Section C - RFI Statement of Work for Legislative Branch CAD-CAFM Software/Services IDIQ

C.1 OVERVIEW / BACKGROUND

The Library of Congress' (LOC or Library) Space Utilization, Planning and Design (SUPD) provides space planning, interior design procurement and construction management services (in conjunction with the Architect of the Capitol (AOC)) for all Library facilities. SUPD also monitors, plans, designs space requirements, and maintains an efficient and cohesive facility aesthetic on and off the Library Capitol Hill Campus including the James Madison Memorial Building (2, 034,443 Sq. Ft), the John Adams Building (1,043,193 SQ. FT), the Thomas Jefferson Building (1,064,859 SQ. FT), the Taylor Street Annex (88,000 SQ. FT), St Ce- Celia's Special Facility (44,000 SQ. FT), Ft. Meade Book Storage Modules (208,535 SQ. FT), the Cabin Branch Facility (146,121 SQ. FT), and the National Audio-Visual Conservation Center (NAVCC) in Culpepper VA (346,500 SQ. FT). SUPD develops and implements Library policy governing the use of space, and furniture and finish standards. Library furniture and finishes include systems furniture, wood case goods, custom wood furniture, meeting and conference furniture, filing and storage, lounge furniture, and furniture accessories and ergonomic devices. Projects managed by SUPD range in scope from designing secured collections storage and processing facilities, to renovating and updating training centers and commercial office environments.

LOC anticipates solicitation and award of a multiple-award, five-year, Indefinite Delivery Indefinite Quantity (IDIQ) contract that will permit the issuance of Firm Fixed Price (FFP) task orders (TO). It is desired that awardees be capable of fulfilling multiple requirement areas. Orders under this contract may be placed by any legislative branch agency within the United States Government, including: The Architect of the Capitol, Congressional Budget Office, Government Accountability Office, Government Printing Office, Library of Congress, Medicare Payment Advisory Commission, Office of Congressional Workplace Rights, Congressional Office of International Leadership, U.S. Capitol Police, U.S. House of Representatives, and the U.S. Senate. Orders may be placed by a contracting officer within a legislative branch agency pursuant to the ordering clause of this contract. The contractor shall report no less than annually to the COR and Contracting Officer of this contract the number, dollar value, ordering agency, and scope of all orders placed within the contract's period of performance. Orders shall be placed for defined requirements that are fulfilled utilizing an incorporated Price Schedule labor categories and rates. In the event that a task order period of performance crosses fiscal or accounting periods as defined in the agreed upon Price Schedule, task order labor rates must comply with the annual price that is current at the time the order is placed. No blended rates will be authorized at the order level.

C.2 SCOPE

This contract shall provide the full range of Computer Aided (CAD), Building Information modeling (BIM) and Computer Aided Facility Management (CAFM) software and technical support services along with facility site surveying and auditing services. The anticipated services resulting from this IDIQ will support activities that include:

1) Server Based Enterprise Licenses for Autodesk/AutoCAD and Revit or equivalent design, drafting, and building information modeling (BIM) software products.
2) CAD, BIM, and Computer Aided Facility Management (CAFM) drafting and technical services.
3) Facility site surveying and auditing services.
4) Training for users and administrators on basic and advanced features of the software including development and training of standard operating procedure documents.
5) Access to help desk support services for the software.

C.3 REQUIREMENTS

C.3.1 Principal Task Areas

The support required in the principal task areas are listed below, Legislative Branch agencies (listed in section C.1) may order the full range of software, support, training and facility site solutions and services necessary in the following task areas indicated below as they fit to fulfill requirements.

C.3.1.1 Task Area 1: Server Based Enterprise Licenses for Autodesk/AutoCAD and Revit or equivalent design, drafting, and building information modeling (BIM) software products

C.3.1.1-1 The suite of Software provided must include:

