Building Physical Security Requirements

For:

Fire, Administrative, and Other Facilities

Major Recreation Sites

Explosive Magazines

USDA Forest Service

Pacific Northwest Region
Alaska Region
Pacific Northwest Research Station

Pacific Northwest Region

Approved By: _____ 15 Jun 17
Regional Forester, Pacific Northwest Region — Date

Recommended By: _____ 06/14/2017
Director of Engineering, Pacific Northwest Region (acting) — Date

Reviewed By: _____ 6/14/2017
Union Representative, Pacific Northwest Region — Date

Alaska Region

Approved By: _____ 5/16/17
Acting
Regional Forester, Alaska Region — Date

Recommended By: _____ 5/16/17
Director of Engineering, Alaska Region — Date

Reviewed By: _____ 5/13/17
Union Representative, Alaska Region — Date

Pacific Northwest Research Station

Approved By: _____ 05/22/2014
Station Director, Pacific Northwest Research Station — Date

Recommended By: _____ 5/12/17
Station Engineer, Pacific Northwest Research Station — Date

Prepared By: _____ 5/1/2017
Pacific Northwest & Alaska Regional Technical Services Lead — Date

Executive Summary

Federal Agencies have been directed by a combination of Presidential, OMB, and National Security mandates to enhance building security. This document synthesizes the information from a range of directives and guidelines, and puts it in a cohesive format so that people who do not work with security on a daily basis can use it to figure out what they need to do. It was written to provide Forest Service engineers and facility managers a resource to help clarify the physical security requirements Forest Service facilities are expected to meet.

This document covers physical security requirements only. There are set standards for operational security, which includes items such as Occupant Emergency Plans, after-hours procedures, managing access within the facility, mail handling, etc. They are not addressed in this document. Those items fall under the operation of the facility and should be handled accordingly.

Determining the Facility Security Level (FSL) is the first step in determining the measures that are required to protect a building. The FSL is comprised of five equally weighted security evaluation factors: Mission Criticality, Symbolism, Facility Population, Facility Size, and Threat to Tenant Agencies. A sixth factor – Intangibles – allows the assessor to consider other factors unique to the facility needs. Nearly all Forest Service facilities will rank out as either Level I or Level II, with only a handful of facilities ranking out higher.

A wide range of undesirable events has been assessed by the Interagency Security Committee to determine their potential likelihood and the countermeasures needed to mitigate the risk. The mitigation measures presented in this document cover the likely undesirable events that may affect Forest Service facilities within Regions 6 and 10 and the Pacific Northwest Research Station.

New construction is expected to meet the level of protection required by its Facility Security Level. In some cases, site limitations may restrict standoff distances, or some measures may be too cost prohibitive. However, the required security measures should be identified as early in the process as possible, so that they can be incorporated into the project up front without the need for exceptions.

Leased facilities are also expected to meet these requirements. If, during the leasing process, it is determined that available facilities cannot meet minimum requirements, then the lease acquisition should be reconsidered. If there are no other options, the highest level of protection that is achievable should be implemented and documented.

For existing facilities, once the FSL is known, this document can be used to determine if a facility's existing Level of Protection matches up with its required Level of Protection. If the existing does not match up with the required, then either a plan can be developed to improve the existing Level of Protection or the Designated Line Officer, which is the Forest Supervisor, can approve a variance to the required Level of Protection.

All facilities will require a physical assessment. An assessment should be done once every 5 years for Level I and II buildings, and once every 3 years for Level III buildings. Any facility can be reviewed at any time, if the situation changes and conditions warrant it.

The Union has not waived its bargaining rights pertaining to the policy. Recognizing that the circumstances under which this policy is applied will vary from one instance to the next and from one location to the next, any bargaining obligations implicated by the policy should be addressed at the time they arise, normally through the Agency's notification of the Union through Article 8 or Article 11 procedures, or both.

Table of Contents

Introduction

Federal Agencies have been directed by a combination of Presidential, OMB, and National Security mandates to enhance building security. Some of the guidelines apply to all Forest Service facilities, and some apply to certain types of facilities. Because so many documents cover security, it can become confusing as to what should actually be followed.

As a result, the Building Physical Security Requirements was written to provide Forest Service engineers and facility managers a resource to help clarify the physical security requirements Forest Service facilities are expected to meet. This document condenses the physical security standards into a single location and describes the required standards so that people who do not work with security on a daily basis can use it to figure out what they need to do.

It defines the process used to determine the level of security a facility needs, and it provides the countermeasures the facility should meet based on its Security Level. It also provides guidance for how to deal with variances. This process applies to both proposed and existing facilities.

New construction, with few exceptions, is expected to fully meet the level of protection required by its Facility Security Level (FSL). In some cases, site limitations may restrict standoff distances, or some measures may be too cost prohibitive. However, the required security measures should be identified as early in the process as possible, so that they can be incorporated into the project up front without the need for exceptions.

Leased facilities are also expected to meet these requirements. The initial FSL determination for newly leased space shall be made as soon as practical after the identification of a space requirement, including succeeding leases. The determination should be made early enough in the space acquisition process to allow for the implementation of required countermeasures, or reconsideration of the acquisition caused by an inability to meet minimum physical security requirements.

For existing facilities, once the FSL is known, the document can be used to determine if a facility's existing Level of Protection matches up with its required Level of Protection. If the existing does not match up with the required, then either a plan can be developed to improve the existing Level of Protection or the Designated Line Officer, which is the Forest Supervisor, can approve a variance to the required Level of Protection. Any time a facility undergoes a major renovation, these security standards should be reviewed and mitigating any deficiencies should be incorporated into the project.

Security activities tend to fall into one of two categories: physical or operational. Physical security is tied to the site itself: its landscaping, the locks, doors, windows, and the electronic systems used to keep the facility and its occupants safe. Operational security covers how people operate; it involves such things as key management, mail handling, after hours procedures, emergency plans, etc.

This document covers physical security requirements only. There are set standards for operational security; however, they are not addressed in this document. Those items fall under the management of the facility and should be handled accordingly.

The Union has not waived its bargaining rights pertaining to the policy. Recognizing that the circumstances under which this policy is applied will vary, any bargaining obligations implicated by the policy should be addressed at the time they arise, normally through the Agency's notification of the Union through Article 8 or Article 11 procedures, or both.

Background and Directives

The day after the April 19, 1995, bombing of the Alfred P. Murrah Federal Building in Oklahoma City, the President directed the Department of Justice (DOJ) and U.S. Marshal's Service to conduct a vulnerability assessment of federal facilities, with an emphasis on acts of terrorism and other forms of violence. The President directed the Department of Justice to assess federal office building vulnerability because of its expertise in court security. Prior to the completion of this assessment and the issuance of the DOJ Vulnerability Assessment of Federal Facilities Report on June 28, 1995, there were no government-wide minimum standards for security at federal facilities.

Using Executive Order 12977, October 19, 1995, the President established the Interagency Security Committee (ISC). This multi-Department group developed the ISC "Security Design Criteria" to ensure that security becomes an integral part of the planning, design, and construction of new federal buildings, modernization projects, and lease agreements. The criteria consider security in all building systems and elements for every type of building occupied by Federal employees.

The ISC's 2016 *The Risk Management Process for Federal Facilities* directs the user to a set of standards that applies to all Government facilities whether they were owned or leased. These documents define the process to be used in determining the Facility Security Level of a building, and its Level of Protection, which serves as the basis for implementing protective measures.

There are two companion documents – *Appendix A: Design-Basis Threat Report* and *Appendix B: Countermeasures.* The *Design-Basis Threat Report* goes through every possible action that the ISC can conceive of occurring at a federal facility and its potential of happening. The *Countermeasures* document details the mitigating actions that should be in place to prevent the design threats. Both documents are available on a need to know basis. Government users may request access by sending an email to ISCAccess@hq.DHS.gov with your full name, email address, the name of your agency, and the reason you need access.

Several of the countermeasures are based on technical documents created by other agencies. In addition, USDA has a set of security standards, and the Forest Service has some guidance on security measures. Many of those resources are cited throughout this document if further information on a topic is desired.

Because Forest Service facilities tend to have many of the same characteristics and threat potentials, this document standardizes the design requirements. If a site has a different threat level in one category than what it typically expected, then countermeasures can be modified to meet that threat level for that site. It should be understood that there are no guarantees that even the best countermeasures and procedures will fully protect our facilities from potential threats. However, experts in the physical security field recommend implementing these measures in order to protect our workforce, our visitors, and our facilities.

Facility Security Levels (FSL)

Determining the Facility Security Level is the first step in determining the measures that are required to protect a building. This section describes each of those requirements so that personnel with responsibilities for security-related programs, projects, and/or operations are able to determine the FSL for a Federal facility.

The FSL determination ranges from a Level I (lowest risk) to Level V (highest risk). Nearly all Forest Service facilities will rank out as either Level I or Level II, with only a handful of facilities ranking out higher. Risk assessments will be conducted at least once every 5 years for Level I and II facilities, and at least once every three years for Level III facilities and above. The FSL will be reviewed and adjusted, if necessary, as part of each initial and recurring risk assessment.

In establishing the FSL, it is important to consider factors that make the facility a target for adversarial acts (threats) as well as those that characterize the value or criticality of the facility (consequences). In 2007, Homeland Security Presidential Directive 20 (HSPD-20) identified 8 National Essential Functions, which are fundamental activities the Federal Government should be able to carry out at any point, including during a major disaster. The continuity of these fundamental activities, as well as primary mission essential functions are part of determining the "value" of a facility to the government.

In addition, the threat to facilities from criminal elements must also be evaluated in determining the FSL. Consideration must be given to the risk from such acts as theft, assault, unlawful demonstrations, workplace violence, and vandalism – acts that historically occur more frequently at Federal facilities than acts of terrorism.

FSL Matrix

The FSL matrix is comprised of five equally weighted security evaluation factors with corresponding points of 1, 2, 3, or 4 allocated for each factor. The following sections provide criteria to be used in evaluating each factor and assigning points. However, the factors cannot capture all of the circumstances that could be encountered. Thus, a sixth factor – intangibles – allows the assessor to consider other factors unique to the facility needs.

To use the FSL matrix, each of the factors is examined and a point value assigned based on the provided scoring criteria. The points for all factors are then added together and a preliminary FSL is identified, based on the sum. The assessor may then consider any intangibles that might be associated with the facility. The FSL may be adjusted by either a one-level increase or a one-level decrease after considering intangibles. An adjustment to the FSL may be made (and documented) accordingly, and a final FSL determined.

Factor	Points				Score
	1	2	3	4	
Mission Criticality	LOW	MEDIUM	HIGH	VERY HIGH	
Symbolism	LOW	MEDIUM	HIGH	VERY HIGH	
Facility Population	≤ 100	101–250	251–750	> 750	
Facility Size	≤ 10,000 sq. ft.	10,001–100,000 sq. ft.	100,001–250,000 sq. ft.	> 250,000 sq. ft.	
Threat to Tenant Agencies	LOW	MEDIUM	HIGH	VERY HIGH	
					Sum of above
Facility Security Level	I: 5–7 Points	II: 8–12 Points	III: 13–17 Points	IV: 18–20 Points	**Preliminary FSL**
Intangible Adjustment	Justification				**+ / - 1 FSL**
					Final FSL

Interagency Security Committee Facility Security Level Determination Matrix

FSL Scoring Criteria Definitions

Further definition of the factors and examples of the values associated with the factors is given below.

Mission Criticality

The value of a facility is largely based on its mission. The more important a facility is to the mission of the Agency, the more attractive it is to adversaries to disrupt the mission. The Mission Criticality score is based on how critical the missions carried out by the tenants in the facility are (not by the tenant agencies overall). In a multi-tenant facility, the highest rating of any tenant should be used for this factor.

> ***Very High****:* Houses personnel or specialized equipment necessary to identify or respond to large-scale or unique incidents such as Emergency Operations Centers and National Fire Caches
> ***High****:* Designated as a shelter in the event of an emergency incident; Regional Offices; Biological/chemical research or storage of research and development quantities of

chemicals, biohazards, explosives, and similar items.
Medium*:* Forest Headquarters or Supervisor's Offices, District Offices
Low: Work Centers

Symbolism

The symbolism of a facility is based on both its attractiveness as a target and the consequences of an event. The symbolic value is based on both its external appearance and its well-known operations inside the facility. Transnational terrorists often seek to strike at symbols of the United States. Domestic extremist groups or individuals may seek to make a statement against government control, taxation, policies, or regulation.

A facility with a large amount of land/acreage associated with it may be perceived as large and/or of high importance regardless of the size and number of buildings housed there. This potentially increases the facility's symbolic value. If the land associated with the facility significantly contributes to target attractiveness, document the rationale and add one point, not to exceed the maximum of 4 points, to the symbolism score.

1. ***Very High****:* A nationally significant historical event has occurred at the facility or the facility has a very high tourist load such as Multnomah Falls Interpretive Center.
2. ***High:*** *P*opular tourist destinations such as Cape Perpetua Visitor Center; houses large numbers of personnel required to wear uniforms and/or perceived to be well protected, such as the Willamette SO.
3. ***Medium:*** Dominant, single Federal facility in a community or rural area. Readily identifiable as a U.S. Government facility either through external features, nature of public contact, or other operations. Readily identifiable, non-facility assets (such as Fleet vehicles) located at site.
4. ***Low:*** No external features or public contact readily identifying it as a U.S. Government facility.

