instructions"

OMB Control Number: 3090-0086

Expiration Date: 12/31/2022

Paperwork Reduction Act Statement - This information collection meets the requirements of 44 U.S.C. § 3507, as amended by section 2 of the Paperwork Reduction Act of 1995. You do not need to answer these questions unless we display a valid Office of Management and Budget (OMB) control number. The OMB control number for this collection is 3090-0086. We estimate that it will take 2 hours to read the instructions, gather the facts, and answer the questions. Send only comments relating to our time estimate, including suggestions for reducing this burden, or any other aspects of this collection of information to: U.S. General Services Administration, Regulatory Secretariat Division (M1V1CB), 1800 F Street, NW, Washington, DC 20405.

1. Request for Lease Proposals (RLP)		2. Statement Date
3. Rental Area (Square Feet)	3A. Entire Building	3B. Leased by Government
4. Building Name and Address (<i>Number, Street, City, State, and Zip Code</i>)		

**SECTION I - ESTIMATED ANNUAL COST OF SERVICES AND UTILITIES
FURNISHED BY LESSOR AS PART OF RENTAL CONSIDERATION**

SERVICES AND UTILITIES	LESSOR'S ANNUAL COST FOR		FOR GOVERNMENT USE ONLY
	(a) Entire Building	(b) Government-Leased Area	
A. CLEANING, JANITOR AND/OR CHAR SERVICE			
5. Salaries			
6. Supplies (<i>Wax, cleaners, cloths, etc.</i>)			
7. Contract Services (<i>Window washing, waste and snow removal</i>)			
B. HEATING			
8. Salaries <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>			
9. Fuel ("X" one) Oil Gas Coal Electric			
10. System Maintenance and Repair			
C. ELECTRICAL			
11. Current for Light and Power			
12. Replacement of Bulbs, Tires, Starters			
13. Power for Special Equipment			
14. System Maintenance and Repair (<i>Ballasts, Fixtures, etc.</i>)			
D. PLUMBING			
15. Water (<i>For all purposes</i>) (<i>Include Sewage Charges</i>)			
16. Supplies (<i>Soap, towels, tissues not in 6 above</i>)			
17. System Maintenance and Repair			
E. AIR CONDITIONING			
18. Utilities (<i>Include electricity, if not in C11</i>)			
19. System Maintenance and Repair			
F. ELEVATORS			
20. Salaries (<i>Operators, starters, etc.</i>)			

Exhibit G

21. System Maintenance and Repair			
-----------------------------------	--	--	--

INSTRUCTIONS

In acquiring space by lease, it is the established policy of GSA to enter into leases only at rental charges which are consistent with prevailing scales in the community for facilities.

ITEM NUMBER

1. Enter the Government lease or Request for Lease Proposals (RLP) number, if available.
2. Enter the date that your statement was prepared and signed.
3. A. Enter in this block a computation of the rentable area (*multiple tenancy basis*) for the entire building. The rentable area shall be computed by measurement to the inside finish of permanent outer building walls to the inside finish of corridor walls (*actual or proposed*) or to other permanent partitions, or both. Rentable space is the area for which a tenant is charged rent. It is determined by the building owner and may vary by city or by building within the same city. The rentable space may include a share of building support/common areas such as elevator lobbies, building corridors, and floor service areas. Floor services areas typically include restrooms, janitor rooms, telephone closets, electrical closets, and mechanical rooms. The rentable space generally does not include the vertical building penetrations and their enclosing walls, such as stairs, elevator shafts, and vertical ducts.
3. B. Enter in this block a computation of the rentable area to be rented to the Government. For this area, follow the procedure as outlined above, except that measurements are to be made only to the center of the partitions which separate the area to be rented by the Government from adjoining rented or rentable areas.
4. Identify the property by name and address.

SECTION I

ESTIMATED ANNUAL COST OF SERVICES AND UTILITIES

5. - 26. The services and utilities listed in this section are required in most of our rented space whether furnished by the Government or the Lessor.

Carefully review the Request for Lease Proposals (RLP) and/or the proposed lease to identify those services and utilities to be furnished by you as part of the rental consideration. Then enter your best cost estimate, or the actual cost from the previous year, for each of these services and utilities in column (a) for the entire building and in column (b) for the area to be rented to the Government. If any service or utility furnished for the space rented by the Government is not furnished throughout the building, or the cost of a service or utility furnished to the Government space exceeds the cost of the same service or utility furnished to other rented space, explain on a separate sheet. For convenience, each major category has been divided into separate items such as salaries and supplies so that they may be entered when applicable. However, in the event that your records are not maintained for each item contained in Section I, 5 through 26, the total for a major category (A through F) may be entered under the category heading in columns (a) and (b) in lieu of the specific items. System maintenance and repairs includes the annual cost of such items as oiling, inspecting, cleaning, regulating, and routine replacement costs.

SECTION II

ESTIMATED ANNUAL COST OF OWNERSHIP EXCLUSIVE OF CAPITAL CHARGES

Items 28 through 32 will be useful in the Government's determination of the fair market value of the space to be rented and shall be completed irrespective of whether Section I is applicable, as follows:

28. Include all applicable real estate taxes imposed upon the property.
29. Enter the annual cost of fire, liability, and other insurance carried on the real estate.
30. Enter the annual cost of wages, materials, and outside services used in repairs and maintenance of the building itself and all similar repairs and maintenance of the building itself and all similar repairs and maintenance costs not included in Section I above (Heating, Electrical, Plumbing, Air Conditioning, and Elevators). This includes major repairs and changes in the nature of a permanent improvement such as annual cost to replace relatively short-lived items such as boiler, compressors, elevators, and roof coverings.
31. Enter any lease commission which you may be responsible for due to the Government leasing action.
32. Include administrative expenses such as agency fees, legal fees, auditing, and advertising. Do not include financial charges such as income or corporate taxes or organization expense.
34. - 35. Complete Lessor certification.

PRELIMINARY FIRE PROTECTION AND LIFE SAFETY EVALUATION FOR AN OFFICE BUILDING

The prelease form contains two parts that must be completed depending on which floor the proposed offered space is located within a building. Part A must be completed when an offered space is located below the 6th floor of a building. Part A shall be completed by the Offeror or their authorized representative. Part B must be completed when an offered space is located on or above the 6th floor of a building. Part B shall be completed by a professional engineer. The Fundamental Code Requirements apply to Part A and Part B.

- a. The offered building shall be evaluated for compliance with the most recent edition of the building and fire code adopted by the jurisdiction in which the building is located; with the exception that the technical egress requirements of the building shall be evaluated based on the egress requirements of the most recent edition of the National Fire Protection Association (NFPA) 101, *Life Safety Code*. (Note: a building with a Certificate of Occupancy indicating that a building fully complies with the International Building Code shall be deemed to comply with this requirement.) All areas that do not meet the above stated criteria shall be identified as to the extent that they do comply.
- b. A fire escape located on the floor(s) where the offered space is located shall not be counted as an approved exit stair.
- c. An interlocking or scissor stair located on the floor(s) where the offered space is located shall only count as one exit stair.
- d. The number of floors used to determine when Part A or Part B is applicable is based on counting the number of floors starting from the street floor.

PART A

The Offeror or their representative shall complete Part A. Part A consists of a series of short answer and yes/no/not applicable questions related to general building information and fire protection and life safety systems. Upon completion of Part A, the Offeror must sign and date the "Offeror's Statement." Part A is applicable to offered space located below the 6th floor of the building.