A. Capabilities for 2D Design, 3D Design, and Building Information Modeling (BIM)

- 2D Design Features must include:
  - Sketching tools
  - Customizable tool palettes, color pallets, and command log
  - Industry-specific toolsets
  - Generate 2D drawings from 3D models
  - Controls for the transparency of objects or layers
  - Controls to find and select objects based on properties
  - Create scalable text in multiple formats and automatically update text via fields
  - Create dimensions automatically and provide tools for area, volume, and distance calculations
  - Have easily format able leader lines
  - Be able to create centerlines and center marks
  - Ability to create tables combining data and symbols
  - Ability to draw revision clouds
  - Save views by name and to quickly navigate between views
  - Create and specify different sized layouts and title blocks
  - Enable simultaneous updates by providing live links between files and Excel spreadsheets
  - The ability to extract data from drawing information, objects, and attributes
  - Include dynamic block functions
  - Create or modify objects in circular or rectangular patterns and along a path
  - Apply geometric and dimensional constrains to maintain relationships between geometry
- 3D Design Features must include:
  - Parametric Modeling Tools
  - Industry-specific toolsets
  - Ability to view real time texture and material changes as they occur
  - Extrude 3D models from 2D Drawings
  - Create photorealistic models
  - Have basic animation features
  - Solid, surface, and mesh modeling tools
  - Orbit, swivel, walk, and fly over 3D navigation tools
  - Visual styles that control edges, lighting, and shading
  - Ability to section planes and create cross-section views
  - Apply lighting and materials to 3D renderings
  - Ability to attach point clouds
- BIM Features must include:
  - Provide Geo Location
  - Industry-specific toolsets
  - Ability to use third-party tools to make changes to material finishes
  - Sketch and create freeform models and create massing studies
  - Store performance data

- Connect laser scans directly to the BIM model
- Ability to derive construction insight from design models

B. Interoperability Features
- Must support the following formats: 3DS, DWF, DWG, PDF, RVT, DGN
- Must have Google Mapping integration
- Must work with readily available model libraries from major furniture manufacturers

C. Autodesk/AutoCAD licenses
- The licenses must last no less than one year and be installed on an enterprise license server so that they may checked out by multiple users.
- The contractor shall install the software on the Library's servers and configure it for use based on Library specifications. The contractor shall assure compliance with the requirements of Federal Information Security Management Act (FISMA).
  - Additional Autodesk/AutoCAD Licensing Features required:
    - The software must be available via a check-out system that allows different users (greater than the number of software licenses purchased) to access and use the software non-concurrently.
    - The software must have a function that allows access to the software when not connected to the inter/intranet.

C.3.1.2 Task Area 2: CAD, BIM, and Computer Aided Facility Management (CAFM) drafting and technical services

C.3.1.2-1 The contractor shall provide technical services including:

A. Creation and updates to design standards and standard operating procedures (SOP) documents to include guidance and standards for internal Library staff use as well as vendor use for Block insertion and development, Layer Management, and CAFM integration.

B. Master CAD File Cleanup and Updates.

i. Incorporating design files into master files
- Revise and/or replace all blocks using Library standard blocks
- Remove all text related to Staff and Organization Names, Space Type (e.g. Office, Pantry, Reading Room, etc.)
  - Remaining text should be Door Numbers, Column Numbers, Stair Numbers, Core Designation (Core A, B, C, etc.), Fixed Equipment Designation (e.g. Thermostat, Fire Extinguisher, etc.), Restroom Designation (e.g. Women, Men, Family), Location Designation (e.g. South Curtain, North-West Court, Roof, Crawl Space, etc.)
- Update Layers to Match Library Standard
  - All files to be saved with the current layer "0"
  - All files to have the same color for layer "0"
  - Delete all unused layers
  - All line weights to be 0.00

ii. XREF Management
- Remove circular references within master files
- Remove items that are not associated with the master drawing type
  - IN drawings to have furniture items only
  - AR drawings to have FTC walls / doors only

- BAS drawings to have all walls except FTC, all doors except FTC, stairs, elevators, columns, fixed items such as colonnades, planters, exhibits, decorative items

C. CAFM Support
   - Provide troubleshooting support for AutoCAD and Revit (BIM) CAFM connectors, assist with creating and correcting configuration parameters in CAD files and Revit models, provide best practices to ensure the correct steps are taken when creating files and integrating them into the CAFM database Produce and/or maintain CAFM line or architecture files incorporating updates from the master CAD files in a format compatible with the Facility Management Database, currently Tririga.