Facility Population

The Facility Population factor is based on the peak total number of personnel in government space, including employees, onsite contract employees, and visitors. The number should not include occasional transient peaks, such as public meetings, unless it is part of normal business, and the facility is intended for that type of use.

For instance, the Facility Population for a Dispatch Center should cover the amount of people it will house during fire activity, and not just the number it has during normal operations.

If there is a childcare center on-site, it automatically receives a "Very High" ranking with a point value of 4.

Facility Size

The facility size factor is based on the square footage of all federally occupied space in the facility. If the entire facility is occupied, gross square footage should be used. If only a portion of the facility is occupied, then the assignable square footage should be used.

Threat to Tenant Agencies

This factor should be viewed in terms of whether the nature of public contact is adversarial, or if there is a history of adversarial acts committed at the facility. Crime statistics and past or current credible threats to all tenants in a facility – including non-federal tenants – should be considered and the highest score used for the rating.

1. ***Very High:*** Tenant mission is controversial and routinely draws attention of organized protest groups; it is located in a high-crime area, or more than 10 incidents/year requiring law enforcement/security response for unruly or threatening persons onsite.
2. ***High:*** Public contact is occasionally adversarial; there is a history of demonstrations, or 5-10 incidents per year requiring law enforcement/security response for unruly or threatening persons onsite.
3. ***Medium:*** Generally non-adversarial public contact, located in a low-crime area, or history of demonstrations or violence directed against the Agency (not the specific facility).
4. ***Low:*** Generally, little to no public contact, no history of demonstrations at the facility, or no history of violence directed at the facility or its occupants.

Intangible Factors

The Forest Supervisor may raise or lower the FSL by one level, based on intangible factors. However, the intangible factor should not be used to raise or lower the FSL in response to a particular threat. The FSL characterizes the entire building – concerns about specific threats should be addressed with specific countermeasures, even if they are over and above those required as the baseline for a particular security level.

Short-term events could also temporarily affect the factors evaluated here. Unless these events happen on a recurring basis, they should not affect the FSL determination. Instead, contingency plans should be developed to implement temporary measures until the event has passed.

It is important to document these intangible factors and the resulting adjustments made to the FSL score. The Forest Supervisor should document any intangible factors and the associated adjustment, and retain this information as part of the official security records for that site.

Finally, the FSL intangible adjustment is not to be used for the purposes of reducing the baseline and necessary security criteria. If a facility cannot meet the baseline level of protection, risk acceptance may be necessary.

Level of Protection (LOP)

Each FSL corresponds to a level of risk that then relates directly to an LOP and associated set of baseline security measures. In general, the baseline LOP will correspond to the FSL as shown in the table below:

Facility Security Level	Level of Risk	Baseline Level of Protection
IV	High	High
III	Medium	Medium
II	Low	Low
I	Minimum	Minimum

A wide range of undesirable events has been assessed to determine their potential likelihood and the countermeasures needed to mitigate the risk. The mitigation measures presented in this document cover the likely undesirable events that may affect Forest Service facilities within Regions 6 and 10 and the Pacific Northwest Research Station.

There may be instances where the baseline risk for an undesirable event may be higher than the baseline LOP. In those cases, a physical security specialist or Agency Law Enforcement must identify the appropriate countermeasures that will provide an LOP equivalent to the risk.

Once the LOP is identified, an evaluation of current conditions at a site should be completed to identify existing countermeasures. If the existing countermeasures match up to the LOP, then they should be maintained. If they do not match up, the shortfalls should be identified and plans to address the vulnerabilities should be developed.

Variances

There may be instances in which the physical limitations of a site may make achieving the appropriate LOP impossible. There may also be instances where it is impractical to meet the LOP due to its cost. For leased facilities, it may be determined that available facilities in the delineated area cannot meet the LOP, or that the terms of an existing lease might not allow the implementation of certain countermeasures.

If that is the case, then the highest achievable LOP must be identified and implemented. The additional amount of risk must be assessed and documented.

The physical security documentation for the site must clearly reflect the reason why the necessary Level of Protection cannot be achieved. The documentation should include the rationale for accepting the risk, the alternate strategies considered or implemented, and opportunities in the future to implement the necessary LOP. Variances must be approved by the Forest Supervisor.

Historic Buildings

Historic buildings are addressed in the same manner as other existing buildings. Compliance with Section 106 of the National Historic Preservation Act must be coordinated with the State Historic Preservation Office consistent with established Agency procedures. Design alternatives for incorporating the necessary security measures into the historic property should be fully explored to balance historic preservation goals and security requirements.

Security Review Occurrence

All facilities should be reviewed on a recurring basis. All Level I's and II's shall be reviewed every 5 years, and Level III's every 3 years. Any facility can be reviewed at any time, if the situation changes and conditions warrant it.

Site Security Criteria

Each facility is required to meet certain countermeasures based on its FSL. As could be expected, countermeasures become more detailed as the Security Level increases. The information below gives a general description of specific countermeasures for each Security Level required by the ISC.[1]

These are the baseline countermeasures for each level that are required to be met. These measures, as well as some additional countermeasures, are described in detail in the "Building Design Criteria and Security Definitions" section. Each countermeasure described in that section states for which FSL that countermeasure should be applied.

Level I – Minimum Level of Protection

Site Security Criteria

1. Vehicle Access:
    a. Limit the number of vehicle access points.
    b. Designate employee and visitor parking areas.
    c. Design site entrance and circulation controls to prevent high-speed approaches to buildings by vehicles.
    d. Use vehicle gates to limit access to government vehicle parking. Locate Government owned vehicles in well-lit areas of fenced surface lots.
1. Landscaping: Minimize areas of concealment in and around parking areas and facilities. Apply Crime Prevention through Environmental Design (CPTED) principles to the site.
2. Site Lighting: Install exterior lighting at entrances and exits. See the *Lighting* section in the "Design Criteria and Security Features" section for more details.

Structure Security Criteria

1. Air Intakes: Fresh air intakes shall be located to prevent easy ground or roof access. Provide emergency shutdown, shelter-in-place, and evacuation procedures.
2. Emergency Generator Protection: If an emergency generator is used, secure against unauthorized access and locate the emergency generator and fuel tank at least 25' away from loading docks, entrances, and parking areas.

Facility Entrance Security

1. Access Control: Keys are an acceptable access control system for Level I facilities.
2. Visitor Access Control: 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 facility.
3. Perimeter Doors and Door Locks: Secure doors with non-removable hinges and high-security mechanical locks. Forest Service Yale locks cannot be used for facility access. See *Perimeter*

[1] ISC– The Risk Management Process Appendix B: Countermeasures. September 2016 (For Official Use Only)

Doors and *Access Control Systems* in the "Building Design Criteria and Security Features" section for details.

4. Emergency Exit Doors: Emergency exit doors shall be secured using an automatic door closer and exit hardware that is compliant with the applicable life safety codes and standards.

Interior Security Criteria

1. Public Access: Use signage to designate non-public areas and establish procedures to prevent unauthorized access.
2. Security of Critical Areas: Secure utility, mechanical, electrical, and telecom rooms with locks and establish procedures to limit access to authorized personnel only. Secure access to interior space from the roof with locks.
3. Public Accessible Restrooms: Control access to public restrooms.

Security Systems Criteria

1. Provide an emergency phone connection via POTs (Plain Old Telephone, or analog) line or VoIP (Voice over Internet Protocol) if main phone system is disabled.
2. Intrusion Detection System (IDS) Monitoring: If an IDS is utilized, monitor at a central station with notification to a building manager or designated Point of Contact. See *Intrusion Detection Systems* in the "Building Design Criteria and Security Features" section.
3. Duress Alarms: Implement duress procedures for emergency situations. If a duress alarm is installed, it shall have an internal bell system and external dial out capability. See *Duress Alarms* in the "Building Design Criteria and Security Features" section.

Cyber Security Criteria

1. Building Automation and Control Systems (BACS): If a BACS is in use, there needs to be documentation kept on site describing its components and their function. Ensure that the Forest Service network cannot be accessed from the BACS. Disable guest/anonymous accounts. Secure physical access to devices and cabling, and actively manage remote and/or wireless access into the BACS. See *BACS* in "Design Criteria and Security Features" section for details.
2. BACS Infrastructure: Ensure systems are up to date and maintained. Ensure that disposal of devices does not release sensitive data. Create and test incident response plans.
3. If external access to BACS is required (through a DSL internet connection), coordinate with CIO to secure access to the system.

Level II – Low Level of Protection

Site Security Criteria

1. Vehicle Access:
    e. Limit the number of vehicle access points.
    f. Designate employee and visitor parking areas.
    g. Design site entrance and circulation controls to prevent high-speed approaches to buildings by vehicles.
    h. Use vehicle gates to limit access to government vehicle parking. Locate Government owned vehicles in well-lit areas of fenced surface lots or in segregated levels of parking lots.
2. Landscaping: Minimize areas of concealment around parking areas and facilities. Establish a clear zone and restrict landscaping from obstructing views of the VSS cameras or interfering with the lighting or intrusion detection system. Apply Crime Prevention through Environmental Design (CPTED) principles to the site.
3. Site Lighting: Install exterior lighting at entrances, exits, parking lots, ware yard areas and VSS locations. See the *Lighting* section in the "Design Criteria and Security Features" section for more details.
4. Restricted Areas: Use trees, hedges, berms, or any combination of these elements to create buffer zones to separate public areas and other functions.
5. Storage, Receptacle, and Container Placement: Locate Hazardous Material lockers in a restricted area away from loading docks, entrances, and uncontrolled parking. Position trash containers, mailboxes, donation/recycle containers, vending machines or other features that could conceal devices away from building exterior or entry points.

Structure Security Criteria

1. Blast Resistance – Façade and Structure: Use construction materials that have inherent ductility (can bend, flex or move, and fails only after considerable deformation occurs) and which are able to respond to load reversals (rebound and/or uplift forces). Design and locate building docks to minimize the effects of blast on building structure and to vent explosive forces and gases.
2. Windows:
    a. Utilize acceptable shatter resistant film meeting performance condition "3b" or an acceptable glazing system to reduce glass fragmentation hazards.
    b. Provide blinds, curtains, or other window treatments that can be used to prevent visual observation into the facility.
    c. Monitor all operable ground floor windows with an Intrusion Detection System (IDS)
3. Air Intakes: Locate fresh air intakes to prevent easy ground or roof access and secure grilles from tampering or removal. Provide emergency shutdown, stay in place, and evacuation procedures.
4. HVAC Controls: Protect HVAC controls from unauthorized access.
5. Emergency Generator Protection: If an emergency generator is used, secure against unauthorized access and locate the emergency generator and fuel tank at least 25 feet away from loading docks, entrances, and parking areas.

Facility Entrance Security Criteria

1. Access Control: Limit the number of building entry points to the fewest number practical. Access control may be provided through either an ePACS (electronic Physical Access Control System) or mechanical locking system. If there is an existing proximity card system in place, it may remain in place. If there is a need to replace the system, it shall be replaced with a Linc Pass compatible system that can be integrated into the USDA security system. See *Access Control Systems* in the "Building Design Criteria and Security Features" section for details.
2. Employee Access Control: Provide a means to secure employee entrance doors and to verify the identity of persons requesting access prior to allowing entry in the facility by either physical or electronic means.
3. Visitor Access Control: Design public areas in such a manner that visitors must either be approved for unescorted access to non-public areas or be escorted at all times.
4. Perimeter Doors and Door Locks: Secure doors with non-removable hinges and high-security mechanical or electronic locks. Forest Service Yale locks shall not be used for facility access. See *Perimeter Doors* and *Access Control Systems* in the "Building Design Criteria and Security Features" section for details.
5. Control of Keys and Access Media: Implement a formal key control program. If an ePACS is in place, ensure it has the ability to electronically disable lost or stolen access media.
6. Emergency Exit Doors: Emergency exit doors shall be secured using an automatic door closer and exit hardware that is compliant with the applicable life safety codes and standards. Provide VSS coverage.

Interior Security Criteria

1. Public Access: Accommodate publicly accessible retail and mixed uses through such means as separating entryways. Use signage to designate non-public areas and establish procedures to prevent unauthorized access.
2. Security of Critical Areas: Secure utility, mechanical, electrical, and telecom rooms, with high-security locks. Establish procedures to limit access to authorized personnel only. Prevent access to interior space from the roof.
3. Publicly Accessible Restrooms: Control access to public restrooms.
4. Interior Public Spaces: Use construction materials that have inherent ductility (can bend, flex or move, and fails only after considerable deformation occurs) and which are able to respond to load reversals (rebound and/or uplift forces).
5. Mail Rooms: Use construction materials in the mail screening and receiving areas that have inherent ductility (can bend, flex or move, and fails only after considerable deformation occurs) and which are able to respond to load reversals (rebound and/or uplift forces).