I. Building Address						
Building Name: _____						
Building Address: _____						
City: _____		State: _____		9-Digit Zip Code: _____		
II. General Building Information						
a. Identify each floor on which space is offered and the square footage of space on each floor offered to Government:						
Floor						
Square Feet Per Floor						
b. Identify the total number of floors in the building starting at the street floor:						
c. Identify the total number of floors in the building below the street floor:						
d. Identify which floor(s) in the building permit reentry from the exit stair enclosure to the interior of the building:						
III. Other Uses in Building (Check All That Apply)						
<input type="checkbox"/> Restaurants	<input type="checkbox"/> Laboratories	<input type="checkbox"/> Storage	<input type="checkbox"/> Retail	<input type="checkbox"/> Parking Garage	<input type="checkbox"/> Other (List Below)	
IV. Automatic Fire Sprinkler System						
Please Check YES, NO, or N/A to the following questions:						
a. Is an automatic fire sprinkler system installed throughout the building?				<input type="checkbox"/> YES	<input type="checkbox"/> NO	
b. If automatic fire sprinklers are installed within the building, is the automatic fire sprinkler system maintained in accordance with the applicable local codes or NFPA 25, <i>Standard for the Inspection, Testing, and Maintenance of Water-Based Fire Protection Systems</i> ?				<input type="checkbox"/> YES	<input type="checkbox"/> NO	<input type="checkbox"/> N/A
V. Fire Alarm System						
Please Check YES, NO, N/A to the following questions:						
a. Is a fire alarm system installed in the building?				<input type="checkbox"/> YES	<input type="checkbox"/> NO	
b. Is an emergency voice/alarm communication system installed in the building?				<input type="checkbox"/> YES	<input type="checkbox"/> NO	
c. If a fire alarm system is installed in the building, are audible devices (e.g., horns, bells, speakers, etc.) installed on the floor in which the offered space is located in the building?				<input type="checkbox"/> YES	<input type="checkbox"/> NO	<input type="checkbox"/> N/A
d. If a fire alarm system is installed in the building, are strobe devices installed on the floor in which the offered space is located in the building?				<input type="checkbox"/> YES	<input type="checkbox"/> NO	<input type="checkbox"/> N/A
e. If a fire alarm system is installed in the building, is the fire alarm system over 25 years old?				<input type="checkbox"/> YES	<input type="checkbox"/> NO	<input type="checkbox"/> N/A
f. If a fire alarm system is installed in the building, does the operation of the fire alarm system automatically notify the local fire department, remote station, or UL listed central station?				<input type="checkbox"/> YES	<input type="checkbox"/> NO	<input type="checkbox"/> N/A
g. If a fire alarm system is installed in the building, is the fire alarm system maintained in accordance with the applicable local codes or NFPA 72, <i>National Fire Alarm and Signaling Code</i> ?				<input type="checkbox"/> YES	<input type="checkbox"/> NO	<input type="checkbox"/> N/A

VI. Exit Signs and Emergency Lighting			
Please Check YES, NO, or N/A to the following questions:			
a. Are exit signs installed in the paths of egress travel to the exit stairs or exits?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
b. Is emergency lighting installed in the paths of egress travel to the exit stairs or exits?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
c. If an emergency lighting system is installed in the building, is the emergency lighting system arranged to provide illumination automatically in the event of any interruption of the building's normal lighting system?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	<input type="checkbox"/> N/A
VII. Elevators			
Please Check YES, NO, or N/A to the following questions:			
a. Are elevators installed in the building?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	
b. If elevators are installed in the building, are the elevator cars equipped with a telephone or another two-way communication system?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	<input type="checkbox"/> N/A
c. If elevators are installed in the building, are the elevators recalled by smoke detectors located in the elevator lobbies and elevator machine rooms?	<input type="checkbox"/> YES	<input type="checkbox"/> NO	<input type="checkbox"/> N/A
VIII. Additional Information			

OFFEROR'S STATEMENT	
I hereby attest that the above information is complete and accurate to the best of my knowledge.	
Signature: _____	Date: _____
Printed Name: _____	
Title: _____	
Name of Firm: _____	

PART B

The Offeror's professional engineer shall complete Part B when an offered space is located on the 6th floor or higher of a building. Part B consists of a detailed narrative report based on an evaluation of the entire building that also includes the review of the preventive maintenance records of the building's fire alarm system and automatic fire sprinkler system. The fire protection engineer shall prepare a detailed narrative report. The detailed narrative report shall address at a minimum the items noted below as they apply to the offered space in the building, with specific attention to fire safety conditions that affect the floor(s) where the offered space to the Government is located, including those floors located below the offered space. In addition, the detailed narrative report shall include all deficiencies that do not meet the specified criteria (see Fundamental Code Requirements), the associated code reference(s), as well as any recommended corrective action(s).

NOTES:

- a. *The professional engineer must be licensed as a fire protection engineer in the same State in which the subject building is located unless the subject State does not formally recognize fire protection engineering. In such cases, GSA will accept the services of any professional engineer in the subject State provided the professional engineer is also recognized as a fire protection engineer in any other U.S. State or Territory.*
- b. *Upon completion of Part B, the Offeror's fire protection engineer must sign and date the "Fire Protection Engineer Statement."*
- c. *Upon completion of Part B, the Offeror must sign and date the "Offeror's "Statement of Correction."*
- d. *The accepted GSA Form 12000, Part B is valid for a time period of 5 years from the noted date on the completed and accepted Part B. This acceptance is conditional in that no major modifications or construction has occurred associated with the building.*

The detailed narrative report shall address at a minimum the items noted below as they apply to the offered space in the _____ building.

1. General Information.

- a. Identify all current citations or violations noted by the local jurisdiction regarding the building.
- b. Provide digital pictures of the building. Include exterior views showing the front of the building and all sides of the building.
- c. Identify the number of floors in the building (above and below grade).
- d. Identify the approximate gross square footage per floor in the building.
- e. Identify the gross square footage and associated floor of offered space proposed to the Government to occupy.
- f. Identify by location and describe hazardous/significant fuel load areas (greater than normal for the type of occupancy).
- g. Identify and describe potential fire ignition sources in hazardous/significant fuel load areas in the building.

2. Occupancy Classifications.

- a. Identify all the different types of occupancies and particular uses on each floor of the subject building. For example, include retail, restaurants, mechanical equipment areas, storage areas, inside parking areas, etc.

3. Building Construction.

- a. Identify the building construction type.

4. Vertical Openings.

- a. Identify by location and describe the enclosure of vertical openings through floors, such as stairways, atriums, hoistways for elevators, escalators, and shafts.
- b. Identify any deficiencies in the rated vertical enclosures that affect the integrity of the enclosure.

5. Means of Egress.

- a. Identify the number of enclosed exit stairs on each floor of the building.
- b. For each exit stair, describe:
 - i. The clear width of each stair tread and location of measurement.
 - ii. The egress capacity of each exit stair.
 - iii. The location of where each exit stair discharges.
 - iv. Identify and describe the operation and application of the exit stair re-entry provisions to the interior of the building, if provided.
 - v. Any penetrations into and openings through each exit stair enclosure assembly.
 - vi. Any headroom obstruction within each exit stair enclosure.
 - vii. If any exit stair has been compromised in such a way to have the potential to interfere with its use as an exit; and
 - viii. The exit stair remoteness arrangement.
 - ix. Identify and describe if all exit stair doors are self-closing and self-latching.
- c. Identify and describe all exit doors that do not swing in the direction of exit travel.
- d. Identify and describe if all fire doors are in proper working order. Provide location of noted fire door and purpose.
- e. Identify by floor and describe any concerns regarding the exit access system (i.e., corridor or open plan office concept), as it applies to the proposed offered space.
- f. Identify by location and describe any concern regarding the exit signage within the building.
- g. Describe the building's emergency lighting system.
- h. Identify and describe if emergency power is provided within the building.
- i. If emergency power for life safety systems is provided by generator(s) or UPS systems describe if they are tested and maintained in accordance with NFPA 110, *Standard for Emergency and Standby Power Systems* or NFPA 111, *Standard on Stored Electrical Energy Emergency and Standby Power Systems* as applicable. If not complying with the applicable NFPA Standards; identify and evaluate the procedures being used.