C.3.1.3 Task Area 3: Facility site surveying and auditing services

C.3.1.3-1 The contractor shall provide Site Surveying services

- The Contractor shall provide site surveys to assist in space audits and master drawing updates. The Contractor will be required to conduct walkthroughs of entire floors or designated sub-areas and conduct field-measurements. The purpose of the walk-throughs is to ensure the Architectural and Interior drawings and information are accurate. Space Audits are used for the correction of architectural and interior elements in tenant/occupied or unoccupied areas throughout the entire floor or designated area. Surveys may require validating or correcting drawing layouts of furniture, equipment, shelving, demountable or Floor-to-Ceiling (FTC) walls, shell and core building elements. The Contractor may also be required to certify occupants and occupant types as defined by Building Owner's and Manager's Association (BOMA) standards, and incorporate the data from the surveys into a CAFM database system.
   - When field measurements are completed, the Contractor shall submit original marked up copies, or color copies of the marked up drawings of their fieldwork to the Contracting Officer's Representative (COR).

C.3.1.4 Task Area 4: Training for users and administrators on basic and advanced features of the software including development and training of standard operating procedure documents.

C.3.1.4-1 The contractor shall provide onsite, virtual, or offsite classroom training to all licensed users to acquire skills for accomplishing the following tasks using the software:

- Project Drawing Setup;
- Network Mapping;
- Printing/Plotting;
- Layering;
- Blocks and Symbols;
- Documentation of Conversion Processes; and
- Project Management
- CAFM updates

C.3.1.4-2 The contractor shall deliver training classes for the ***basic and advanced user*** so they will know how to convert data files on their own. Training shall be offered onsite, virtually, or at a location where the versions and configurations match the software purchased by the Library. The contractor shall provide training material at these locations. Training shall be provided by an instructor who is an Autodesk Certified Professional or equivalent expertise for another brand proposed for that module.

C.3.1.5 Task Area 5: Access to helpdesk support services

C.3.1.5-1 The contractor shall provide online services and a live helpdesk with remote access to Library systems as well as on-site troubleshooting support. The contractor's helpdesk shall provide responses to the Library within one business day of submission.

C.4. CONTRACT PERFORMANCE

C.4.1 SCHEDULE OF EVENTS/DELIVERABLES

Paragraph reference	**Description of Event/Deliverable**	**Due date/ Payment schedule**
	IDIQ Kickoff Meeting	Within *five business days of IDIQ period of performance start date.*
C.3.1.1	Software Licenses - Server Based Enterprise Licenses for Autodesk/AutoCAD and Revit or equivalent design, drafting, and building information modeling (BIM) software products.	Within 30 days of task order start date. Payment upon acceptance
C.3.1.2	CAD, BIM, and Computer Aided Facility Management (CAFM) drafting and technical services.	Within 30 days of task order start date. Payment upon acceptance
C.3.1.3	Facility site surveying and auditing services.	Delivery/Schedule to be outlined in Task Orders. Payment upon acceptance
C.3.1.4	Training for users and administrators on basic and advanced features of the software including development and training of standard operating procedure documents.	Within 30 days of task order start date. Payment upon acceptance
C.3.1.5	Access to helpdesk support services.	Within 30 days of task order start date. Payment upon acceptance
C.4.2	Finalized Quality Control Plan (QCP)	Draft submitted with proposal; final 10 days after kick off meeting
C.5.4.1	Monthly Summary Report on active task orders for services identified under Task Areas 2 through 4.	Monthly reports are due on the 5th business day of the month following the task order start date.

C.6.2	Implementation File Transfer Protocol (FTP) Accessible site through users passwords and ID	10 days after kick off meeting to be accessible by licensed users/ COR

Additional schedule of deliverables will be provided at the task order level.

C.4.2 QUALITY CONTROL

The contractor shall develop and maintain an effective quality control program (QCP). Draft submitted within proposal; final due 10 days after kick off meeting. Services shall have performed in accordance with this contract. The contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The contractor's quality control program is the means by which it assures its work complies with the requirement of the contract. After acceptance of the quality control plan the contractor shall receive the contracting officer's representative acceptance in writing of any proposed change to its QC system. Task Orders (TO) may specify additional QCP requirements specific to that TO.

C.4.3 CONTROLLED UNCLASSIFIED INFORMATION (CUI)

If the contractors or sub-contractors are performing work on the Library's master drawings, then the contractor will be required to attend a mandatory training provided by the AOC/LOC in security of controlled unclassified Information. In May 7, 2008 the Executive Branch adopted "CUI" as the single designator for all sensitive but unclassified information to facilitate the movement of sensitive information.