Security Systems Criteria

1. Video Surveillance System (VSS) Coverage: Provide VSS coverage of locations where money transactions take place and at personnel entrances and exits. Record VSS views using a digital medium. Post signage at the entrance of the location where coverage exists.
2. Intrusion Detection Systems (IDS): Provide IDS on perimeter entry and exit doors, and operable ground floor windows. Monitor at a central station with notification to a building manager or designated Point of Contact.
3. Emergency Communications: Provide an emergency phone connection via POTs (Plain Old Telephone, or analog) line or VoIP (Voice over IP) if main phone system is disabled.

4. Duress Alarms: Provide duress buttons in reception areas and at every location that handles cash transactions. Provide an audible bell at a monitored location in building and interconnection to a central station monitor with notification to a building manager or designated Point of Contact.
5. Security Systems General Operation: Provide uninterruptible emergency power to essential electronic security systems for a minimum of 1 hour of battery backup. Some security items require more than 1-hour back up and have internal batteries. See Electronic Infrastructure Protection in "Building Design Criteria and Security Features" below. Conduct security system performance testing annually. Implement a preventive maintenance program for all security systems. Any critical component that becomes inoperable must be replaced or repaired within 5 business days.

Cyber Security Criteria

1. Building Automation and Control Systems (BACS): If a BACS is in use, there needs to be documentation kept on site describing its components and their function. Ensure that the Forest Service network cannot be accessed from the BACS. Disable guest/anonymous accounts. Secure physical access to devices and cabling, and actively manage remote and/or wireless access into the BACS. See *BACS* in "Design Criteria and Security Features" section for details.
2. BACS Infrastructure: Ensure systems are up to date and maintained. Ensure that disposal of devices does not release sensitive data. Create and test incident response plans.
3. If external access to BACS through a DSL internet connection is required, coordinate with CIO to secure access to the system.

Level III – Medium

Site Security Criteria

1. Vehicle Access:
   a. Separate employee, visitor, and Government vehicle parking.
   b. Limit the number of vehicle access points.
   c. Design site entrance and circulation controls to prevent high-speed approaches to buildings by vehicles.
2. Controlled parking areas:
   a. Limit parking to employee vehicles, authorized visitor vehicles, and government vehicles.
   b. Use gates to limit access to authorized vehicle parking and other restricted areas. Locate Government owned vehicles in well-lit areas of fenced surface lots or in segregated levels of parking lots.
   c. Screen visitor vehicles before entry into the controlled parking area.
   d. If the site has underground or in-building parking, control vehicle access to the parking area.
3. Pedestrian entrances: Provide vehicle barriers to protect pedestrian entrances from penetration by a vehicle. Monitor pedestrian access to parking areas utilizing guard force or VSS.
4. Landscaping: Minimize areas of concealment around parking areas and facilities. Establish a clear zone and restrict landscaping from obstructing views of the VSS cameras or interfering with the lighting or intrusion detection system. Apply CPTED principles to the site.
5. Site Lighting: Install exterior lighting at entrances, exits, parking lots, walkways from parking areas to entrances, VSS locations and ware yard areas. See the *Lighting* section in the "Design Criteria and Security Features" section for more details.
6. Restricted Areas: Provide fences, walls, gates, or other barriers to prevent unauthorized access to restricted areas and monitor with VSS or guard patrols. Use access control and IDS.
7. Storage, Receptacle, and Container Placement: Locate Hazardous Material lockers in a restricted area away from loading docks, entrances, and uncontrolled parking. Position trash containers, mailboxes, donation/recycle containers, vending machines, or other features that could conceal devices away from building exterior and entry points. Monitor storage area utilizing guard force or VSS. Control access to areas.

Structure Security Criteria

1. Blast Resistance: Use a combination of setback, site planning, façade hardening, and structural measures to provide a medium level of façade protection. For buildings 4 stories or taller, use a combination of the above to prevent progressive collapse or the loss of any single exterior column or load bearing wall. Design and locate building docks to minimize the effects of blast on building structure and to vent explosive forces and gases.
2. Blast Resistance Materials; Use construction materials which have inherent ductility (can bend, flex or move, and fails only after considerable deformation occurs) and which are able to respond to load reversals (rebound and/or uplift forces).
3. Blast Resistance – Under Building Parking: Implement architectural or structural features that deny contact with exposed primary vertical load members.

4. Windows:
    a. Utilize acceptable shatter resistant film meeting performance condition "3b" or an acceptable glazing system to reduce glass fragmentation hazards.
    b. Provide blinds, curtains, or other window treatments that can be used to prevent visual observation into the facility.
    c. Operable windows are not allowed on the ground floor. Monitor ground floor windows with IDS.
5. Air Intakes: Locate fresh air intakes to prevent easy ground or roof access and secure grilles from tampering or removal. Provide emergency shutdown, stay in place and evacuation procedures, and protect accessible air intakes with fencing. Monitor with VSS or guard patrols.
6. HVAC systems: Provide separate isolated HVAC systems in reception areas, loading docks, mailrooms and other locations susceptible to a Chemical/Biological/Radiological (CBR) attack.
7. HVAC Control: Protect the system controls from unauthorized access. Install an emergency shut-off and exhaust system for air handlers. Control movement of elevators and close applicable doors and dampers to seal building.
8. Biological Filtration: Use a Minimum Efficiency Reporting Value (MERV) 10 particulate filter on all exterior air-handling units. Use a MERV 13 particulate filter on all air-handling units in reception areas and mailrooms.
9. Protection of Water Supply: Secure handles, control mechanisms, and service connections at on-site publicly accessible locations with locks or other anti-tamper devices.
10. Emergency Generator: If an emergency generator is used, secure against unauthorized access. Locate the emergency generator and fuel tank at least 25' away from loading docks, entrances, and parking. Generators must be protected from physical access by fences, gates, walls, or other means.

Facility Entrance Security Criteria

1. Access Control: Limit the number of building entry points to the fewest number practical. Access control shall be provided through an ePACS. If there is an existing proximity card system in place, it may remain in place. If there is a need to replace the system, it shall be replaced with a Linc Pass compatible system that can be integrated into the USDA security system. See *Access Control Systems* in the "Building Design Criteria and Security Features" section for details.
2. Employee Access Control: Provide an electronic access control for employee entrance doors without a guard post in conjunction with VSS coverage.
3. Visitor Access Control: Design public areas in such a manner that visitors must either be approved for unescorted access to non-public areas or escorted at all times.
4. Occupant Screening: Provide an X-ray and metal detector area for screening all occupants – and their property – that do not possess an acceptable ID for access to the facility. Design the system to minimize queuing caused by screening, visitor processing, and access control system throughput.
5. Mail/Package Handling and other Deliveries: Provide an X-ray screening area for all mail and packages at either a loading dock or an existing screening location if there is no loading dock.
6. Perimeter Doors and Door Locks: Secure doors with non-removable hinges and high-security mechanical or electronic locks. Forest Service Yale locks shall not be used for facility access. Emergency exit doors shall be secured using an automatic door closer and exit hardware that

is compliant with the applicable life safety codes and standards. Provide VSS coverage. See *Perimeter Doors, Access Control Systems*, and *Video Surveillance Systems* in the "Building Design Criteria and Security Features" section for details.

7. Control of Keys and Access Media: Implement a formal key control program and ensure it has the ability to electronically disable lost or stolen access media.

Interior Security Criteria

1. Space Planning: Locate critical systems and areas at least 25' away from loading docks, entrances, mailrooms, personnel and package screening locations, and uncontrolled parking areas.
2. Blast Resistance: Implement architectural or structural features, or other countermeasures that deny contact with exposed primary vertical load members.
3. Public Access: Accommodate publically accessible retail and mixed uses through such means as separating entryways. Use signage, stanchions, counters, furniture, knee walls, etc., to establish physical boundaries to control access to non-public areas.
4. Restrooms: Place restrooms so that occupants and visitors will be screened prior to gaining access.
5. Security of Critical Areas: Secure utility, mechanical, electrical, and telecom rooms with electronic access control and IDS to control and monitor access. Prevent access to interior space from the roof using locks and IDS.

Security Systems Criteria

1. VSS Coverage: Provide Color HDMI VSS coverage of locations where money transactions take place, screening checkpoints, personnel and vehicle entrances and exits, reception areas, restricted areas, air intakes, loading docks, and storage, receptacle and container areas. Record VSS views using a digital medium. Post signage of VSS surveillance when required.
2. IDS: Provide IDS on perimeter entry and exit doors, and all ground floor windows. Monitor at a central station with notification to law enforcement or security responders.
3. Duress Alarms: Provide duress buttons in reception areas and at every location that handles cash transactions. Provide an audible bell at a monitored location in building and interconnection to a central station monitor with notification to a building manager or designated Point of Contact.
4. Provide an emergency phone connection via POTs (Plain Old Telephone, or analog) line or VoIP (Voice over Internet Protocol) if main phone system is disabled.
5. Building Communication System: Provide a communication system for security and emergency announcements.
6. Security Systems General Operation: Provide uninterruptible emergency power to essential electronic security systems for a minimum of 1 hour. Some security items require more than 1 hour backup and have internal batteries. See Electronic Infrastructure Protection in the "Building Design Criteria and Security Features" section below for details. Conduct security system performance testing annually. Implement a preventive maintenance program for all security systems. Any critical component that becomes inoperable must be replaced or repaired within 72 hours.

Cyber Security Criteria

1. BACS: If a BACS is in use, there needs to be documentation kept on site describing its components and their function.

2. BACS Access: Ensure that the Forest Service network cannot be accessed from the BACS. Deny access by default/allow access by exception when there is a need. Ensure unique identifications and passwords for all individuals with a need to access the system. Secure physical access to devices and cabling, and actively manage remote and/or wireless access into the BACS. See *BACS* in "Design Criteria and Security Features" section for details.

3. BACS Infrastructure: Ensure systems are up to date and maintained. Ensure that disposal of devices does not release sensitive data. Backup critical data to alternate site and ensure that it is encrypted. Create and test incident response plans.

4. If external access to BACS through a DSL internet connection is required, coordinate with CIO to secure access to the system.

Level IV – High

Regions 6 and 10, and the Pacific Northwest Research Station do not currently own any Level IV facilities (however, the Edith Green – Wendall Wyatt, which houses the Region 6 Regional Office and the Research Station Director's Office, and the Hurff Ackerman Saunders Federal Buildings, which houses Region 10 Regional Office, are Level IV facilities). If the security level of any facilities changes to where it would rank as a Level IV, it will be handled as a special case.

Building Design Criteria and Security Features

The following information provides further detail regarding the requirements listed above. In some instances, the information will apply to all Facility Security Levels. In others, it will only apply to certain security levels. The requirements and the level they pertain to are listed in the Table below, with each requirement described in more detail in the following sections.

Requirement	Level I	Level II	Level III
Site Security Criteria			
Signage	X	X	X
Setback, Vehicle Access to Site	X	X	X
Controlled Parking Areas			X
Clear Zones		X	X
Landscape Design	X	X	X
Restricted Areas		X	X
Storage, Receptacle, and Container Placement	X	X	X
Bollards and Barriers		X	X
Fencing		X	X
Site Lighting			
Entrances and Exits	X	X	X
Parking Lots, Ware yards, and VSS Locations		X	X
Pedestrian Walkways			X
Utility Protection		X	X
Propane Tanks	X	X	X
Structure Security Criteria			
Building Blast Resistance		X	X
Windows – Blast Resistance		X	X
Air Intake and Ventilation System Protection	X	X	X
Emergency Generator Protection	X	X	X
Facility Entrance Security Criteria			
Facility Entrance Considerations	X	X	X
Doors	X	X	X
Access Control	X	X	X
Interior Security Criteria			
Non-Public and Critical Areas	X	X	X
Security Systems Criteria			
Video Surveillance System (VSS) Monitoring		X	X
Locations where money transactions take place		X	X
Personnel entrances and exits		X	X
Reception Areas			X
Vehicle entry/exit points, Restricted Areas			X
Loading docks, Air Intakes, Receptacle Areas			X
Burglar/intrusion alarm systems (IDS)		X	X
Duress Alarm	X	X	X
Public Address System		X	X
Emergency telephone – VoIP or POTS backups	X	X	X
Electronic Infrastructure Protection			
UPS emergency backup power		X	X
Backup Generator		As needed	As needed
Cyber Security Criteria			
Building Automation and Control Systems (BACS)	X	X	X

Site Security Criteria

Signage

The following signage requirements apply to all security levels.

Where the interaction with visitors is customer-service oriented and signage improves the ability of customers to locate the facility, use distinctive external signage. Otherwise, keep external signage identifying the facility to a minimum[2].

When Agencies are co-located, only post signage identifying the 'customer service' agencies.

Avoid marking outside locations such as air intakes, fuel supply valves, gas or power distribution locations, evacuation assembly areas, etc. Appropriately sign hazards, but orient signs so they are not normally in the view of visitors, when possible.