6. Automatic Fire Suppression Systems

- a. Identify and describe if the building is protected or not protected throughout by an automatic fire sprinkler system. If the building is not protected throughout by an automatic fire sprinkler system, identify those areas of the building where partial fire sprinkler protection is provided.
- b. Identify and describe the different types of automatic fire sprinkler systems (e.g., dry, wet, pre-action, etc.) that are installed within the building and their respective locations.
- c. Identify and describe any other fire suppression systems installed within the building.
- d. Identify and describe the types of standpipes installed in the building.
- e. If automatic fire sprinkler systems are installed in the building, describe if they are tested and maintained in accordance with the applicable local codes or NFPA 25, *Standard for the Inspection, Testing, and Maintenance of Water-Based Fire Protection Systems*. If not complying with the applicable NFPA Standards; identify and evaluate the procedures being used. If not complying with the applicable NFPA Standard; identify and evaluate the procedures being used.

7. Fire Alarm System

- a. Identify and describe the fire alarm system, as a minimum, the date of installation, type, manufacturer and model, and components such as manual pull stations, etc.
- b. Describe if the fire alarm system is connected to a U.L. listed Central Station, Remote Station, or to the local fire department.
- c. Describe in detail the operation of the fire alarm system, including if it has emergency voice/alarm communication capabilities.
- d. Describe in if the fire alarm system is tested and maintained in accordance with NFPA 72, *National Fire Alarm and Signaling Code*. If not complying with the applicable NFPA Standard; identify and evaluate the procedures being used.

8. Elevators

- a. Verify the elevators have a current certificate (date of inspection) of elevator inspection from the local jurisdiction.
- b. Identify and describe the emergency recall operation features of the elevators. Describe all differences with the requirements of ASME/A17.1, *Safety Code for Elevators and Escalators*, Phase I Emergency Recall Operation requirements.
- c. Identify and describe the emergency in car operation features of the elevators. Describe all differences with the requirements of ASME/A17.1, *Safety Code for Elevators and Escalators*, Phase II Emergency In-Car Operation requirements.
- d. Identify and describe if the elevators are equipped with telephones or other two-way emergency signaling systems connected to an emergency communication location staffed 24 hours per day, 7 days per week.

STATEMENT OF FIRE PROTECTION ENGINEER

I hereby attest that I have performed a full assessment of the subject premises; and that the above information is complete and accurate to the best of my knowledge. I have initialed at the bottom of each page. My official seal, professional license information, and signature are affixed below. I have included findings, recommended corrective action(s), and made specific references to the applicable code sections as an attachment to this report. Such findings specifically identify instances where the building does not comply with the specified criteria, and recommendations have been made in order to rectify the situation and assure substantial compliance of the building to all applicable criteria. (If no deficiencies were identified, during the evaluation, please explicitly state so in the findings and recommendations portion of the report.)

Signature: _____ Date: _____

Printed Name: _____

Name of Firm: _____ Phone _____

License Number: _____

Number: _____

Stamp Here:

OFFEROR'S STATEMENT OF CORRECTION

In the event any of the offered space does not meet the above criteria, the Offeror shall attest below that all work required to bring the offered space into full compliance with all applicable criteria will be completed at the Offeror's sole cost and expense prior to the Government's acceptance of the offered space under the terms of any prospective lease agreement.

NOTE: REPORTS SUBMITTED WITHOUT THE FPE'S FINDINGS, RECOMMENDED CORRECTIVE ACTIONS AND CODE REFERENCES WILL BE RETURNED WITHOUT REVIEW BY THE GSA REGIONAL FIRE PROTECTION ENGINEERING OFFICE.

Signature: _____ Date: _____

Printed Name: _____

Title: _____

Name of Firm: _____



Attachment 2: Seismic Offer Forms

Instructions to Leasing Specialists:

The following seismic forms are intended to be issued as an attachment to the RLP package. Therefore, unless the transaction is exempted as described under paragraph 3a of this Appendix, the LCO must attach the entire group of six Seismic Forms to the RLP package. The Offeror/Offeror's engineer must fill out the appropriate form(s) among the four pre-award submittals to complete his or her offer. The pre-occupancy submittals are also included as part of the RLP package, to inform Offerors of potential post-award obligations.



RLP OFFER ATTACHMENT - SEISMIC OFFER FORMS

Instructions for Offeror:

Forms A through D are pre-award submittals. Depending upon the form, either the Offeror or the Offeror's engineer shall complete and sign the form to confirm seismic compliance with RP 8. When the engineer fills out a form, he or she is also required to stamp it. The Offeror's engineer shall represent whether the Building meets RP 8 standards, using Form A for Benchmark Buildings or Form B for other existing buildings. If the engineer's certification indicates that the Building does not meet RP 8 standards, the Offeror shall agree to retrofit the building to meet the standards, using Form C, Part 1. Offerors providing new construction shall commit to a design code, using Form C, Part 2. Offerors may represent that their building meets an exemption criteria, using Form D.

Forms E and F are post-award submittals. They only apply when the Offeror has agreed to either retrofit an existing building (use Form E) or is constructing a new building (use Form F). Prior to the Government accepting leased space, the Lessor's engineer shall complete, stamp, and sign the appropriate representation.

The forms must include the supporting documentation stated in the RLP and Lease.

Below is a detailed explanation of each of the forms.

SEISMIC FORM A - CERTIFICATE OF SEISMIC COMPLIANCE BENCHMARK BUILDING

A benchmark building is one that was designed and built or retrofitted in accordance with structural provisions that are considered to provide acceptable life-safety protection. RP 8, Section 1.3, Table 1-1 shows the construction codes that qualify a building as a Benchmark Building. If a building qualifies, no additional hazards need be considered. If the seismicity of a region has changed since the benchmark dates listed in the table, the building must be evaluated in accordance with the now current or greater seismicity of the region to be compliant with the RP 8 Standards.

SEISMIC FORM B - CERTIFICATE OF SEISMIC COMPLIANCE EXISTING BUILDING

The engineer shall evaluate the building to determine compliance with the Life Safety Performance Level. He or she shall use RP 8 Chapter 3 and ASCE/SEI 31 to determine compliance. The evaluation must include the appropriate Structural, Nonstructural, and Geologic Site Hazard and Foundation Checklists with backup calculations.

SEISMIC FORM C – BUILDING RETROFIT OR NEW CONSTRUCTION PRE-AWARD COMMITMENT

Part 1 only applies to planned retrofit of an existing building. The Offeror shall identify the engineer in charge of the seismic retrofit and commit that the retrofit's design and construction will conform to the requirements of ASCE/SEI 41, Basic Safety Objective. The commitment must also include a Tier 1 report with supporting documentation, a narrative, scope, and schedule of the proposed renovations.



Part 2 only applies to new construction. The Offeror shall identify the engineer in charge of the design of the building and specify which building code he or she is using to design and construct.

SEISMIC FORM D – OFFEROR’S REPRESENTATION OF EXEMPTION FROM SEISMIC STANDARDS

The Offeror may claim an exemption from seismic compliance if representing that the offered building meets either of the following exemptions:

- In an area of moderate seismicity, the total space leased in the building by the Federal government, including the offered space, will be less than 10,000 ABOA SF upon commencement of the lease term.
- In an area of high to very high seismicity, the offered building is a one-story building of steel light frame or wood construction with less than 280 m² (3,000 ABOA SF).

SEISMIC FORM E - CERTIFICATE OF SEISMIC COMPLIANCE RETROFITTED BUILDING

The engineer in charge of the building’s structural retrofit of the leased building shall certify that the design standard was the Basic Safety Objective as set forth in ASCE/SEI 41, Seismic Rehabilitation of Existing Buildings, and that the building was retrofitted to that standard.