C.5 ADDITIONAL INFORMATION

C.5.1. PLACE OF PERFORMANCE. The work to be performed under the contract will be performed at contractor's offices, training facilities, or government facilities as indicated in each task order.

C.5.2. HOURS OF OPERATION. The Library's hours of operation are: Monday thru Friday 8:30 AM to 5:00 PM, except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings.

C.5.3. GOVERNMENT FURNISHED PROPERTY

A. Applicable Documents: The government will provide all relevant and available project information necessary for the work, including: drawing files; drawing standards; program assessments; facility construction standards; electronic copies of existing floor plans; and Library of Congress regulations as indicated on individual orders.

B. Services/ Computer Hardware: The government may provide workspace and/ or a workstation/Laptop on an as needed basis to the selected contractor and based on the requirements of the individual orders. All contractor personnel performing site surveys on a recurring basis will need to apply and be issued a LOC security badge in accordance with Library security requirements currently in effect. Contractors accessing the Library's computer systems will be required to take mandatory Library security training and refresher courses.

C.5.4 INFORMATION AND REPORTING

The Contractor shall provide information identified below. This information shall be intended to provide the COR and end user maximum visibility of the status of their requested actions, and the COR and

Contracting Officer visibility of funding requirements and prices experienced, both to date, and anticipated. Monthly reports are due on the 5th business day of the month and are required to have the following information:

C.5.4.1 A Monthly Summary Report on active task orders for services identified under Task Areas 2 through 4. The Report should include:

a. Progress made towards deliverables and if deliverables will be completed per contract requirements.
b. Number of hours spent on deliverables.
c. Action items and assignments needed to complete deliverables.

C.5.4.2 The contractor may be required to produce weekly reports and meeting minutes as outlined at the task order level.

C.5.5 Travel

Travel costs may be included in specific task orders at the discretion of the LOC contracting officer. Any authorized travel expenses shall not exceed the amounts expressed in the Federal Travel Regulation.

C.5.6 Administrative and Other Direct Costs

Other Direct Costs (ODCs) may be included in task orders for applicable costs that are not accurately categorized as labor, material, overhead, or profit under any type of order (FFP or Labor-Hour). ODCs may be included based on the CO's determination that the ODCs are offered at a fair and reasonable price, and the inclusion of ODCs is in the best interest of the government in order to complete associated requirements.

C.5.7 Project Management Costs

Any contractor Project Management costs shall be included as a direct labor cost in the price of each task order, if required. Project Management (PM) costs shall not be authorized as an indirect cost under any order.

C.6 SPECIAL QUALIFICATIONS.

C.6.1 KEY PERSONNEL:

Contractor will assign a contract manager who will participate and maintain oversight of production, deliverables, provide quality control, attend progress review meetings, and be responsible for the overall performance of the work under the IDIQ. The name of this person and an alternate who shall act for the contractor when the manager is absent shall be designated in writing to the Contracting officer. The contract manager or alternate shall have full authority to act for the contractor on all contract matters relating to daily operation of this contract.

C.6.2 FILE SHARING CAPABILITIES AND HANDLING CUI:

Contractor will create an FTP (File Transfer Protocol) site to transfer drawing files and electronic deliverables to the Library. The site must be accessible to the Library through a user ID and password be maintained per Architect of the Capitol Security Standards, which will be provided upon contractor request.

Contractors handling drawing files will be required to take government led CUI training and refresher courses.

-END RFI STATEMENT OF WORK-

Relevant Information Technology (IT) Clauses:

From AOC52.223-3 Security Markings

(a) This clause applies to all contractors and subcontractors who have access to, or generate, information or other resources that contain Controlled Unclassified Information (CUI). This includes contractors, subcontractors and the employees of contractors and subcontractors.

(1) Contractors shall instruct, train and supervise its personnel on safeguarding CUI.

(2) CUI must not be disseminated in any manner; orally, visually or electronically to unauthorized personnel.

(3) This clause shall be inserted into all subcontracts.

(b) This clause requires compliance with the AOC program to identify, mark, and protect documents containing such CUI information.

(1) Contractors and Subcontractors shall use categories cited in the National Archives and Records Administration (NARA) CUI registry to designate information as CUI. The registry can be found at: http://www.archives.gov/cui/. CUI documents do not require a document register.