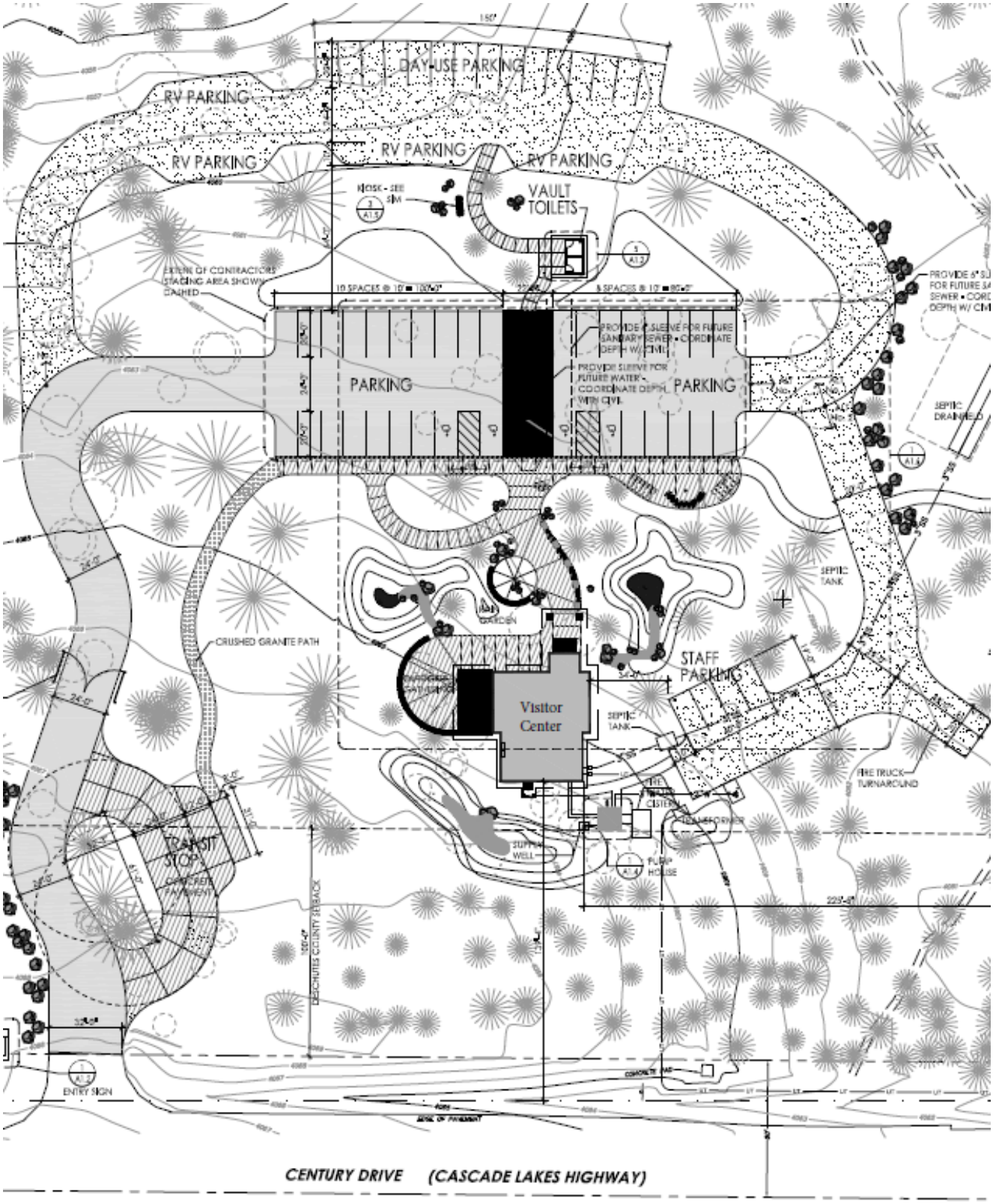
Setback

Setback refers to the distance from the subject building to the curb (access road), other buildings on site, property of other ownership or other boundaries. These setback requirements apply to all security levels.

In new construction, and projects that include extensive site redesign, the minimum parking setback is 20', with an optimum setback of 50'[3]. If it is not feasible, e.g., existing construction of sites and roadways does not permit this distance; strive to limit parking closest to buildings to government owned vehicles or employees only.

In urban areas, parking is often permitted in curb lanes with a sidewalk between the lane and the building. Where the distance between the building and the nearest curb provides insufficient setback, install bollards or barriers along the curb.

[2] ISC– The Risk Management Process Appendix B: Countermeasures. September 2016 (For Official Use Only)
[3] USDA Integrated Physical Security Standards & Procedures Handbook



Cascade Lakes Visitor Center Site Design – Showing Setback, Vehicle Access, and Landscaping

Vehicle Access to Site

Vehicle access controls should be in place for all security levels. VSS should be used for Levels III and above.

Control access to the site by maintaining the minimum number of entry points required for operation. Separate Government/employee entrances and visitor entrances, where possible. Use landscaping and bollards or fencing to define the perimeters of each area.

Design site entrance and circulation controls to force speed reduction and prevent high-speed approaches to buildings. Use various types and designs of bollards and static barriers such as walls, fences, trenches, boulders, water features, vegetation, sculpture, and street furniture to deny a vehicle a direct approach to a site.

Parking area design should require drivers to enter and leave the area at the point furthest from the site. This moves activity away from the building and provides surveillance of parked vehicles and pedestrians approaching or leaving the site.

Controlled Parking Areas

Controlled Parking areas are required for Level III and above. However, any of the components can be used for any Facility Security Level if conditions for the site warrant it.

A parking pass or similar system should be used to clearly identify vehicles authorized to park in the controlled area. If an electronic gate is in use, program the system to allow access only to authorized vehicles.

Provide an area for screening. When possible, locate the inspection area beyond the setback distance and use barrier systems to ensure vehicles cannot pass beyond the screening checkpoint until cleared. At a minimum, screening should be a visual inspection of the vehicle, however detection technology can be installed if it is determined conditions warrant it. Provide adequate lighting and VSS coverage for screening area.

Clear Zones

Fence lines or other barriers should be clear of debris and vegetation that might conceal objects or persons from view. Ideally, the clear zone should be 20' on both sides of a barrier.

Landscape Design

Landscape Design is an essential element in the process of siting a facility. It may be used as a protective measure to obstruct views from outside a facility or as a physical barrier. In general, landscape design is a part of all Facility Security Levels, especially in regards to eliminating hiding places. At Facility Security Levels II and above, the landscape design will also have to take into account lighting, VSS, and other protective elements appropriate for the particular site.

Essential documents include "The Built Environment Image Guide for the National Forests and Grasslands" (BEIG)[4] and the application of Crime Prevention through Environmental Design (CPTED)[5] principles to each site. The BEIG sets standards for the 'look' of a site. CPTED is a crime

[4] Built Environment Image Guide, United States Department of Agriculture Forest Service, FS-710, September 2001.

[5] Problem-Oriented Guides for Police Problem Solving Tools Series Guide No. 8, Using Crime Prevention Through Environmental Design in Problem Solving, by Diane Zahm. US Department of Justice, August 2007.

prevention strategy intended to create a potentially crime free environment by influencing human behavior. CPTED involves the use of 5 principles:

1. Natural Surveillance (by placing physical features, activities, lighting, and people to preclude blind spots or hiding spots to keep intruders easily observable)

2. Territorial Reinforcement (using buildings, fences, different paving material, changes in street elevation, signs, and other landscaping to express ownership by distinguishing to potential offenders private spaces from public spaces)

3. Natural Access Control (strategic placement of entrances, exits, fencing, landscaping, and lighting to create in potential offenders a perception of risk);

4. Target Hardening (use of features that prohibit entry or access, such as perimeter boulders/large rocks, streetscape furniture, art ornaments, etc.).

5. Maintenance (Vegetation that obstructs views of guards or VSS, or interferes with lighting or IDS should be removed).

Utilize landscape design features to provide facility protection by extending the envelope of the protective measures beyond the immediate proximity of the building.

Landscaping used as entrance protection.

Design landscaping elements that are attractive, welcoming, fit with the BEIG guidelines, and enhance the security of the building. For example, thorny plants can deter unwanted foot traffic. Ponds and fountains can block vehicle access. Shrubbery, paths, or knee walls can be used to encourage pedestrians to use appropriate pathways.

Avoid landscaping that permits concealment, or obstructs the view of personnel and closed circuit television cameras. Avoid placing tall trees close to areas that facilitates intruder access to roofs or aids in circumventing perimeter fencing.

Storage, Container, and Receptacle Placement

Containers used for donation should be kept in secure areas of the facility accessible by the employees and not the public.

Locate dumpsters at least 25 feet away from buildings, preferably behind buildings – out of view, away from fuel storage and aircraft taxi ways. Lock paper and cardboard recycling containers, as arsonists use this refuse to start fires. Ensure that the local refuse and recycling haulers have access to the containers.

Restricted Areas

Restricted areas include, but are not limited to, utility connections, loading docks, emergency power supplies, childcare play yards, Hazardous Materials Storage, HVAC systems, and exterior access to critical rooms. The level of protection afforded by barriers should be commensurate with the need to limit pedestrian access. Higher levels of protection, intended to prevent determined intruders, are achieved using anti-climb fences or razor/barbed wire. Lower levels of protection, intended to guide pedestrians can be achieved using shrubbery, decorative fencing, or knee walls.

Bollards and Barriers

Although they are not required for Security Level I facilities, bollards and barriers can be used for all Levels, and they should be used to protect areas where vehicular damage will be costly. Bollards and barriers may take many forms: concrete posts, decorative steel posts, steel bicycle racks, anchored benches, large planters, walls, fences, trenches, ponds, water features, plantings, trees, sculpture, and street furniture are examples.

Maximum clear spacing between vehicle barriers is 4'. Minimum barrier height is 30".[6]

Barriers must be certified to meet performance requirements for vehicle size and speed specific to the facility under ASTM F 2656, *Standard Test Method for Vehicle Crash Testing of Perimeter Barriers*, or Dept. of Defense SD-STD-02.01, Revision A, *Test Method for Vehicle Crash Testing of Perimeter Barriers and Gates*. Normally the capacity to stop a 15,000-pound Gross Vehicle Weight Rating medium-duty truck traveling at 30 mph is sufficient for Forest Service sites.

Post and rail anti-crash barrier may be hidden with shrubbery to remove the 'keep out' message projected by many systems.

Typical Forest Service Bollard Use

[6] ISC– The Risk Management Process Appendix B: Countermeasures. September 2016 (For Official Use Only)

Planters Used as Bollards

Fencing

The perimeter fence is usually the most obvious physical protective measure and a strong psychological deterrent to criminal activity. Fencing restricts, or impedes access and should be fully integrated to form a continuous obstacle around a site, building, or area. Fencing is primarily applicable to Facility Security Level II and III, and should be focused on providing assets with an acceptable level of protection. It may be used at Facility Security Level I sites, but it is not required.

For Facility Security Level II and III sites, fencing is required around Government vehicle parking areas and restricted areas. Restricted areas include ground level utility mains, backup power generators, transformers, natural gas lines, LP gas tanks, fuel tanks and ground level heating, ventilation, and air conditioning (HVAC).

Government vehicle parking areas should be fenced, with electronic gates. Government vehicle parking area access gates/entrances should have electronic controls to minimize unauthorized vehicle entry and removal. This access control system should be tied into a Lenel/Linc Pass compatible system, if the building has that system. It may be a non-proprietary, common, off the shelf product and shall be scalable from a small to large system if the building does not have a Lenel/Linc Pass compatible system.

Electronic Gate Using Proximity Card Access Control

Use fencing to define the physical limits of a site, building, or area. Avoid blocking lines of sight with fencing and landscaping.

Normally select 8' chain link with a 3 strand barbed wire top guard. The barbed wire of a top guard should be at a 45-degree angle pointing upward and outward toward the unsecured side. Fence to employ galvanized 9 gauge or heavier wire with a mesh of 1" or less[7]. Set fence posts in concrete and bury the fence a minimum of 12". Fencing may be vinyl coated to reduce visual impact. Privacy slats should be considered as a feature to conceal assets.

Office parks, campus settings and privately owned buildings, may employ decorative fencing as long as it meets security requirements. A mix of fencing types may be installed to best serve each site.

Site Lighting

Good lighting is the single most effective deterrent to criminal activity. All Facility Security Levels have requirements for lighting, with more lighting needed at higher Security Levels. See the requirements table to find out which locations are required to be lit for each Facility Security Level.

Lighting should be sufficient to illuminate potential areas of concealment, enhance the observation of guard patrols and VSS, and provide for the safety of personnel moving between adjacent parking areas, streets, alleyways, and around the facility. Motion detectors may be used to trigger the illumination of pedestrian entrances to buildings. If the site has a VSS system, sufficient lighting must be provided to ensure VSS video images can be used to provide a clear description of a person and any activity they may be engaged in.[8]

Building entrance lighting shall have a minimum of one and a half hours of emergency power backup.

Parking lots should be designed with high-efficiency, pole mounted luminaires. LED lamps are preferred but consideration should be given to existing site illumination and the local environment. Emergency power is not required for parking lot lighting.

Horizontal illumination should have a uniformity ratio average of 4:1 and a maximum of 15:1. In the following table, lux multiplied by 10.7 equals foot-candles.