SEISMIC FORM F - CERTIFICATE OF SEISMIC COMPLIANCE NEW BUILDING

The engineer shall certify that the design and construction of new buildings or additions to existing buildings conforms to the seismic provisions of the latest edition of the applicable State or local government codes under which it was built.

DEFINITIONS - The following definitions apply to the completion of the above-referenced forms:

1. **Engineer** means a professional engineer who is licensed in Civil or Structural Engineering and qualified in the structural design of buildings. They must be licensed in the state where the property is located.
2. **ASCE/SEI 31** means the American Society of Civil Engineers standard, Seismic Evaluation of Existing Buildings.” ASCE/SEI 31 can be purchased from ASCE at (800) 548-2723, or by visiting <http://www.pubs.asce.org>.
3. **ASCE/SEI 41** means American Society of Civil Engineers standard, Seismic Rehabilitation of Existing Buildings.” ASCE/SEI 41 can be purchased from ASCE at (800) 548-2723, or by visiting <http://www.pubs.asce.org>.
4. **Seismic Certificate** means a certificate executed and stamped by an Engineer on the appropriate Certificate of Seismic Compliance form included with this solicitation together with any required attachments.



5. **RP 8** means "Standards of Seismic Safety for Existing Federally Owned and Leased Buildings ICSSC Recommended Practice 8 (RP 8)," issued by the Interagency Committee on Seismic Safety in Construction as ICSSC RP 8 and the National Institute of Standards and Technology as NIST GCR 11-917-12. You can obtain RP 8 from the Building and Fire Research Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899, or download copy at http://www.wbdg.org/ccb/NIST/nist_gcr11_917_12.pdf.



SEISMIC FORM A

CERTIFICATE OF SEISMIC COMPLIANCE
BENCHMARK BUILDING

Date: _____

This affirms that _____ served as engineer in charge of the seismic evaluation of the building located at _____.

The building has the following characteristics:

ASCE Building Type:	No. of Stories:	Approx. Area:
Building Design Code:	Year of Design Code:	Year of Construction:

On the basis of the building characteristics and to the extent permitted by this level of evaluation, it is my opinion that the subject Building qualifies as a Benchmark Building as indicated in ASCE/SEI 31, Table 1-1.

Affix Stamp and Sign Here

Engineer's Name:

Firm:

Address:

Telephone:

License No.:

License State:

Expiration Date:



SEISMIC FORM B

**CERTIFICATE OF SEISMIC COMPLIANCE
EXISTING BUILDING**

Date: _____

This affirms that _____ served as engineer in charge of the seismic evaluation of the building located at _____.

The building has the following characteristics:

ASCE Building Type:	No. of Stories:	Approx. Area:
Building Design Code:	Year of Design Code:	Year of Construction:

I have evaluated this building at the Life Safety Performance Level as set forth in the ICSSC RP 8, Standards of Seismic Safety for Existing Federally Owned and Leased Buildings, using ASCE/SEI 31 methodology:

___ Tier 1 Evaluation

___ Tier 2 Evaluation

___ Tier 3 Evaluation

___ Other (please explain below)

Documentation of this evaluation must be attached to this Certificate.

On the basis of the building characteristics and to the extent permitted by this level of evaluation it is my opinion that subject Building (*check one*) does / does not meet the Life Safety Performance Level of ICSSC RP 8.

Affix Stamp and Sign Here

Engineer's Name:

Firm:

Address:

Telephone:

License No.:

License State:

Expiration Date:

Comments:

Attach: ASCE/SEI 31 Checklist(s) Structural, Nonstructural, and Geologic Site Hazards and Foundation.



SEISMIC FORM C

BUILDING RETROFIT OR NEW CONSTRUCTION
PREAWARD COMMITMENT

PART 1

PREAWARD COMMITMENT TO RETROFIT BUILDING:

Date: _____

This affirms that _____ shall serve as the engineer in charge of the seismic retrofit of the building located at _____. The retrofit must be designed to meet the **Basic Safety Objective**, as set forth in ASCE/SEI 41 Seismic Rehabilitation of Existing Buildings.

In accordance with the requirements of this Standard and the seismic paragraph in the Request for Lease Proposals (RLP), our offer includes a commitment to retrofit the building to satisfy all of the Basic Safety Objective requirements of ASCE/SEI 41. The offer includes a Tier 1 report with all supporting documents, a narrative explaining the process, scope of renovations, and a schedule for the seismic retrofit. Documentation shall be provided before award that demonstrates the seismic retrofit will meet the seismic standards and be completed within the time frame required.

PART 2

PREAWARD COMMITMENT TO CONSTRUCT A NEW BUILDING:

Date: _____

This affirms that _____ will serve as the engineer in charge of the structural design of the building located at _____. The criteria for design must be the _____ edition of the _____ building code.

In accordance with the requirements of this code, we prepared a quality assurance plan that included requirements for testing and inspecting critical elements of the structure and also periodic observation by our staff. We reviewed special inspection and testing reports prepared by the inspection agency and contractor submittals. On the basis of this, and to the extent permitted by this level of construction surveillance, it is my opinion that the Building was designed and constructed in conformance with the requirements of the above code.

The building has the following characteristics:

Building Type:	Building Height:	Approx. Area:
Building Design Code:	Year of Design Code:	Year of Construction:

OFFEROR

SIGNATURE

NAME OF SIGNER



SEISMIC FORM D

OFFEROR'S REPRESENTATION OF EXEMPTION FROM SEISMIC STANDARDS

Date: _____

I represent that my building is exempt from the requirements of RP 8 because:

- The Building is located in an area of medium seismicity and the Building will have less than 10,000 ABOA SF of space leased to the Federal Government upon commencement of the lease term.

- The Building is located in an area of high to very high seismicity, and it is a one-story building with a steel light frame or wood construction with less than 3,000 ABOA SF of space in the building.

OFFEROR	
SIGNATURE	NAME OF SIGNER



SEISMIC FORM E

CERTIFICATE OF SEISMIC COMPLIANCE
RETROFITTED BUILDING

PRE-OCCUPANCY CERTIFICATE:

Date: _____

This affirms that _____ served as the engineer in charge of the structural retrofit of the building located at _____. The standard for design was the Basic Safety Objective as set forth in ASCE/SEI 41 Seismic Rehabilitation of Existing Buildings.

In accordance with this Standard, we prepared a quality assurance plan, which requires staff to observe, test, and inspect the seismic retrofit work. We have also reviewed special inspection and testing reports prepared by the inspection agency and contractor submittals. On the basis of this, and to the extent permitted by this level of construction surveillance, it is my opinion that building was designed and constructed to conform with the requirements of the Standard listed above.

The building has the following characteristics:

ASCE Building Type:	No. of Stories:	Approx. Area:
Building Design Code:	Year of Design Code:	Year of Construction:
Retrofit Design Standard:	Year of Retrofit Standard:	Year of Retrofit:

Documentation of this retrofit must be available to GSA.

On the basis of the above, it is my opinion that subject Building ___ does, ___ does not meet the Basic Safety Objective - Performance Level as set forth in ASCE/SEI 41, Seismic Rehabilitation of Existing Buildings.

Affix Stamp and Sign Here

Engineer's Name:
Firm:
Address:

Telephone:
License No.:
State:
Expiration Date:



SEISMIC FORM F

CERTIFICATE OF SEISMIC COMPLIANCE
NEW BUILDING

PRE-OCCUPANCY CERTIFICATE:

Date: _____

This affirms that _____ served as the engineer in charge of the structural design of the building located at _____. The criteria for design were the _____ edition of the _____ code.