(2) All contractors and subcontractors have a duty to protect CUI from improper disclosure. Personnel with custody of CUI are responsible for taking reasonable steps to safeguard CUI and are under an affirmative duty to report any known security breaches to the Contracting Officer.

(c) CUI is unclassified information that is pertinent to the security of the Congress, the Supreme Court or the national interest of the United States or originated by entities outside the U.S. Federal Government, and under law or policy requires special handling safeguards, protection from disclosure, and prescribed limits on exchange or dissemination. CUI includes, but is not limited to: information related to personal and proprietary information, agency operations, security protected information, and records or sensitive information compiled for AOC or LOC authorized activities. It is essential that this information be marked, properly handled, stored and protected from inadvertent or deliberate disclosure, alteration or destruction.

(d) Information designated as CUI will be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements:

(1) The lack of CUI markings on CUI materials does not relieve a person from CUI safeguarding responsibilities.

(e) Documents shall be marked "CONTROLLED" at the top center of each page containing CUI. For consistency with classified systems, the document may also be marked "//CONTROLLED//." For consistency with classified systems, internal pages may be marked "//CONTROLLED II" or "//CUI//"; in such cases internal pages shall be marked at both the top and bottom.

(1) Each part of electronically transmitted messages, including e-mail containing CUI shall be marked. Unclassified messages containing CUI shall be marked "CONTROLLED" (optionally "//CONTROLLED//" or "//CUI//") before the beginning of the text. The subject field of a CUI electronically transmitted message must contain the marking "(CUI)" positioning the CUI marking at the end of the Subject field to ensure message recipient(s) identify safeguarding responsibilities.

(2) Transmittal documents that have CUI attachments shall be marked with the following statement or a similar one: "CONTROLLED ATTACHMENT."

(f) Blueprints, engineering drawings, charts, maps, and similar items not contained within another document shall be marked with the CUI designation when applicable. The marking shall be unabbreviated, conspicuous and applied to the top and bottom, if possible, in such a manner as to ensure reproduction on any copies. The legend or title shall also be marked. The parenthetical marking "(CUI)" following the legend or title may be used. If the blueprints, maps and other items are large enough that they are likely to be rolled or folded, additional CUI markings shall be placed to be visible when the item is rolled or folded. Additionally, the following statement shall be imprinted on each page of drawings to include the cover page of construction drawings and on the cover page of the specifications:

PROPERTY OF THE UNITED STATES GOVERNMENT
COPYING, DISSEMINATING, OR DISTRIBUTING THESE DRAWINGS, PLANS OR SPECIFICATIONS TO UNAUTHORIZED USERS IS PROHIBITED

Do not remove this notice
Properly destroy documents when no longer needed

(g) Congressional Security Sensitive (CSS) is a marking sometimes applied, in addition to or in lieu of the marking "Controlled Unclassified Information," by the Capitol Police Board and select Member(s), officer(s), and committee(s) of either the House or Senate. It denotes information that is: (1) sensitive with respect to the policing, protection, physical security, intelligence, counterterrorism actions or emergency preparedness and response relating to Congress, any statutory protector of the Capitol Police and the Capitol buildings and grounds; and (2) is obtained by, on behalf of or concerning the Capitol Police Board, the Capitol Police or any incident command relating to emergency response.

(1) On documents containing CSS information, the phrase "Congressional Security Sensitive" shall accompany the marking CUI at the bottom of the outside front cover (if there is one), the title page (if there is one), and the outside back cover (if there is one).

(i) Each page containing this information shall be marked "Controlled Unclassified Information//Congressional Security Sensitive" or "(CUI-CSS)" at the bottom.
(ii) Access to CSS information shall be granted only to persons who have a valid need to know the information.
(iii) The originator of CSS shall be responsible for ensuring that it qualifies for CSS status and for applying the appropriate marking at the time of origination
(iv) CUI-CSS information shall be safeguarded in the same manner as CUI.