Location	Maintained Illumination Level (lux) [9]
Horizontal and vertical illumination of roofs and exposed parking areas (Gov't, employee and visitor)	2.5 lux
Horizontal illumination of covered and under-building parking areas (Gov't, employee and visitor)	10 lux
Vertical illumination of covered parking areas (Government, Employee and Visitor)	5 lux
Vehicular entrance to site/compound, illuminating sign	160 lux
Pedestrian entrance to building	160 lux
Horizontal illumination of stairwells and elevator lobbies	20 lux
Vertical illuminations of stairwells and elevator lobbies	10 lux

[7] The Tested and Proven Performance* of Security Grade Chain Link Fencing Systems
[8] ISC– The Risk Management Process Appendix B: Countermeasures. September 2016 (For Official Use Only)
[9] ISC– The Risk Management Process Appendix B: Countermeasures. September 2016 (For Official Use Only)

Utility Protection

Utility Systems have requirements for Facility Security Level II and above. Underground service is preferred, and any access point should be controlled. If utility systems cannot be located away from high-risk areas, service feeds, equipment, or equipment rooms should be hardened.

Protect utility systems by locating them away from vulnerable areas, and restricting access to assure that services will facilitate life safety and operations support after an event.

Access to security systems, emergency communications, and associated systems wiring and conduit shall be controlled. If possible, route these lines through separate and secure IT Rooms. Restrict access to utility closets. At a minimum, the doors should be locked with controls in place to manage the keys. If the facility has a card key system, use it to restrict access to these spaces.[10]

In existing buildings, assess whether the location of loading docks, or shipping and receiving areas are located within 50' of critical utility rooms, utility mains, telephone or data rooms, or cooling and heating mains. If the structure was designed with loading dock or shipping and receiving areas close to critical infrastructure areas, consider hardening the loading area to provide blast protection from potential vehicle or mail-borne explosives.

Propane Tanks

Tank Distances: Tanks under 500 gallons may be placed a minimum of 10' away from the building. Tanks over 500 gallons shall be placed a minimum of 25' away from a building. They shall also be placed a minimum of 25' away from a property boundary line and 50' from places of public assembly.

The distance between LP tank(s) and structures are listed in table below:

Tank or Cylinder Sizes	Building Clearances			Clearance to Fire Lookout Tower
	Underground Tank	Above Ground Tank	Distance Between Tanks	
	Feet	Feet	Feet	
4 - 420 lb. DOT Cylinders	n/a	10	3	Minimum 25 Feet
Up to 500 Gallons	10	10	3	
500 Gal. to 1,200 Gal.	10	25	3	
1,200 Gal. to 2,000 gal.	50	50	5	Per Code

Above Ground Tanks: Install fencing and bollards to protect tanks from trespassing and vehicular impact, as needed.

Below Ground Tanks: Underground tanks only need to have the tank dome 10" visible. Landscaping may be brought within a few feet of the tank. The average tank life is 30 years (no maintenance required). Underground tanks do not require fencing, only bollards/barriers in areas where they are vulnerable to traffic. Bollards may be camouflaged by vegetation. Barriers may be large concrete planters or something similar. Do not use benches in this area and prohibit smoking.

[10] USDA Integrated Physical Security Standards & Procedures Handbook; and Interagency Security Committee (ISC) Security Design Criteria For New Federal Office Buildings and Major Modernization Projects

Structure Security Criteria

Blast Resistant – Façade, Structure, Progressive Collapse

The construction type selected must meet all performance criteria for the specified Facility Security Level. Level I does not have performance criteria for this category. Level II requires the use of construction materials that are ductile (can bend, flex or move, and fails only after considerable deformation occurs) and can handle load reversals.

Level III requires a "Medium Façade Protection" as the baseline for design. Medium Façade Protection means that the facility will sustain a significant degree of damage, but the structure should be reusable. Assets may be damaged. Building elements other than major structural members may require replacement.

All building materials and types acceptable under model building codes are allowed. Design detailing is required for material such as pre-stressed concrete, pre-cast concrete, and masonry to adequately respond to the design loads. Unreinforced masonry shall not be used. Pre-stressed concrete is not very ductile and may not be appropriate where load reversals may occur.

All building components requiring blast resistance must be designed using established methods and approaches for determining dynamic loads, structural detailing, and dynamic structural response. The demands on the structure will be equal to the combined effects of dead, live, and blast loads. Blast loads or dynamic rebound may occur in directions opposed to typical gravity loads.

Design and analysis approaches should be consistent with U.S. Department of the Army Technical Manuals. Response limits shall follow U.S. Army Corps of Engineers PDC-TR 06-08, "*Single Degree of Freedom Structural Response Limits for Antiterrorism Design.*"

Progressive collapse is defined as an extent of damage or collapse that is greater than what the initial event created. Facility Security Levels I and II are exempt from considering progressive collapse, regardless of the number of floors. For Levels III, buildings under 4 stories tall are exempt from progressive collapse consideration[11]. Analysis for progressive collapse shall follow GSA's "*Alternate Path Analysis & Design Guidelines for Progressive Collapse Resistance,*" October 24, 2013.

Blast Resistance for Windows

Window blast resistance is a requirement for Facility Security Level II and above.

Design window systems so that the glazing will fail prior to the window framing and anchorage. Windows in doors shall meet the same specification as the windows in the building or not fail before the door under blast loadings. New glazing systems shall be designed with a minimum ½" bite[12].

Preferred glazing systems include:

1. Thermally tempered heat strengthened or annealed glass with a fragment retention film installed on the interior surface and attached to the frame;
2. Laminated thermally tempered, laminated heat strengthened, or laminated annealed glass.

An acceptable glazing system would be thermally tempered, heat strengthened or annealed glass with fragment retention film on the interior surface (edge to edge, wet glazed, or daylight

[11] ISC– The Risk Management Process Appendix B: Countermeasures. September 2016 (For Official Use Only)
[12] ISC– The Risk Management Process Appendix B: Countermeasures. September 2016 (For Official Use Only)

installations). Unacceptable systems include untreated monolithic annealed or heat strengthened glass, and wire glass.

In some cases, a combination of one of these preferred or acceptable systems and a catchment system (blast curtains, blast blinds, catch rods, etc.) may be effective, particularly when pressures above the designed strength are possible.

If fragment retention film is used, it must have a film composite strength and elongation rate measured at a strain rate not exceeding 50% per minute and shall meet the following as a minimum:

1. Yield strength: 12,000 psi
2. Elongation at yield: 3%
3. Longitudinal Tensile Strength: 22,000 psi
4. Traverse Tensile Strength: 25,000 psi
5. Longitudinal Elongation at break: 90%
6. Traverse Elongation at break: 75%

In most cases, a 7-mil retention film will be sufficient to meet the minimum physical properties.

Shatter Resistant Material for Windows

It is recommended that shatter-resistant film that meets performance condition '3b' be applied to the inside surface of existing exterior windows in the following locations:

1. The first floor windows of all office buildings.
2. Locations where rotating machinery may create projectiles or laboratory experiments may have unexpected results;
3. To the office windows of Line Officers (Ranger, Area Manager, Forest Supervisor, Station Manager, etc.).
4. In other locations when recommended by a security assessment.

Shatter-resistant film meeting performance condition '2' shall be applied to the exterior windows of areas occupied by law enforcement officers and the windows of day care centers in owned and leased office spaces.

Laminated Glass

Laminated glass, if broken, captures the glass fragments with an adhesive vinyl interlayer causing the broken glass and interlayer to remain in the frame. Laminated glass cannot be cut from the outside, which reduces the effectiveness of entry by glasscutter.

Laminated glass is more effective than annealed/tempered glass with an external security film, as the security film is incorporated into the layers of glass laminate, making it more secure. Laminated glass used within Forest Service facilities shall be constructed of two or more panes of glass with one or more layers of polyvinyl butyral (PVB) sandwiched between them and treated.

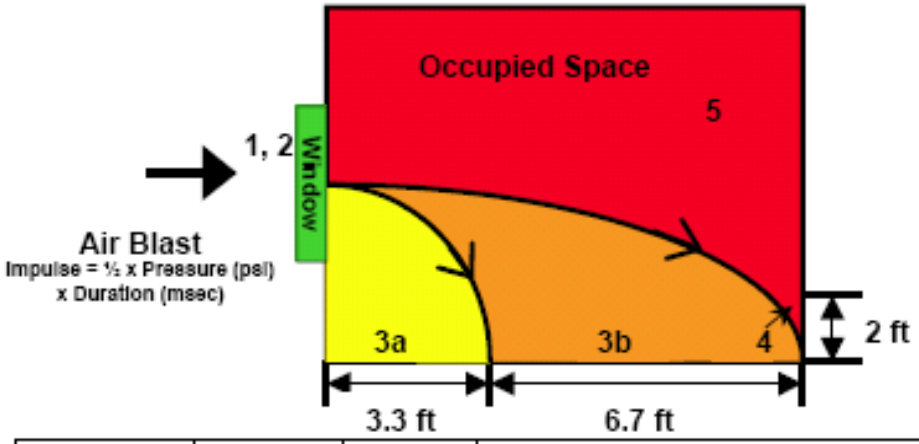
Laminated glass to meet the American Society of Testing Materials standard for preventing forced entry (ASTM F1233) and Underwriters Laboratories (UL972) burglary resistance guidelines.

Interior Windows

No special measures are required unless directed by the results of a Threat Assessment or if the building's blast or ballistic design would create pressures greater than 1 psi on interior windows.

GSA Performance Conditions for Window System Response

The below graphic and table represent the performance criteria that can be specified for a blast window. This performance condition, along with the Impulse of a blast should be specified when ordering a blast product. Note that ballistic and forced entry protection can also be specified and achieved in a blast product.



Performance Condition	Protection Level	Hazard Level	Description of Glazing System Response
1	Safe	None	Glazing does not break. No visible damage to glazing or frame.
2	Very High	None	Glazing cracks but is retained by the frame. Dusting or very small fragments near sill or on floor acceptable.
3a	High	Very Low	Glazing cracks. Fragments enter space and land on floor no further than 3.3 ft. from the window.
3b	High	Low	Glazing cracks. Fragments enter space and land on floor no further than 10 ft. from the window.
4	Medium	Medium	Glazing cracks. Fragments enter space and land on floor and impact a vertical witness panel at a distance of no more than 10 ft. from the window at a height no greater than 2 ft. above the floor.
5	Low	High	Glazing cracks and window system fails catastrophically. Fragments enter space impacting a vertical witness panel at a distance of no more than 10 ft. from the window at a height greater than 2 ft. above the floor.

Source: GSA Test Protocol: GSA-TS01-2003

Air Intake and Ventilation System Protection

The following applies to all Facility Security Levels:

Non-window openings greater than 96 square inches in perimeter walls should be secured with grilles, bars and IDS, if the facility is equipped with an IDS.

Fresh air intakes shall be relocated, extended or secured to prevent easy ground or roof access[13]. Relocating or elevating fresh air intakes reduces the possibility noxious or toxic substances may be introduced into the building by direct or indirect means. Locating intakes high on a wall is preferred over a roof location. When choosing secure locations for intakes in urban areas, take into consideration the vantage points offered to threats from nearby buildings and roofs.

For Facility Security Level III and above, provide separate HVAC systems for the reception area, mailroom, and loading docks. In addition, these systems shall not share a return-air system with each other.[14]

Areas served by a dedicated exhaust system shall be maintained at a negative pressure relative to the rest of the building, but at a positive pressure relative to the outdoors. Physical isolation of these areas (well-sealed floor to roof deck walls, sealed wall penetrations) is critical to maintaining the pressure differential and requires special attention to ensure airtight boundaries between these areas and adjacent spaces.

Additional information is available in The Centers for Disease Control and Prevention "*Guidance for Filtration and Air-Cleaning Systems to Protect Building Environments from Airborne Chemical, Biological, or Radiological Attacks*" DHHS (NIOSH) Publication No. 2003-136 and U.S. Army Corps of Engineers ETL 1110-3- 498, "*Design of Collective Protection Shelters to Resist Chemical, Biological, and Radiological (CBR) Agents.*"

[13] USDA Integrated Physical Security Standards & Procedures Handbook; and Interagency Security Committee (ISC) Security Design Criteria For New Federal Office Buildings and Major Modernization Projects; GSA Facilities Standards for the Public Buildings Service

[14] ISC– The Risk Management Process Appendix B: Countermeasures. September 2016 (For Official Use Only)

Facility Entrance Security Criteria

Facility Entrance Considerations

This information applies to all Facility Security Levels.

Limit the number of building entry points. All entry points must be controlled and monitored. For Level I facilities, control may take the form of ensuring the doors are locked when there are no personnel on site. Level II facilities and above require the use of an access control system for all entry points into the facility. Those entry points should be monitored via VSS and IDS.

Provide separate employee and visitor entrances, where possible.

Perimeter Doors

This information applies to all Facility Security Levels.

Select doors that resist forced entry and are appropriate for the type of facility. Exterior doors shall be hollow metal with hollow metal frames and they shall comply with the Steel Door Institute Publication 108, Level 4.

In order to meet BEIG requirements for the look and feel of the building, main entry doors may be a storefront type with heavy-duty aluminum frames. They need to have a minimum 5" bottom rail, 3" side rail, and cross rails. Door hardware shall be ANSI Grade 1 commercial mortise locksets with cylinder guards. Glazing shall be minimum of Underwriters Laboratory 752 Level 1.