In accordance with the requirements, we prepared a quality assurance plan, which requires staff to observe, test, and inspect the structure's critical elements. We have also reviewed special inspection and testing reports prepared by the inspection agency and contractor submittals. On the basis of this, and to the extent permitted by this level of construction surveillance, it is my opinion that the building was designed and constructed to conform with the requirements of the code listed above.

The building has the following characteristics:

Building Type:	Bldg. Height:	Approx. Area:
Building Design Code:	Year of Design Code:	Year of Construction:

Affix stamp and sign here

Engineer's Name:

Firm:

Address:

Telephone:

License No.:

State:

Expiration Date:

Comments:

52.204-26 Covered Telecommunications Equipment or Services-Representation.

As prescribed in 4.2105(c), insert the following provision:

COVERED TELECOMMUNICATIONS EQUIPMENT OR SERVICES-REPRESENTATION (DEC 2019)

(a) *Definitions.* As used in this provision, “covered telecommunications equipment or services” has the meaning provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) *Procedures.* The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (<https://www.sam.gov>) for entities excluded from receiving federal awards for “covered telecommunications equipment or services”.

(c) *Representation.* The Offeror represents that it does, does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(End of provision)

Parent topic: 52.204 [Reserved]

PRE-LEASE BUILDING SECURITY PLAN

OFFEROR'S PRE-LEASE BUILDING SECURITY PLAN
EVALUATION FOR AN OFFICE BUILDING

The Offeror must complete a report based on a walk through of the building, parking areas, and structure's perimeter that includes the review of windows or window systems, facade protection level, and perimeter evaluation.

The Offeror states, as part of this offer, that the proposed space/building is as described below and contains the identified features and devices. Should this exhibit not provide sufficient space to respond adequately to any question, additional pages should be attached.

BUILDING ADDRESS	
BUILDING NAME:	
BUILDING ADDRESS:	
CITY:	
STATE:	
Year Built:	Year Last Renovated:
SIZE AND LAYOUT	
The following information applies to (check one):	
<input type="checkbox"/> an existing building <input type="checkbox"/> a building planned for lease construction	
Space offered to Government (By Floor):	
Approximate gross area of typical floor (identify atypical floors individually)	
Building Height in Feet:	
Number of Stories Above Grade	
Number of. Stories Below Grade:	
OTHER OCCUPANCIES IN BUILDING (Check All That Apply)	
Restaurants:	_____
Laboratories:	_____
Storage:	_____
Retail:	_____
Day Care Center:	_____
Other, list:	_____

PRE-LEASE BUILDING SECURITY PLAN

GENERAL INFORMATION

Provide digital pictures of the building. Include exterior views showing the front of the building and all sides of the building.

Identify the number of stories of the building (above and below grade)

Identify the approximate gross square footage per floor in the building.

Identify the proposed floors offered to the Government to occupy

<u>Exterior Materials</u>	<u>Yes</u>	<u>No</u>
Brick		
Block		
Concrete – Precast		
Concrete – Poured		
Metal Panels		
Glass Exterior		

Answer each question below, then, identify and discuss measures to be taken to protect and secure utilities.

<u>Question</u>	<u>Yes</u>	<u>No</u>
Is the water supply to the building protected?		
Is the main unit of air/ventilation system accessible to the public?		
Is the wire closet locked?		
Is utility access locked?		
Is there exterior access to the electric service?		
Is there exterior access to the gas service?		
Is there exterior access to the water service?		
Is there exterior access to the telephone service?		
Is there exterior access to any other heating source?		
Is fuel stored within the building?		
Are there exterior propane fuel tanks?		
For the facilities with exterior propane fuel tanks, are they protected?		

PRE-LEASE BUILDING SECURITY PLAN

PERIMETER INFORMATION

<u>General Public Access</u>	<u>Distance in Feet</u>
Distance in feet from the building to the nearest public street.	
Distance in feet from the building to the nearest public on-street parking.	
Distance in feet from the building to the nearest public parking lot.	

Provide a site sketch showing perimeter distances.

Describe the building's emergency lighting system.

Identify and describe the lighting levels provided at entrances/exits, garages, parking lots or other adjacent areas to the building to discourage "crimes against persons".

Identify and describe if emergency power is provided within the building.

If emergency power for life safety systems is provided by generator(s) or UPS systems describe if they are tested and maintained in accordance with NFPA 110 or NFPA 111, as applicable.

Identify and describe any garage or parking area control or surveillance systems in place.

Identify and describe the location of mechanical areas, along with protocol and procedures taken to secure these areas to ensure access by only authorized personnel.

Identify and describe roof access and the roof security, along with protocol and procedures taken to secure the roof to ensure access by only authorized personnel.

Identify and describe alarm/emergency notification system.

Review and evaluate the occupancy emergency plan.

Identify and describe window-glazing system, including,

- Typical size
- Thickness of panes
- Type of frame
- Type of anchorage
- Number of windows
- Type of glass
- Type of configuration (single-pane, insulated, laminated, etc.)
- Security film thickness (if installed)
- Date film was installed

If the proposed shatter-resistant window film is less than the 0.18 millimeter (7 mil) thickness specified in the SFO, a licensed professional engineer shall complete the evaluation specified below.

PRE-LEASE BUILDING SECURITY PLAN

For Build-to-Suit Solicitations and Alternative Blast Mitigation Proposals

A registered Professional Engineer shall complete the evaluations for window glazing and facade protection. The Professional Engineer's stamp (professional license) must be placed on the report.

For Build-to-Suit solicitations, identify and describe window systems in accordance with WINGARD 4.1 or later or WINLAC 4.3 software using the test methods provided in the US General Services Administration *Standard Test Method for Glazing and Window Systems Subject to Dynamic Overpressure Loadings* or F1642-04 *Standard Test Method for Glazing and Glazing Systems Subject to Airblast Loadings* - ASTM International.

For Build-to-Suit solicitations, identify and describe the facade protection level as prescribed by WINGARD 4.1 or later or WINLAC 4.3 software.

For Build-to-Suit solicitations, identify and describe the distance from the face of the building's exterior to the protected/defended perimeter (i.e., any potential point of explosion), around the complete circumference of the structure's exterior. This would mean the distance from the building to the curb or other boundary protected by bollards, planters or other barrier. All potential points of explosion must be evaluated that could be accessible by any motorized vehicle (i.e. street, alley, sidewalk, driveway, parking lot).

PRE-LEASE BUILDING SECURITY PLAN

STATEMENT OF PROFESSIONAL ENGINEER

I hereby attest that I have performed an assessment of the subject premises; and that the above information is complete and accurate to the best of my knowledge. I have initialed at the bottom of each page. My official stamp, professional license information, and signature are affixed below.

I HAVE INCLUDED FINDINGS, RECOMMENDED CORRECTIVE ACTION(S), AND MADE SPECIFIC REFERENCES TO THE APPLICABLE CODE SECTIONS OR SECURITY REFERENCE DOCUMENTS AS AN ATTACHMENT TO THIS REPORT. SUCH FINDINGS SPECIFICALLY IDENTIFY INSTANCES WHERE THE BUILDING DOES NOT COMPLY WITH THE SPECIFIED CRITERIA, AND RECOMMENDATIONS HAVE BEEN MADE IN ORDER TO RECTIFY THE SITUATION AND ASSURE SUBSTANTIAL COMPLIANCE OF THE BUILDING TO ALL APPLICABLE CRITERIA.