(h) CUI shall be protected from unauthorized access or observation. When not under the direct control of an individual(s) acting within the scope of their contractual relationship with the LOC, independent contractors and vendors conducting business within the scope of their engagement with the LOC and representatives of LOC partners conducting business within the scope of the entity's partnership with the LOC, CUI shall be protected by at least one physical or electronic barrier. This requirement is satisfied by any one of the following:

(1) Locking in a cabinet, drawer, office, office suite, and briefcase or courier bag.
(2) Storing within a password protected or segregated electronic storage device, email account, computer system or network drive.
(3) Storing within a sealed envelope.
(4) When discussing or transferring CUI to another individual(s), ensure that the individual is performing an activity, function, operation or other circumstance authorized by the AOC and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

(i) When CUI is contained in media or material (including hardware and equipment) not commonly thought of as documents (e.g., computer files and other electronic media, audiovisual media, chart, maps, films, sound recordings), the requirement remains to identify, as clearly as possible, the information that requires protection. The main concern is that the material is clearly identified as CUI. The markings required by this Order shall be applied either on the item or the documentation that accompanies it.

(j) When transmitting hard copy CUI, reasonable steps shall be taken to minimize the risk of access by unauthorized persons. Such steps include:

(1) By Mail- Outside of a Facility. CUI material will be placed in a sealed, opaque envelope or wrapping marked with the recipient's address, a return address and the words "TO BE OPENED BY ADDRESSEE ONLY." Any of the following U.S. mail methods may be used:

(i) First Class, Express, Certified or Registered Mail.

(ii) Any commercial carrier (FedEx, UPS, DHL, etc.) may be used.

(2) By Mail- Within a Facility. Use a sealed, opaque envelope with the recipient's address and the words "TO BE OPENED BY ADDRESSEE ONLY" on the front.

(3) By Hand- Between Facilities or Within a Facility. A document marked as containing CUI may be hand carried between or within a facility as long as the person carrying the document can control access to the document.

(4) Transmittal via Fax. Unless otherwise restricted by the originator, CUI information may be sent via non-secure fax. Where a non-secure fax is used, the sender will coordinate with the recipient to ensure that the materials faxed will not be left unattended or subjected to possible unauthorized disclosure on the receiving end. The person(s) receiving the material will comply with any access, dissemination and transmittal restrictions cited by the originator.

(5) Transmittal via E-Mail. CUI transmitted via email should be protected by encryption using AES-256 encryption. To do this, include the CUI in an attachment only (not in the text of the email), and encrypt the attachment with 7 Zip (software program). Recipients of CUI will comply with any email restrictions imposed by the originator. Email CUI within an encrypted attachment with the password provided separately (e.g., by phone, another email, or in person).

(6) AOC Intranet/Internet. CUI will not be posted to intranet sites such as SharePoint collaboration sites, shared drives, multi-access calendars, or on the Internet (including social networking sites) that can be accessed by individuals who do not have an authorized purpose for the information. To control access to an AOC network shared drive and/or SharePoint collaboration site(s) contact the ITD Helpdesk (helpdesk@aoc.gov).

(7) Secure File Transfer Systems. CUI delivered through a secure file transfer system must provide methods (e.g., authentication, file access controls, passwords) to prevent access to CUI stored on the system by persons who do not require the information to perform their jobs or other LOC/AOC-authorized activities.

(k) CUI Destruction Procedures: CUI material will be destroyed when no longer needed.

(1) "Hard Copy" materials will be destroyed by cross-shredding or placed in a secure bin designated for discarding sensitive documentation.

(2) Electronic storage media [e.g., hard disks, floppy disks, zip drives, CDs, thumb drives, pen drives, and similar USB storage devices] shall be sanitized appropriately by overwriting or degaussing.

(3) Paper products containing CUI will not be disposed of in regular trash or recycling receptacles unless the materials have first been destroyed as specified above.

(l) Incident Reporting: The loss, compromise, suspected compromise or unauthorized disclosure of CUI will be reported immediately, but no later than the next duty day, to the Contracting Officer and the AOC Security Officer as shall suspicious or inappropriate requests for information by any means, e.g., email or verbal.

- END Clause –

LC52.212-2 SUPPLEMENTAL LICENSE AGREEMENTS (JUL 2017)

The Library does not agree to licensing agreements or any other provisions that attempt to: (1) replace an order as the governing contract; (2) establish new or supplemental payment terms; or, (3) affect the legal relationships of the parties. Notwithstanding any clauses in this contract or order, or the contractual vehicles against which the order is placed, that establish order of precedence, the rights and obligations provided by this contract or order take precedence over the rights and obligations set forth in any licensing agreements provided to the Library.

The Library's incorporation of a licensing agreement into this contract or order excludes all terms of the licensing agreement that contravene, modify or conflict with the terms of 36 C.F.R. 701.7 available at: https://www.ecfr.gov/cgi-bin/text-idx?SID=87a865ce2bd109313a951a3d477895d8&mc=true&node=se36.3.701_17&rgn=div8.