Fire rated doors should not be modified for security equipment.

Hinges should be located on the secure side of exterior and critical interior doors. If they need to be located on the unsecured side, the hinges shall be designed to prevent door removal.

Door strikes shall have cover plates installed or otherwise designed to prevent the ability to break the lock. Door strikes should not allow the dead latch to be in the fully extended position when the door is closed.

Access Control Systems

Items listed in this Section apply to all Facility Security Levels, unless specifically noted otherwise.

Install locks on each perimeter door, the door between the reception area and the employee work area, and doors to utility rooms, janitor rooms, equipment rooms, manager offices, and storage areas within the facility.

Magnetic locks should have at least 1,200 pounds of shear holding power.

If there are electronic locks in use, the locks on perimeter doors must be set to lock if there is a power failure (fail secure), and the locks on interior doors must be set to unlock in that situation (fail safe). Electric strikes should meet all specification of UL Standard 1034, Burglary-Resistant Electric Locking Mechanisms.

Emergency exit doors shall be secured using an automatic door closer and exit hardware that is compliant with the applicable life safety codes and standards. Emergency exit door hardware should have an audible annunciator to provide notification of use and, if the door is monitored by IDS, the door should be on a 24 hour zone (never disarmed). Signs designating the door to be only

used in an emergency and notification of the alarm system should be posted on the door in an easy to see location.

Keyed Locks

Keyed locks are allowed as the primary access control for Security Level I and II facilities. However, the Forest Service Yale locks are not allowed. Replace all Forest Service Yale locks at buildings that are occupied by employees, store mission essential data, material or equipment, or contain components that are – or can be used – as a chemical, incendiary, or biological hazard. This includes utility buildings.

All new and replacement locks shall be commercial high security type meeting UL Standard 437, ANSI/BHMA Standard A156.30- 2003 - *High Security Cylinders* and ANSI/BHMA Standard 156.5-2001 - *Auxiliary Locks and Associated Products*, with a minimum rating of Grade 1. Select systems that feature keys that cannot be duplicated without signed authorization.

Locations possessing critical rooms or sites keyed without the benefit of electronic access controls, should consider re-keying each lockset at least annually.[15]

Electronic Access Control – Facility Security Level II and above

Level II facilities can have a high quality mechanical locking system that meets the qualifications listed above, and they can continue to have a mechanical locking system if the existing system needs to be replaced.

Facilities rated as Level II and above can have an existing legacy proximity card system. There is no direction requiring the Agency to upgrade existing systems. However, if the system needs to be replaced, it must meet the following requirements.

The Department of Agriculture Manual (DM) 4620-002 requires all new Physical Access Control Systems being installed into a USDA facility to be HSPD-12 compliant and to interface with the Department's Enterprise Physical Access Control System (ePACS). This requirement applies to owned and leased facilities.

Lenel is currently the only ePACS provider that can interface with the Department's national ePACS system and is the only system that is USDA approved. Other systems may be used, but they will require the use of a 3rd party middleware at the expense of the unit installing the system. In addition, since PACS are considered IT systems, it must undergo an extensive System Accreditation and Authorization process, also at the expense of the unit installing the system.

For leased facilities, if there will only be USDA Agencies as tenants in the facility, the access control system shall be a Lenel system. If the leased facility has several Government agencies as tenants, GSA will install the system of their choice and manage it. The USDA tenants may either work with GSA to have the GSA system cover their area of the building, or they may install a Lenel system on their suite and manage that themselves.

The only part of the Lenel access control system that is proprietary is the main control boards, door card reader boards, the card reader and the operating software. All other components are generic and multiple brands can be used, such as door hardware, door position switches, REX sensors, door operators, pushbuttons, conduit, wire, etc. This system must be put on the USFS wide area network to connect to USDA central system.

[15] USDA Integrated Physical Security Standards & Procedures Handbook

Region 6/10 Facilities has developed access control systems design guidelines, construction specifications, and example drawings for the devices required including card readers, main control panel, door hardware, REX sensors, door position sensors and other devices.

The following photos show typical access control system components.

Main Lenel Control Boards

Main Control Battery Supply

Link Pass Card Reader

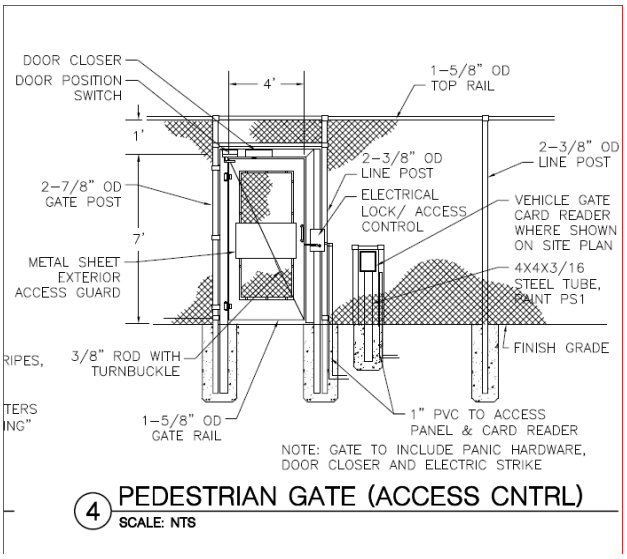
Door Pushbutton

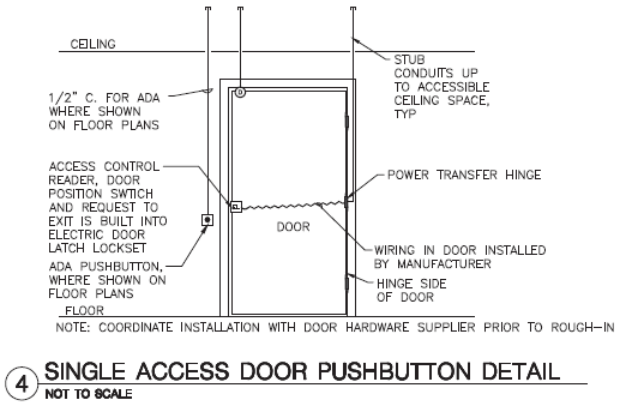
Door Hardware

Door position switch

REX Sensor

Motorized opener





Interior Security Criteria

Non-Public and Critical Areas

The level of protection provided should be in line with the risk to each non-public area. A single facility may have non-public areas protected at different levels of protection.

Stairwells, in general, should be avoided in secure areas. If that is not possible, the doors should be alarmed and monitored to prevent unauthorized use.

Where roof access allows entry to critical building areas or air intakes, IDS should be in place. For Level III facilities and above, VSS monitoring and recording should be used in conjunction with IDS.

All elevator control panels should have provisions for lockout of every floor, except the main reception area floor. The lockout should be reversible by key, except that elevators in buildings with card access systems should be equipped with a card reader to allow employees access to their area after hours. The card reader should be part of the cab panel design.

Corridor doors on upper floors giving access to tenant suites should be connected into the electronic access control system, as appropriate.

Doors to mechanical, electrical, and communications rooms, custodial spaces, storage rooms, and other equipment spaces must be locked by either electronic or mechanical means, and access shall be restricted to only those employees that need access.

More information on critical area security can be found at NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, April 2013; NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010, and NARA ISOO Directive 1, parts 2001.43 and 2001.52.

Security Systems Criteria

Video Surveillance Systems (VSS)

VSS are typically used in facilities that are Facility Security Level II and above. However, there can be circumstances in which a VSS should be used for a Level I facility. If the facility's mission is primarily for public contact, it has a sizable number of cash transactions, or it is in a location where there is a high crime potential, a VSS system should be installed.

VSS location requirements vary per security level. Level II facilities should have cameras covering locations where money transactions take place, and at personnel entrances and exits. In addition to those locations, Level III facilities should have cameras covering the building perimeter, vehicle entry and exit points, vehicle parking areas, in reception areas, roof access points, critical air intakes, restricted areas, and storage, container and receptacle locations. Each camera location should have a designated purpose and should be verified that they are meeting that purpose.

Signs should be posted at entrances to the site, facility, parking garages, etc., where VSS coverage exists. Signs should be large enough to be noticed, placed in easy to see locations, and have both words and pictures indicating video surveillance is being conducted at the location.

VSS Equipment

VSS are comprised of cameras, housings, mounts, power supplies, recording equipment, control equipment and monitors.

The design of the system will vary depending on the objective of the surveillance, environment, facility type, and end-user requirements. Use of a professional for the design and installation is essential to maximize the operational effectiveness of VSS.

The VSS should be stand-alone and operate independently from all Forest Service computers or networks. Recording resolution to be in high definition 80 pixels/foot, such that 'criminal' activities are easily recognized as well as faces.

It is recommended that surveillance video is stored for 60 days; however, that is a negotiable item with the Union. Recommend that the system be based on using a standard PC with a large hard drive as DVR and control system to simplify O&M.

VSS to consist of full color surveillance cameras with 24 hour/day time lapse digital video recording. When possible, the images shall be recorded at a minimum rate of 15 frames/second on digital media. For most cameras, motion recording with conditional refresh is recommended to reduce bandwidth and storage challenges. External entrance/exit cameras and cameras covering significant assets should record at all times. Power supplies for cameras, recording equipment should have battery back-up of 1 hour.

Sufficient lighting should be provided for hours of darkness. If lighting is not available, desirable, or feasible, low light cameras with infrared illumination (on or off camera) should be considered.

Pan, Tilt, and Zoom (PTZ) camera use should be limited to facilities that have active monitoring, or designed to focus on a specific area upon alarm activation. They should only be used if significant areas or assets have fixed cameras monitoring them. Panoramic cameras or lenses should be considered as an alternative to PTZ since they can be used for large area monitoring while still maintaining the ability to move the camera view without moving the camera itself.

All VSS cameras shall be UL listed and FCC compliant.

In the office, a large display should be located with a local controller at a reception area to allow real time monitors of all cameras in facility. Local controller allows selection of specific camera as well as reviewing previous recorded images. Some analytics, such as motion detection and magnetic door contacts, can be utilized to show specific locations when there is cause.

Steps should be taken to prevent tampering with VSS system, including installing cables and wire in a manner that will prevent unauthorized access, transmitting video signals via secure mediums, positioning exterior cameras out of reach, and placing cameras in tamper and weather resistant housings. VSS equipment and recorder shall be located in locked IT rooms. VSS shall be powered from IT room power panel and UPS.

Intrusion Detection System (IDS), General

Intrusion Detection Systems provide physical security, property protection and allow the monitoring of sites, extending the reach of our workforce. They are required for facilities that meet Facility Security Level II and above.

Install IDS to protect the perimeter of the building. An internal system may be installed when important exhibits, laboratories, computer/telecomm rooms, hazardous storage areas or valuables storage areas require protection.

Professional design, engineering, and installation are critical to ensure operational effectiveness of the IDS system itself and its integration with other physical security equipment. UL Listed intrusion detection equipment is required. Initial installation should include validation (testing) of the entire system, including monitoring center notification and connected equipment. Periodic testing and maintenance are required to ensure continuous operational effectiveness. Repair/replace malfunctioning equipment within 24 hours of failure.

At a minimum, an IDS should have the following coverage: Entry doors should have magnetic switches, an alarm system keypad at the main employee entrance, and motion sensor coverage. Windows and other openings greater than 96 square inches should have a glass break detector and magnetic switches or shock sensors. Motion detectors should also be used at first floor window locations and at entry doors. Alarm panels should be locked in a tamper proof container with a tamper switch, and should be located in a secured area.

Each alarm sensor should have its own zone to help with troubleshooting alarm points and response to alarms. Double doors should be zoned on each leaf, not both doors on one zone. Garage doors should have a sensor on each side to prevent lifting one side without an alarm. Install door contacts on the opening side of the door. The contacts should not allow the door to open far enough to provide the ability to tamper with the contact inside the door without going into alarm.

When new intrusion detection equipment is installed or upgrades are made to existing access controls, it is important to complete a detailed security system commissioning program and extensively train employees.

Each IDS shall be connected to a UL Listed central station that monitors the system 24/7/365 and will alert local (police, sheriff) or Federal authorities of an incident. If the facility also has a VSS, integrate the two systems together to facilitate immediate alarm assessment. Power supplies for alarm systems to have battery back-up of at least 24 hours.

A dedicated POTS (Plain Old Telephone System, or analog) line shall be run to the Central Office.

Consider integrating security systems with communications, fire monitoring, and other environment alarms to broaden the foundation of access control. The system should be located in the IT room – or other locked room if there is no IT room – and powered from the IT room UPS. It should also have an internal 24 hour battery backup.

Duress Alarms

Duress alarms should be utilized at any facility that has a front desk, cash/public transaction area, or at-risk area, regardless of its Facility Security Level.

Duress devices shall be concealed from the public. The duress alarm shall annunciate locally, in a distinct, loud and unmistakable tone, alerting every building occupant that there is a problem. The goal is to cause the 'troublemaker' to leave. The duress alarm shall be connected to a UL approved Central Station or FPS[16] when Agency LEO's or a security assessment require this connection.

Tie duress alarms in to the IDS as a separate zone for remote monitoring.