(if no deficiencies were identified, during the evaluation, please explicitly state so in the findings and recommendations portion of the report)

Signature: _____ Date: _____

Printed Name: _____

Name of Firm: _____

Phone #: (____) _____

License Number: _____

Stamp Here:

PRE-LEASE BUILDING SECURITY PLAN

OFFEROR'S STATEMENT OF CORRECTION

In the event any of the offered space does not meet the minimum specified performance conditions '3b' using the test methods provided in the US General Services Administration Standard Test Method for Glazing and Window Systems Subject to Dynamic Overpressure Loadings or F1642-04 Standard Test Method for Glazing and Glazing Systems Subject to Airblast Loadings - ASTM International, the Offeror shall attach a sheet describing the exact nature of the deficiency and will bring the offered space up to compliance with all applicable criteria to complete at the Offeror's sole cost and expense prior to the Government's acceptance of the offered space under the terms of any prospective lease agreement.

The Offeror shall attest below that the government, may implement all security operating standards. The base building security standards may include additional performance criteria for facade and setback, if feasible.

NOTE: REPORTS SUBMITTED WITHOUT RECOMMENDED CORRECTIVE ACTIONS WILL BE RETURNED WITHOUT REVIEW.

Signature: _____ Date: _____

Printed Name: _____

Title: _____

Name of Firm: _____

SAFETY AND ENVIRONMENTAL MANAGEMENT RELEASE CERTIFICATION CHECKLIST	
Building Name:	_____
Street Address:	_____
City:	_____ State: _____ Zip Code: _____
INSTRUCTIONS: Complete the following information that applies to the building being offered for lease by the Government. If building is not yet constructed, complete based on building plans and specifications.	
The following information applies to: (CHECK ONE)	
<input type="checkbox"/> an existing building <input type="checkbox"/> a building planned for construction	
Building structural support (check one):	
<input type="checkbox"/> Combustible (timber, wood, etc.) <input type="checkbox"/> Noncombustible (concrete, steel, masonry, etc.)	
Other types of uses present in the building (check all that apply):	
<input type="checkbox"/> Restaurants <input type="checkbox"/> Laboratories <input type="checkbox"/> Storage <input type="checkbox"/> Retail <input type="checkbox"/> Other; list _____	
Vertical openings between two or more floors:	
Stairs (check one):	<input type="checkbox"/> open <input type="checkbox"/> enclosed with doors
Shafts (check one):	<input type="checkbox"/> open <input type="checkbox"/> enclosed; describe _____
Other (check one):	<input type="checkbox"/> open <input type="checkbox"/> enclosed; describe _____
Sprinklers (check one):	
<input type="checkbox"/> None <input type="checkbox"/> Corridors only <input type="checkbox"/> All but corridors and lobbies <input type="checkbox"/> Total building <input type="checkbox"/> Other; describe locations: _____	
Fire fighting capability (check one):	
<input type="checkbox"/> None <input type="checkbox"/> Fire extinguishers only <input type="checkbox"/> Standpipes only <input type="checkbox"/> Standpipes and fire extinguishers	
Fire alarm (check one): _____	

**SAFETY AND ENVIRONMENTAL MANAGEMENT
PRELEASE CERTIFICATION CHECKLIST**

- None
- Building alarm without automatic fire department notification
- Building alarm with automatic fire department notification

Smoke detectors (check one):

- None
- All corridors
- Total building
- Other; describe locations: _____

Wall interior finish in space being offered for lease (check one):

- Painted walls of plaster, sheetrock, or masonry
- Wallpaper or vinyl wall covering
- Cloth or corkboard
- Hardwood paneling
- Other; describe: _____

Floor finish in space being offered for lease (check one):

- Carpet
- Tile
- Concrete
- Hardwood
- Other; describe: _____

Building size and layout

Approximate outside dimensions of building: _____

Total gross area of building: _____ square feet

Area of proposed lease: _____ square feet

Total number of floors in building: _____ Floor(s) of proposed lease: _____

Describe building layout, e.g., rectangular, E-shaped, U-shaped, etc.:

Exits (check one):

- No stairway; one floor on grade
- Stairways as described in the table below (Place checks in appropriate boxes except for "distance to Next Stair" column which should contain a number, measured in feet, indicating the required walking distance to the next exit stair.):

**SAFETY AND ENVIRONMENTAL MANAGEMENT
RELEASE CERTIFICATION CHECKLIST**

Which Stair	Stairway Enclosure		Location of Exit Discharge		Distance to Next Stair (in feet)
	Open	Separated by Doors	Inside Building	Directly to Outside	
Example	X		X		120
No. 1					
No. 2					
No. 3					
No. 4					

The example represents an open stair (no doors) which discharges inside the building (perhaps into a lobby). A person must walk approximately 120 feet to reach the next exit stair. **Note:** fire escapes and ladders must not be counted as exit stairs.

Additional information on exits, if any, e.g., sketch of building:

Asbestos. the building has (*check all that apply*):

- No asbestos
- Asbestos fire proofing or surfacing material
- Undamaged asbestos floor tile
- Asbestos pipe or boiler insulation in good condition
- Other undamaged asbestos; describe: _____
- Damaged asbestos; describe: _____
- Don't know

This information provided by the offeror on this form is material facts upon which the Government relies in making an award. The Government has the right to require remedy if there is a misrepresentation. The Owner or Authorized Representative certifies that all features are in operating order and properly maintained.

**SAFETY AND ENVIRONMENTAL MANAGEMENT
RELEASE CERTIFICATION CHECKLIST**

OWNER or AUTHORIZED REPRESENTATIVE	a. TYPED NAME AND ADDRESS (including ZIP code)	b. Telephone No. (including area code)
	c. SIGNATURE	d. Date Signed

INFECTION CONTROL RISK ASSESSMENT GUIDELINES – VA DESERT PACIFIC HEALTHCARE NETWORK

Identify the Type of Construction Project Activity (Types A-D)

A	<p>Non-invasive activities, including, but not limited to:</p> <ul style="list-style-type: none"> a. Removal of ceiling tiles where no dust or asbestos is expected b. Painting, but not sanding c. Wall covering, electrical trim work, minor plumbing, and activities which do not generate dust or require cutting of walls or access to ceilings other than for visual inspection
B	<p>Small scale, short duration activities which create minimal dust, including but not limited to:</p> <ul style="list-style-type: none"> a. Installation of electrical, plumbing, HVAC, telephone and computer cabling b. Access to chase spaces where asbestos is not present c. Cutting of walls or ceiling where dust migration can be controlled.
C	<p>Work that generates a moderate to high level of dust or requires demolition or removal of any fixed building components or assemblies, including but not limited to:</p> <ul style="list-style-type: none"> a. Sanding of surfaces for painting or wall covering b. Removal of floor coverings, ceiling tiles, and casework c. New wall construction d. Minor duct work or electrical work above ceilings e. Major cabling activities f. Any type A, B or C activity that cannot be completed within a single work shift.
D	<p>Major demolition and construction projects, including but not limited to:</p> <ul style="list-style-type: none"> a. Activities requiring heavy demolition or removal of a complete utility or cabling system b. New construction and renovation. c. Friable asbestos and mold abatement projects.

Identify the Patient Risk Group that will be affected. If more than one risk group will be affected, select the higher group. For all construction classes, patients must be removed from the room while work is performed.

Low	Medium	High	Highest Risk
All outpatient clinics, offices areas, administrative and industrial spaces.	All non-critical inpatient areas. cardiology, echocardiography, endoscopy, nuclear medicine, rehabilitation medicine, radiology, MRI, respiratory therapy, dry research labs.	DOU, emergency room, clinical laboratory, wet lab research, ambulatory surgery, pharmacy, surgical and medical inpatient beds, procedure center.	Immunocompromised patient area, cath lab, SPD, ICU, occupied, negative pressure rooms, PACU operating rooms.