- END Clause –

LC52.204-3 INFORMATION SYSTEMS SECURITY (SEP 2018)

(1) Computer Security Policy. The Library requires anyone using or accessing its digital assets (including networks, servers, workstations, systems, data, web pages, and email) to protect them and use them only for official business, and only in accordance with Library regulations and applicable Library bargaining agreements. Unauthorized or inappropriate use may be grounds for termination or other contractual remedy.

(2) Privacy Policy. No one has the right to privacy while using any Library computer system, including internet or email services. Usage may be monitored.

(3) Level of Access. The Host Office will determine the level of access to the Library's IT equipment, staff and software needed to successfully perform under this Contract. Access may include, for example, email, word processing, internet, and intranet.

(4) Mandatory IT Security Training. Contractor personnel must successfully complete mandatory information systems security training prior to use of or access to any of the Library's digital assets. The required training is available online at http://www.loc.gov/extranet/cld/. Contractor staff with access to Library digital assets shall complete the information systems security training annually. The training is available on the Library intranet at: http://www.loc.gov/staff/cld/.

-END Clause –

LC52.204-27 HANDLING OF FEDERAL RECORDS (JUL 2021)

(a) Definitions "Records," as defined in 36 C.F.R. § 703.4(a), includes all books, papers, maps, photographs, reports, and other documentary materials, exclusive of materials in the Library's collections, regardless of physical form or characteristics, made or received and under the control of the Library in pursuance of law or in connection with the transaction of public business, and retained, or appropriate for retention, by the Library as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of data contained therein. The term refers only to such items in being and under the control of the Library. It does not include the compiling or procuring of a record, nor does the term include objects or articles, such as furniture, paintings, sculpture, three-dimensional models, structures, vehicles, and equipment. All data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Privacy Act of 1974 (5 U.S.C. 552a), as amended, and Library of Congress regulations at 36 CFR Part 703.

(b) Requirements

1. Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act

(44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, Library of Congress regulations at 36 CFR Part 703 and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.

2. In accordance with 36 CFR 1222.32, Contractor shall manage and schedule records for disposition only as permitted by statute or regulation.

3. The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or which is exempted from public disclosure by 36 C.F.R. 703.5.

4. The Library of Congress shall own the rights to all data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which the Library of Congress shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any Contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.

5. In accordance with 36 CFR 1222.32, Contractor shall maintain and manage all records in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.

6. The Contractor shall only remove records from the legal custody of the Library of Congress or destroy them in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must report the event to the Contracting Officer.

7. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to Library of Congress control unless otherwise directed by the Contracting Officer.

8. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the contract vehicle in accordance with instructions provided by the Contracting Officer. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).

9. The Contractor shall not create or maintain any records containing any non-public Library of Congress information that are not specifically authorized by the contract.

10. All Contractor employees assigned to this contract who create, work with, receive, store, or otherwise handle records shall take Library of Congress-provided records management training. The Contractor shall be responsible for confirming training has been completed.

11. The Contractor shall obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts.

12. The Contractor (and any sub-contractor) shall abide by Government and Library of Congress guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information. The Contractor shall immediately notify the Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment.

(c) Flowdown of requirements to subcontractors

1. The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this contract vehicle, and require written subcontractor acknowledgment of same.

2. Violation by a subcontractor of any provision set forth in this clause will be attributed to the Contractor.

-END Clause –

LC52.239-3A ASSESSMENT AND AUTHORIZATION (ALT I) (JAN 2016)

The information technology identified in this contract will be subject to review and approval of Assessment and Authorization (A&A) prior to connecting the system(s) to the Library of Congress Network.

(a) The contractor shall provide the COR with documentation demonstrating Authorization.

(b) The Library will perform a security assessment, assessment, risk assessment, and security testing & evaluation pursuant to NIST SP 800-37.

(c) The Contractor shall provide Authorization support to the Authorizing Official, including producing copies of the Assessment Package, drafting memorandums and assisting in the briefing of the Designated Approving Authority.

(d) The Contractor shall ensure that the IT system is not connected to the Library of Congress Data Network until accredited.

-END Clause –

-END RFI Relevant Information Technology (IT) Clauses -