Procedures on response and telephone contact where the alarm occurred shall be established.

Public Address System (PA)

Facility Security Level II and higher facilities shall have a loudspeaker paging system. System shall be zoned and include a group function so communications may be with everyone or an isolated area/group without disrupting other areas or any combination of areas. System to include loudspeakers to provide emergency announcements, alerts, and instructions to occupants.

PA's are normally tied into the phone system for access by any phone. The PA system shall have a 1 hour back up power from IT Room UPS.

Emergency Communications Voice and Alarm Systems

Where Voice over IP (VoIP) telephone systems are used, keep two 'normal' (POTs) phone lines on site for emergency communications use or install sufficient emergency power to keep these systems operating for 24 hours after a power failure.

Fire Alarm Systems, if used, shall have dual communications lines that are POTS lines to a central office or have a 24 hour battery backup for communication to alarm receiving agency.

Intrusion alarm systems shall have communication lines that are POTS lines to a central office or have a 24 hours battery backup for communication to alarm receiving agency.

[16] Central stations alert local police/sheriff. FPS = Federal Protective Service. FPS alerts an internal central dispatch who contact local police/sheriff or Federal police.

Electronic Infrastructure Protection

Battery Backed Up UPS (Uninterruptible Power Supply)

This information applies to all Facility Security Levels where these systems are used. However, it is expected that the emergency power systems will increase in complexity as the Facility Security Level increases and as the number and types of systems needing emergency power increases.

If electronic systems or other critical building functions require longer term emergency power a generator may be required, see discussion for generator applications.

Provide a central IT room battery backed up UPS to feed one IT room panel which will power all electronic system in the IT room and protect sensitive electronic systems from power surges, and short term power outages up to 1 hour. See list of systems below.

Provide UPS backup power to support Agency mission, life safety requirements and to keep important systems functioning. Provide emergency power via an IT room UPS to critical systems (alarm systems, radio communications, telephone communications, emergency smoke evacuation, computer and network facilities, VSS monitoring, fire detection, access control system, PA system, and similar systems). Critical systems are defined as those where failure of the equipment to perform could result in loss of human life or serious injuries or could disrupt critical mission functions.

Connect critical Information Technology (IT) electrical circuits to the IT room UPS. The UPS should provide a minimum of one hours on a full load and the backup generator (if used) should provide a minimum of eight hours on a full load.17

The following table summarizes the minimum duration for backup power. These systems are powered by IT room UPS for equipment protection and short term power outages up to 1 hour. Some system have additional internal batteries for longer term operations as listed below. Run time duration longer that those listed below may require a backup generator.

System	Emergency Power Duration (min)
Burglar/intrusion alarm systems	24 hours on internal batteries
VSS monitoring	1 hours
Computer/IT facilities/network equipment. Verify with CIO	1 hours
Emergency telephone – VoIP or POTS backups	24 hours on internal batteries
Smoke control/ evacuation system Not on UPS	1 hours
Entry control/access control devices	24 hours on internal batteries
Fire Alarm and Detection	24 hours on internal batteries
HVAC for IT room if run on generator	8 hours if run on generator
Lighting – Exit lights Interior – per NFPA 101 internal batteries or generator power	1 ½ hours
Lighting – Exterior Entrance Lighting internal batteries not on UPS or generator power	1 ½ hours
PA systems	1 hours
Fire alarm system, if used	24 hours on internal batteries
Radio communications. Verify time with CIO	1 hours
Backup Generator minimum run time if used	8 hours

[17] USDA Integrated Physical Security Standards & Procedures Handbook

IT Room EPO System

Provide an IT room Emergency Power Off (EPO) system to shut down power to IT room per NEC article 645 with emergency power shut off to UPS, UPS batteries and HVAC equipment. Room shall have manual shutdown pushbutton at each exit door. Provide a high temperature shutdown system of IT room power for over temperature with a waring alarm connected to intrusion detection system for remote monitoring and a high temperature shut down time delayed second temperature sensor. Interlock IT room fire alarm system with IT room EPO system. See IT design guidelines for details.

Surge Protective Devices

Provide a Surge Protective Device on all building electrical service entrances and on all power panels feeding electronic systems such as IT rom power panels or other panels that feed electronic equipment.

Emergency Power Outlets

Main mechanical and electrical equipment rooms shall each have one emergency power receptacle that is identified as Emergency Power at the receptacle.

Grounding

Provide a maximum of 25-ohm ground to the building service through multiple electrodes and a Ufer concrete encased electrodes if possible. Intertie IT room grounding system to main building grounding system and to any antenna structures.

Emergency Generators

This information applies to all Facility Security Levels where generators are used.

Supply emergency generators when necessary to support the Agency mission and life-safety requirements. The need for a backup generator and systems to be powered shall be evaluated on a case-by-case basis.

Building systems that should be supported by an emergency generator include fire alarm, intrusion detection systems, access control system shall have internal 24-hour battery backup time for operation.

Some facilities, such as a dispatch center, may require long-term generator power in portions of a building or all of a building. These backup power needs may include lighting and HVAC systems, IT and network system and other electronic systems or other systems.

The generator shall power in addition to any mechanical or electrical loads the building IT room UPS and any other life safety items as required, such as exit lighting as part of the uninterruptable power supply for critical electronic systems (IT, security etc.).

Generators shall provide power to the IT room UPS, the IT room cooling system, and other critical systems as required.

Generators are only required if the required duration of operation is greater than the 1 hour provided by the IT room UPS system or if other critical building functions must be operational for an extended time, such as a dispatch center or other telecommunications needs such as radio systems.

Install generators in the most secure location available. More secure locations include the roof, protected grade level, and protected interior areas. VSS and IDS should be utilized to protect the generator, if such systems are in place.

If the emergency generator is installed outdoors, it should be provided with a suitable enclosure with perimeter walls, locked entrances and have provisions to ensure reliable starting in cold weather. The generator should not be located in an area prone to flooding.

Provide measures to secure the refueling and shut off valves in fuel lines within or in close proximity to the building.

A remote stop on exterior of building shall be required in a locked enclosure, and an internal generator monitoring panel shall be provided inside building in an accessible area such as reception.

Silence interior generators and generator rooms.

Generator fuel storage should be located away from loading docks, entrances, and parking. Access should be restricted and protected (e.g., locks on caps and seals).[18] Provisions for securing refueling and shut-off valves in fuel lines within or in close proximity to the building must be addressed.

Generator shall have 8 hour run time at full load, unless a larger backup run time is required.

Generators shall meet all EPA and local codes and shall be supplied with double wall fuel tank and leak detection system.

[18] USDA, DoD, GSA and ISC requirements

Cyber Security Criteria

Building Automation and Control Systems (BACS)

Building Automation and Control Systems are often referred to as Direct Digital Control (DDC) Systems. Some of the systems that may be tied into a BACS system includes fire alarm and suppression, emergency lighting, access controls, advanced meters, HVAC controls, and surveillance.

Forest Service facilities often do not have a BACS, especially if they are older facilities. However, if a BACS is installed and operational within a facility, it needs to meet the following criteria. Work with CIO (Chief Information Office) to ensure the BACS are protected.

BACS equipment shall be protected against remote electronic access by unauthorized persons. Firewalls or other means are required for any system placed on an external DSL or other internet access line. In addition, the BACS system should be physically isolated from the Forest Service network (the BACS system cannot be on a computer that connects to the network). If that is not possible due to cabling limitations, the system will require virtual separation, which will need to be completed by CIO.[19]

Access to BACS systems and networks should be restricted to users, processes, and devices that are authorized. Place the BACS components in a secured area, and work with CIO to limit virtual access to the system.

The physical BACS structure should be protected by ensuring proper maintenance, timely lifecycle replacements, and installation of patches and updates.

An up to date list of all of the devices connected to the BACS should be kept in the IT room. The list should include information on manufacturers, model numbers, configuration settings, and contact information for the party responsible for maintenance.

[19] ISC– The Risk Management Process Appendix B: Countermeasures. September 2016 (For Official Use Only)

Specific Facility Requirements

Some types of facilities – and some areas within facilities – have specific requirements in addition to the general requirements. Those are listed below.

Reception Areas

Reception areas shall be designed to divide public and employee secure areas. Each reception area shall have an emergency egress (escape) door located behind the desk. The area shall be designed so that visitors are required to make contact with a front line employee prior to being allowed within the facility. Visitors shall have only one access point to the facility.[20]

For Security Level III facilities and above, provide an area for screening.[21] Screening should be accomplished using non-intrusive electronic methods such as X-rays and magnetometers, but may include other means.

Public toilets, service spaces, stairs and elevators should not be located in non-secure areas including the queuing area before screening at the public entrance.

Each location should establish procedures to control the movement of visitors, ensuring they are afforded access only to areas within the building and/or information consistent with the scope of the visit. Locking barriers should be installed to restrict visitor movement and prevent unauthorized access to office work areas.

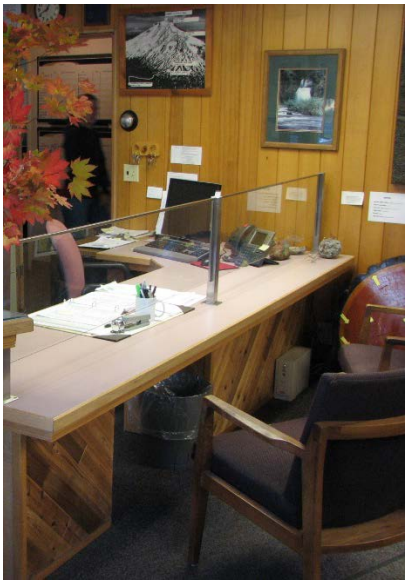
Duress Alarms: There shall be a duress alarm provided in every building with a reception area.

Reception Desk Requirements:

- Accessible and Desk Section Height: 28" to 30"
- Gallery Height: 42"- 48"
- Protective Barrier at the Accessible Section: The goal of this barrier is to prevent someone from reaching over and attacking the front line employee. It should be as high as the rest of the counter. However, to ensure that the counter can be used as intended, leave a 6" – 8" gap between the counter and barrier.
- Provide a concealed duress alarm pushbutton.
- Reception Desk Access Door: There is not a requirement to have a door in the reception desk – it can be one contiguous unit. However, if there is an access point in the reception desk that allows access to the reception area, an access door that is the height of the reception desk is required.

[20] ISC– The Risk Management Process Appendix B: Countermeasures. September 2016 (For Official Use Only)
[21] ISC– The Risk Management Process Appendix B: Countermeasures. September 2016 (For Official Use Only)

Reception Desk Examples



Protective Glass at Accessible Counter

Sliding Wood Barrier at Accessible Counter

Laboratories

Provide all security requirements listed for a Level II or higher facility. The following items are in addition to these requirements.

The requirements for laboratories are based on USDA Department Regulations and 42 CFR – part 73. A laboratory is considered a "Property Protection Area", which is a secure area established to protect against damage, destruction, or theft of USDA owned property or equivalent. If there are multiple laboratories in a building, the entire building shall be classified as a Property Protection Area. If there is a single laboratory in a building, the Property Protection Area shall apply only to that room.

The laboratory standard would be equivalent to a Biosafety Level 2. (BSL-2). See USDA and OSHA standards for additional information.

Access Control

All facilities in the property protection area must be locked and security keys shall be protected. Physical access control shall be in place to ensure that only authorized personnel are allowed into areas that have a designation of "limited" or "exclusion."

Duress Alarms

Duress alarms in laboratories serve two functions: they alert the facility of a hazardous situation caused by an unplanned release of agents or equipment failure, and they alert managers and the central station of an intrusion into a restricted area.

Location and operation of duress alarms used in labs should be specifically addressed as part of the design.

Shatter Resistant Material for Windows

Shatter-resistant window film or laminated glass shall be specified for windows in laboratories where moving machinery or chemical reactions may have unexpected results.

HVAC System

Fresh air intake openings and exhaust air outlets shall be strategically placed to prevent reintroduction of particulates from the exhaust air back into the building. It is recommended that a professional engineer with experience in design of laboratory HVAC systems evaluate air contamination risks in existing laboratory facilities. To mitigate the contamination risk, a Computational Fluid Dynamic (CFD) study might be warranted.

Fume hoods in the laboratory areas shall be tested for code compliance with minimum/maximum allowable face velocities in various sash positions. Testing shall also be conducted to verify that laboratory spaces are maintained in negative static pressures relative to the adjacent non-laboratory spaces. Fume hood testing shall comply with ASHRAE 110 performance testing guidelines.

Laboratory areas may consider a combination of ultraviolet germicidal irradiation (UVGI) lamps in combination with MERV 13 filters, to prevent contaminants from spreading throughout the facility.

Emergency Power System

Auxiliary power shall be capable of maintaining full operation of the intrusion detection and assessment system for 8 hours or for such a time as would be needed to implement contingency plans, whichever is greater.

Ensure that mission critical systems, such as HVAC units for quarantined laboratory areas or greenhouses have emergency back-up capability in order to maintain negative pressure within quarantine areas in the event of a loss of power.

Auxiliary power shall be available for chemical and experiment containment, refrigeration, or other critical systems for such time as needed to implement contingency plans. Transfer to auxiliary power shall be automatic upon failure of the primary source and shall not effect operation of the security system or powered device(s).