Match the Patient Risk Group with the Construction Project Type (A, B, C, D) to find the Class of Precautions (I – V)

Construction Project Type

Patient Risk Group	TYPE A	TYPE B	TYPE C	TYPE D
Low Risk	I	II	III	V
Medium Risk	I	II	IV	V
High Risk	I	II	IV	V
Highest Risk	II	III	V	V

Description of Required Infection Control Precautions by Class

Class	During Construction Project	Upon Completion of Project
Class I	<ol style="list-style-type: none"> 1. Execute work by methods to minimize raising dust from construction operations. 2. Immediately replace ceiling tile if displaced. 	
Class II	<ol style="list-style-type: none"> 1. High Risk patients must remain out of room for one hour after completion of work and cleanup. 2. Execute work by methods to minimize raising dust. 3. Immediately replace ceiling tile if displaced. 	<ol style="list-style-type: none"> 1. Remove all visible debris with a wet towel and/or mop. 2. Housekeeping to wipe work surfaces and floors with disinfectant.
Class III	<ol style="list-style-type: none"> 1. Execute work by methods to minimize raising dust. 2. Immediately replace ceiling tile if displaced 3. Provide active means to prevent airborne dust from dispersing into atmosphere. 4. Water-mist work surfaces to control dust while cutting. 5. Seal unused doors with duct tape. 6. Isolate HVAC system in areas where work is being performed to prevent contamination of duct system. 7. Place dust mat at entrance and exit of work area. 8. Cover construction waste before transport in covered containers 	<ol style="list-style-type: none"> 1. Cover construction waste before transport in covered containers. 2. Wet mop and/or vacuum with HEPA filtered vacuum before leaving work area. 3. Open previously sealed HVAC registers and grills. 4. Housekeeping to wipe work surfaces and floors with disinfectant.
Class IV	<ol style="list-style-type: none"> 1. Install plastic dust barriers to seal area from non-work area or implement control cube method (cart with plastic covering and sealed connection to work site with HEPA vacuum for vacuuming prior to exit) before construction begins. 2. Isolate HVAC system in areas where work is being performed to prevent contamination of duct system. 3. Maintain negative pressure within work site utilizing HEPA equipped air filtration units. 4. Place dust mat at entrance and exit of work area. 5. Cover construction waste before transport in covered containers. 6. All work associated with a major project that has an approved ICRA authorization form will be assessed on an individual basis. 	<ol style="list-style-type: none"> 1. Cover construction waste before transport in covered containers. 2. Wet mop and vacuum with HEPA filtered vacuum. 3. Do not remove barriers from work area until a Health System responsible person inspects completed project. 4. Remove barrier materials carefully to minimize spread of dirt and debris associated with construction. 5. Wet mop and vacuum with HEPA filtered vacuum before leaving work area. 6. Remove isolation of HVAC system in areas where work was being performed. 7. Housekeeping to wipe work surfaces and floors with disinfectant.
Class V	<ol style="list-style-type: none"> 1. Construct gypsum board/metal stud dust partition, extend and seal to ceiling. 2. Isolate HVAC system within work areas to prevent contamination of duct system. 3. Seal doors opening to adjacent areas with duct tape. 4. Block off and seal HVAC registers, grills and any openings in ductwork to remain. 5. Maintain negative pressure within work site utilizing HEPA equipped air filtration units. 6. Place dust mat at entrance and exit of work area. 	<ol style="list-style-type: none"> 1. Cover construction waste before transport in covered containers. 2. Wet mop and vacuum with HEPA filtered vacuum. 3. Do not remove barriers from work area until a Health System responsible person inspects completed project. 4. Remove barrier materials carefully to minimize spread of dirt and debris associated with construction. 5. Wet mop and vacuum with HEPA filtered vacuum before leaving work area. 6. Remove isolation of HVAC system in areas where work was being performed. 7. Housekeeping to wipe work surfaces and floors with disinfectant.

	<ul style="list-style-type: none"> 7. Cover construction waste before transport in covered and sealed containers. Biohazards to be double bagged. 8. All work associated with a major project that has an approved ICRA authorization form will be assessed on an individual basis. 9. Provide monitoring and clearance samples for mold/asbestos. 	
--	---	--

INFECTION CONTROL CONSTRUCTION PERMIT FOR CLASS IV AND V PRECAUTIONS

	Location of Activity:	Project Start Date:
	Project Coordinator:	Estimated Duration:
	Contractor Performing Work:	Permit Expiration Date:
	Supervisor:	Telephone:
Construction Type:		Risk Group:
Precaution Class:		
Class I	<ul style="list-style-type: none"> 1. Execute work by methods to minimize raising dust from construction operations. 	<ul style="list-style-type: none"> 2. Immediately replace ceiling tile if displaced. 3. Clean work area upon completion of task.
Class II	<ul style="list-style-type: none"> 1. High Risk patients must remain out of room for one hour after completion of work and cleanup. 2. Execute work by methods to minimize raising dust. 	<ul style="list-style-type: none"> 3. Immediately replace ceiling tile if displaced. 4. Remove all visible debris with a wet towel and/or mop. 5. Housekeeping to wipe work surfaces and floors with disinfectant.
Class III	<ul style="list-style-type: none"> 1. Execute work by methods to minimize raising dust. 2. Immediately replace ceiling tile if displaced 3. Provide active means to prevent airborne dust from dispersing into atmosphere. 4. Water-mist work surfaces to control dust while cutting. 5. Seal unused doors with duct tape. 6. Isolate HVAC system in areas where work is being performed to prevent contamination of duct system. 	<ul style="list-style-type: none"> 7. Place dust mat at entrance and exit of work area. 8. Cover construction waste before transport in covered containers 9. Wet mop and/or vacuum with HEPA filtered vacuum before leaving work area. 10. Open previously sealed HVAC registers and grills. 11. Housekeeping to wipe work surfaces and floors with disinfectant.
Class IV	<ul style="list-style-type: none"> 1. Obtain infection control permit before construction begins. 2. Install plastic dust barriers to seal area from non-work area or implement 	<ul style="list-style-type: none"> 7. All work associated with a major project that has an approved ICRA authorization form will be assessed on an individual basis using the Risk Assessment and Exposure Control

	<p>control cube method (cart with plastic covering and sealed connection to work site with HEPA vacuum for vacuuming prior to exit) before construction begins.</p> <p>3. Isolate HVAC system in areas where work is being performed to prevent contamination of duct system.</p> <p>4. Maintain negative pressure within work site utilizing HEPA equipped air filtration units.</p> <p>5. Place dust mat at entrance and exit of work area.</p> <p>6. Cover construction waste before transport in covered containers.</p>	<p>Checklist.</p> <p>8. Wet mop and vacuum with HEPA filtered vacuum.</p> <p>9. Do not remove barriers from work area until a Health System responsible person inspects completed project.</p> <p>10. Remove barrier materials carefully to minimize spread of dirt and debris associated with construction.</p> <p>11. Wet mop and vacuum with HEPA filtered vacuum before leaving work area.</p> <p>12. Remove isolation of HVAC system in areas where work was being performed.</p> <p>13. Housekeeping to wipe work surfaces and floors with disinfectant.</p> <p>14. Complete daily log documenting work activity and completion of remedial and preventive procedures required.</p>					
Class V	<p>1. Obtain infection control permit before construction begins.</p> <p>2. Construct gypsum board/metal stud dust partition, extend and seal to ceiling.</p> <p>3. Isolate HVAC system within work areas to prevent contamination of duct system.</p> <p>4. Seal doors opening to adjacent areas with duct tape.</p> <p>5. Block off and seal HVAC registers, grills and any openings in ductwork to remain.</p> <p>6. Maintain negative pressure within work site utilizing HEPA equipped air filtration units.</p> <p>7. Place dust mat at entrance and exit of work area.</p> <p>8. Cover construction waste before transport in covered containers.</p> <p>9. All work associated with a major project that has an approved ICRA authorization form will be assessed on an individual basis using the Risk Assessment and Exposure Control Checklist.</p>	<p>10. Wet mop and vacuum with HEPA filtered vacuum.</p> <p>11. Cover construction waste before transport in covered and sealed containers. Biohazards to be double bagged.</p> <p>12. Provide monitoring and clearance samples for mold/asbestos.</p> <p>13. Do not remove barriers from work area until a Health System responsible person inspects completed project.</p> <p>14. Remove barrier materials carefully to minimize spread of dirt and debris associated with construction.</p> <p>15. Wet mop and vacuum with HEPA filtered vacuum before leaving work area.</p> <p>16. Remove isolation of HVAC system in areas where work was being performed.</p> <p>17. Housekeeping to wipe work surfaces and floors with disinfectant.</p> <p>18. Complete daily log documenting work activity and completion of remedial and preventive procedures required.</p>					
Exceptions or additions to this permit are noted on the attached page. <input type="checkbox"/> Yes <input type="checkbox"/> No							
Permit Requested By:		Date:		Approval By Service Affected:		Date:	
Approval by Safety Officer/IH:		Date:		Approval by Infection Control:		Date:	

Lessor: _____ Govt: _____

Exhibit N

VA Department of Veterans Affairs

DAILY LOG - FORMAL CONTRACT			STATION:
PROJECT TITLE			NAME OF CONTRACTOR
DATE			CONTRACT NUMBER
DAY OF WEEK			PROJECT NUMBER
WEATHER			TEMPERATURE

BRANCH OF WORK	SKILLED WORKERS	UNSKILLED WORKERS	LOCATION AND DESCRIPTION OF WORK

DELIVERY OF MATERIALS:

REMARKS:

Barrier installed	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Isolate HVAC	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Seal Doors	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Maintain negative pressure	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Dust mat at entrance to work area	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Cover construction waste for transport	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Wet mop, HEPA vacuum and inspection prior to barrier removal	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Remove construction barrier	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Wet mop and HEPA vacuum	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Reinstate HVAC	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Wipe work surfaces with disinfectant	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A

Signature of Project
Manager

VA Department of Veterans Affairs

DAILY LOG - SAFETY/ILSM CHECKLIST	STATION:
PROJECT TITLE	NAME OF CONTRACTOR
DATE	CONTRACT NUMBER
DAY OF WEEK	PROJECT NUMBER

Interim Life Safety Measure / Hazard Surveillance	
Means of egress is clear in construction and adjacent areas.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Access for the fire department and emergency services is clear.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Note the status of the fire detection/sprinkler system	
Fire sprinkler system is active.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Fire alarm system is active.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Smoke detectors are active.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Temporary systems are in place	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Construction partitions are being maintained and are smoketight.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Good housekeeping practices are being maintained.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Exterior balconies, corridors, and stairways clear of storage	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Flammables & combustibles kept to a minimum and in proper containers.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Buildings, grounds, and equipment are maintained in a safe manner.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Smoking regulations are being followed.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Fire extinguisher are readily available in construction area.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Hot work permit issued	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Work site inspected after hot work	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Other Environmental Considerations / Hazard Surveillance	
Caution/ danger signs and barricades in place where needed.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Lock out/tagout in place	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Extension cords protected/disconnected at end of day.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Dust barriers maintained.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
MSDS maintained on site and products labeled.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Asbestos is properly controlled and interstitial doors are closed & locked.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Area is secured from public and at the end of the day.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Odors from construction operations are cleared.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Safety and temporary signage is in place.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Emergency recall numbers left at work site.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Utility systems returned to operation in occupied areas.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Construction storage/field offices maintained and secured.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Excavations properly barricaded.	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
All external openings in walls/roof are sealed from inclement weather	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Exterior storm drains flushed and cleared of debris	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Subcontractors aware/trained in safety/environmental issues	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
HEPA unit in place, functioning, and on E Power	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Environmental monitoring for mold	<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A
Inspected by:	

VA Desert Pacific Healthcare System

Project: _____

Date: __

Hazard	Concern? Y/N	Control Measure	Remarks
Asbestos			
Dust			
Moisture/water leaks			
Vapors/fumes			
Noise			
Vibration			
Air pressure relationships			
Traffic flow			
Open outside walls			
Impact to levels above and below			
Proximity of air intakes			
Pest control within construction area			
Proximity of immune suppressed patients			

Approval Signatures:

Project Manager: _____

Chief Engineering Section: _____

Infection Control: _____

Industrial Hygienist: _____

Contractor: _____

Service/Section/Program Chief: _____

Control Measures

Asbestos

1. Contractor has hired an asbestos abatement contractor for control and cleanup.
2. VA to hire independent IH to inspect and clear area for re-occupancy based on monitoring and/or professional judgment.
3. Published asbestos protocol to be followed for work thru ceiling.
4. Published asbestos protocol to be followed for work above ceilings.
5. Perimeter barrier will be constructed in the interstitial space to isolate the construction area with other areas in the interstitial.
6. Project area will be encased with spray applied hard surface encasement material.
7. Provide mini containments under negative air in public areas.
8. Sealed gypsum board barrier will be constructed to isolate the construction area from the public.
9. Transit Panels will be removed which is considered Class B removal

Dust

1. Sealed gypsum board barrier will be constructed to isolate the construction area from the public.
2. Trash carts will be covered when transported thru the building.
3. Provide negative air machine exhausted to outside.
4. Provide mini containments under negative air in public areas.
5. Provide negative air machine in space as air scrubber.
6. Provide walk off mats at entrances to work area
7. Perimeter barrier will be constructed in the interstitial space to isolate the construction area with other areas in the interstitial.

Moisture Water Leaks

1. Contain any water from core drilling activities.
2. Dike any floor penetrations to minimize risk of leaks from construction zone.

Vapors/Fumes

1. Use of products with low VOC's.
2. Provide negative air in construction zone exhausted to outside away from intakes.
3. Seal work area airtight barrier.
4. Cut all metal outside the building.
5. Seal any floor penetrations to minimize risk of fumes thru construction zone.
6. Shut down air handler to minimize infiltration of fumes from outside.

Noise

1. Schedule demolition work after normal work hours.
2. Cut all metal outside the building.

Vibration

1. Schedule demolition work after normal work hours.
2. Coordinate with occupants in surrounding areas to explain the work occurring

Air Pressure Relationships

1. Provide negative air during asbestos abatement.
2. Provide negative air during construction
3. Seal off supply and exhaust HVAC registers.
4. Provide anti room under negative pressure at entrance to project zone.

Traffic Control

1. Access construction area via exterior door.
2. Schedule delivery of large quantities of material and demolition haul out after hours.

Open Outside Walls

1. Construct temporary outside wall to limit the infiltration of wind, air, and temperature differences into the project site.

Impact to Levels Above and Below

1. Coordinate with occupants in surrounding areas to explain the work occurring.
2. Follow asbestos protocol when doing under floor work
3. Vacate areas when doing below floor work off of the catwalk.

Proximity of Air Intakes

1. Shut down air handlers to reduce infiltration of fumes from exterior activities such as painting, gasoline powered engines, roofing operations, equipment, etc.

Pest Control Within Construction Area

1. Provide barriers to any open outside walls
2. Contact Pest Controller if any evidence of pests are found during the course of the work.

Proximity of immune suppressed patients

1. Relocate patients away from construction zone for entire project.
2. Relocate patients away from construction zone during demolition operations.

Offeror's Rate for Routine Cleaning and Disinfection Requirements

Note to Offeror: If submitting offer electronically through GSA's Lease Offer Platform (AAP or RSAP), upload using the "Other" attachment type from the options provided.

Indicate rental charge to provide routine cleaning and disinfecting services as described under the sub-paragraph N of the Lease paragraph "Janitorial Services." The Government reserves the right to cancel these services and reduce the rent accordingly.

\$ _____ per ABOA SF

\$ _____ per Rentable SF

.