The alarm central station shall receive an alarm indicating failure of the security system power and transfer to the auxiliary power source.

Law Enforcement Offices

Law Enforcement Officers have possession of evidence, weapons, ammunition and equipment that allows them to perform their function. The following features are to be included in the area designated for occupancy by law enforcement officers.

Perimeter and Entrance Security

1. If there is a VSS on site, it should cover the entry into the law enforcement office/suite and parking areas with LE vehicles.
2. Exterior entrances shall have high security locks. If the building has an access control system, all doors in the law enforcement suite/office shall be wired for access control systems.
3. Buildings where Law Enforcement Officers store firearms, ammunition or evidence shall be protected by IDS. The law enforcement area shall be on a separate zone and have access restricted to authorized personnel only.

Construction

1. Design walls surrounding law enforcement offices to achieve a glazing performance condition of "2" and a façade protection level of "higher" given a blast load standard of 10 psi/89 psi-msec. [22]
    a. Glazing performance condition "2" provides for a very high protection level and a hazard level of "none". For a blast of 10psi/89 psi-msec, the glazing cracks but is retained by the frame. Dusting or very small fragments near the sill or on the floor are acceptable.
    b. A "higher" level protection to the facade will result in minor damage, but repairable. The facility or protected space may globally sustain minor damage with some local significant damage possible. Occupants may incur some injury, and assets may receive minor damage.
2. Walls surrounding the suite/office shall be extended through the attic to the bottom of the roof structure to prevent access to the office from above.

HVAC

1. Protection measures shall not adversely affect the performance of the building HVAC system. Supply and return ductwork leading into the law enforcement suite shall have "burglar bars" within the ducts to prevent a person from crawling in the ducts to access the law enforcement office/suite.
2. Dedicated HVAC shall be required for evidence storage areas to provide negative space static pressures to prevent widespread dispersion of a contaminant released in those areas.
3. Install MERV 13 filters in the dedicated HVAC units serving the evidence storage areas.

Aircraft Sites

Tanker Bases, Rappel Bases, Air Attack Bases and Reload Bases are facilities used to deploy fixed-wing or rotary aircraft on a wildland fire, to drop retardant or extinguishing agents, shuttle and deploy crews and supplies, or perform aerial reconnaissance of a fire situation. Aircraft sites are locations where Contract or Government owned aircraft are stationed or stored during or between Government operations.

[22] Design using WINGARD 3.15 or later or WINLAC 4.3 software.

Setbacks and Parking

Maximize distance between the parking areas and terminal/hanger buildings. Curb should be at least 20' from the front of the building. The site should have a buffer zone of at least 100' from public roads and property of other ownership.

Unscreened/unknown vehicles should not be permitted to park within 50' of the terminal building. If it is not feasible (e.g., existing construction of sites and roadways does not permit this distance) strive to limit parking closest to buildings to known staff or employees only.

Provide a path for delivery vehicles that does not allow access to unauthorized areas.

Adhere to all Federal Aviation Administration (FAA) and Department of Homeland Security requirements for airport layout and access.

Lighting

Perimeter exterior lighting should be turned on at night. Hangars that are in close proximity to perimeter fencing should install lighting to cover the area between the fence, the hangar, and five feet past the fence.

Access Control and Perimeter Security

Government vehicle and aircraft parking area access gates/entrances should have electronic controls to minimize unauthorized entry and vehicle/aircraft removal. This access control system may be a non-proprietary, common, off the shelf product and shall be scalable from a small to large system. If a Linc Pass system is installed in the building, then the perimeter security system should be tied into the Linc Pass system.

Shatter Resistant Material for Windows

Shatter-resistant film meeting performance condition "3b" shall be applied to the exterior windows of terminals, pilot ready rooms and airport/aircraft management offices.

Child Care Centers (CCCs)

At a minimum, a CCC should meet all of the requirements for a Level II facility.

Setbacks and Siting

Maximize the building setback, locating all vehicles as far away as possible from the building. Under optimum conditions, require at least a 50' setback. Make every effort to locate CCCs away from streets, parking areas, and staff or public entrances. The location must allow for the safe arrival and departure of children.

Children are more vulnerable to all forms of pollution than adults. Ensure child care facilities and play areas are located away from roads that contribute air pollution (exhaust, brake and tire dust), equipment or machinery that generate noise pollution, orchards/gardens that are sprayed with fertilizers or pesticides and shops or maintenance yards that create other types of dusts, paint/finish fumes and other airborne chemicals or noise.

Locate childcare facilities as far away from main gas and electrical utility lines as practical so that children are not threatened in the event of a line disruption or catastrophic failure. Ground-level electrical transformer boxes should always be distant and secured from children's play areas. Gas meters and emergency cut-off valves should be similarly placed and secured. Consideration should also be given to the location of lower voltage electric lines supported by wood poles that have been known to snap in high winds and electrify perimeter chain link or cyclone metal fencing.

Barriers and Fences

Child play areas should not be adjacent to a parking lot. Where this is unavoidable, use barriers, bollards, and differences in grading and creative landscaping to prevent vehicles from deliberately or accidentally entering play areas.

Enclose play yards with fencing. The minimum height of the perimeter fence is 6'.

Receptacle and Container Placement

Position trash containers, vending machines, or other fixtures and features that could conceal devices away from building entrances, windows, or play yards.

Entrance Security

The key system should be on a separate restricted system from the rest of the facility.

Parents and visitors shall have only one access point to the facility. The entrance into the facility shall be provided with a means to secure the door and to verify the identity of persons requesting access prior to allowing them into the facility.

Locking barriers shall be installed to restrict visitor movement and prevent unauthorized access to childcare areas. All perimeter doors, except a lobby entrance, to remain locked. If there is no receptionist in the lobby, a bell or alert device attached to the main door to activate automatically on visitor/parent entrance alerting staff of the presence.

Use delayed egress hardware on all emergency exits, if fire code allows.

Windows

Locate operable windows so children cannot crawl out, nor an intruder lift a child through them.

Use a combination of protected setback, window glazing, and/or blast protection film to achieve at least a Performance Condition "2" for exterior windows. Interior windows should be laminated tempered glass with a minimum 0.06 inch polyvinyl butryral (PVB) interlayer.

Security Systems

Provide VSS coverage for all entrances (both primary and emergency egress) and for the play yard. Monitoring shall be provided in the CCC Director's Office as well as at another monitoring location.

During hours of operation (when children are on-site), the Intrusion Detection System should have on-site annunciation.

Provide duress alarm buttons in the staff offices and in the play yard. Classrooms may also require duress buttons, depending on facility layout.

Hazardous Material Storage Buildings, Gas & Oil Houses

Locate hazardous materials storage buildings, and gas and oil houses as far away from visitors and routinely accessed buildings as practicable. Setbacks should be at least 100', when possible, from other facilities.

Fencing is required. An area of the compound may be fenced rather than an individual building. Post required signs that alert persons of the hazards without calling attention to the hazard. Ensure that valves and control mechanisms associated with the facility are protected from unauthorized access.

When power is supplied to the building, light building perimeter to a level that is not less than an average of 10.8 lux (1 foot-candle) within a 10' radius of the structure. All wiring for these facilities must meet NFPA 70 for the specific classification of hazard.

Refer to pertaining State fire code for maximum allowed storage of hazardous material in a given storage space. Mechanical ventilation shall be required if it exceeds maximum allowed, otherwise it is acceptable to install natural ventilation to reduce space heat built-up and dilute flammable and combustible substances. Mechanical ventilation shall use only nonferrous fan blades for fans located within the ductwork and through which hazardous materials are exhausted. Motors shall be located outside the duct.

All electrical wiring for these facilities shall comply with NEC for the classification required for the materials being used in the facility.

Explosive Magazines

The building should be at least 100' from other buildings, public roads, and property of other ownership.

Prohibit parking within 100' of the building when located on a compound. Authorized personnel may park adjacent to the magazine only for the duration of blasting program related activities.

Fencing shall be 8' chain link with 3-strand barbed wire, if magazine is above ground. Locate fence 50' from the magazine.

Do not call attention to the facility by lighting it. Do not add electricity unless mandated by other requirements.

Tree Coolers and Nursery Storage Coolers

If ammonia is used as a refrigerant, no parking is allowed within 50 feet of the building. In addition, the building should be at least 100' from public roads and property of other ownership.

Acronyms

ANSI/BHMA	American National Standards Institute/Builders Hardware Manufacturers Association
BACS	Building Automation and Control System – also known as DDC (Direct Digital Control) System
BEIG	Built Environment Image Guide
CBR	Chemical/Biological/Radiological
CCC	Child Care Center
CCTV	Closed Circuit Television – now referred to as "VSS"
CIO	Chief Information Office
CPTED	Crime Prevention Through Environmental Design
ePACS	electronic Physical Access Control System
FPS	Federal Protective Service
FSL	Facility Security Level
HDMI	High Definition Multimedia Interface
HSPD	Homeland Security Presidential Directive
HVAC	Heating Ventilation and Air Conditioning
IDS	Intrusion Detection System
ISC	Interagency Security Committee
LOP	Level of Protection
MERV	Minimum Efficiency Reporting Value
NARA ISOO	National Archives and Record Administration Information Security Oversight Office
NEC	National Electrical Code
NEF	National Essential Functions
NFPA	National Fire Protection Association
NIST	National Institute of Standards and Technology
PA	Public Address (System)
POTS	Plain Old Telephone (analog) System
PTZ	Pan, Tilt, and Zoom – video surveillance cameras
PVB	Polyvinyl Butyral
UL	Underwriters Laboratory
USDA	United States Department of Agriculture
VoIP	Voice Over Internet Protocol – telephone system
VSS	Video Surveillance System

Definitions

Acceptable Risk	Acceptable risk describes the likelihood of an event whose probability of occurrence is small, whose consequences are so slight, or whose benefits (perceived or real) are so great that individuals or groups in society are willing to take or be subjected to the risk that the event might incur.
Baseline Level of Protection	The degree of security provided by the set of countermeasures for each facility security level that must be implemented unless a deviation (up or down) is justified by a risk assessment.
Baseline Threat	The estimate of the relative threat posed to a Federal facility from an undesirable event. Baseline threat is categorized as Minimum, Low, Medium, High, or Very High.
Buffer Zone	A tract of land between a facility or protected area.
Building Entry	An access point into, or exit from, the building.
Building Envelope	The outside surface and dimension of a building, inclusive of the façade and roof.
Consequence	The level, duration, and nature of the loss resulting from an undesirable event.
Critical Areas	Areas that, if damaged or compromised, could have significant adverse consequences for the health and safety of individuals within the building or the surrounding community. May also be referred to as "limited access areas," "restricted areas," or "exclusionary zones." They do not necessarily have to be within government-controlled space.
Design-Basis Threat	A profile of the type, composition, and capabilities of an adversary.
Essential Functions	Government functions that enable Federal Executive Branch agencies to provide vital services, exercise civil authority, maintain the safety and well-being of the general populace, and sustain the industrial/ economic base in an emergency.
Existing Level of Protection	The degree of security provided by the set of countermeasures determined to be in existence at a facility.
Exterior	Area between the building envelope and the site perimeter.
Façade	The exterior face of a building, inclusive of the outer walls and windows.
Facility Security Committee	A committee that is responsible for addressing facility specific security issues and approving the implementation of security measures and practices.

Facility Security Level	A categorization based on the analysis of several security related factors, which serves as the basis for implementation of countermeasures.
Facility Security Assessment	The process and final product documenting an evaluation of the security risks to a facility. The process analyzes potential threats, vulnerabilities, and estimated consequences culminating in the risk impacting a facility using a variety of sources and information.
Level of Protection	The degree of security provided by a particular countermeasure or set of countermeasures.
Level of Risk	The combined measure of the threat, vulnerability, and consequence posed to a facility from a specified undesirable event.
National Essential Functions	The most critical functions necessary for leading and sustaining our Nation during a catastrophic emergency.
Necessary Level of Protection	The determined degree of security needed to mitigate the assessed risks at the facility.
Risk	A measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence.
Risk Acceptance	The explicit or implicit decision not to take action that would affect all or part of a particular risk.
Risk Assessment	The process of evaluating credible threats, identifying vulnerabilities, and assessing consequences.
Risk Management	A comprehensive approach to allocating resources for the protection of a facility, assets, and occupants to achieve an acceptable level of risk. Risk management decisions are based on the application of risk assessment, risk mitigation, and, when necessary, risk acceptance.
Risk Mitigation	The application of strategies and countermeasures to reduce the threat of, vulnerability to, and/or consequences from an undesirable event.
Security System(s)	Electronic system(s) that are designed to prevent theft or intrusion and protect property and life. Intrusion detection, access control, fire alarm, and video surveillance systems are all types of security systems.
Setback	The distance from the façade to any point where an unscreened or otherwise unauthorized vehicle can travel or park.
Threat	The intention and capability of an adversary to initiate an undesirable event.
Undesirable Event	An incident that has an adverse impact on the facility occupants or visitors, operation of the facility, or mission of the agency.
Vulnerability	A weakness in the design or operation of a facility that an adversary can exploit.