INTERAGENCY SECURITY COMMITTEE

The Risk Management Process

An Interagency Security Committee Standard

2021 Edition

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Interagency Security Committee

Change History and Document Control

Rev. #	Date	Changes	Approver
1.0	08/2013	Initial Issue	ISC
2.0	11/2016	Document Update	ISC
3.0		Document Update	ISC

Document Control

Distribution of this document to federal, state, local agencies, and private individuals or enterprises is authorized.

Message from the Interagency Security Committee Chief

One of the priorities of the Department of Homeland Security (DHS) is the protection of federal employees and private citizens who work within and visit federally owned or leased facilities. The Interagency Security Committee (ISC), chaired by the DHS, consists of 64 departments and agencies and has a mission to develop security policies, standards, and recommendations for nonmilitary federal facilities in the United States.

As Chief of the ISC, I am pleased to introduce the updated *Risk Management Process: An Interagency Security Committee Standard, 2021 Edition*. This ISC standard defines the criteria and processes that those responsible for the security of a facility should use to determine its facility security level and provides an integrated, single source of physical security countermeasures. The standard also provides guidance for customization of the countermeasures for federal facilities.

Consistent with Executive Order 12977 (October 19, 1995), *The Risk Management Process: An Interagency Security Committee Standard (2021)* is intended to be applied to all buildings and facilities in the United States occupied by federal employees for nonmilitary activities. These include existing owned, to be purchased or leased facilities; stand-alone facilities; federal campuses; individual facilities on federal campuses; and special-use facilities.

This standard represents exemplary leadership from the Standards Subcommittee and collaboration amongst members across the entire ISC. This document will be reviewed annually and updated as needed.

Daryle Hernandez
Chief, Interagency Security Committee
Cybersecurity and Infrastructure Security Agency

Executive Summary

The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard defines the criteria and processes that those responsible for a facility's security should use to determine its facility security level (FSL). *The Risk Management Process* provides an integrated, single source of physical security countermeasures for all federal facilities. This standard also provides guidance for how to customize countermeasures for facilities and how to integrate the standards and concepts contained in the Interagency Security Committee's (ISC) *Appendix A: The Design-Basis Threat Report*.

New construction—with few exceptions—is fully expected to meet the necessary level of protection (LOP). In some cases, site limitations may restrict standoff distances, or fiscal limitations may prohibit the implementation of some measures; both examples illustrate why the security requirements should be identified as early in the process as possible (see Section 5.2.1). During the design process, there is a point where design changes are cost-prohibitive and make the LOP unachievable.

During the lease process, it may be decided that available facilities in the delineated area cannot meet the requirements of the LOP. This decision may be determined by providing a market survey, or when responses to a solicitation do not meet the requirements specified to meet the LOP.

All users of the standard should understand that there are no guarantees that even the best assessments, countermeasures, and procedures will protect federal facilities from potential threats. However, non-compliance with these ISC standards has the potential to leave federal agencies exposed to risks in protecting their workforce, visitors, and facilities. This standard uses a "building block" approach, which consists of the following sections:

Section 1.0: The Interagency Security Committee Risk Management Process not only introduces the risk management process but also outlines the approach necessary to identify, assess, and prioritize the risks to federal facilities. This approach is followed by a coordinated application of countermeasures to minimize, monitor, and control the probability of an undesirable event and its associated impact. Risk management decisions are based on the application of risk assessment, risk mitigation, and—when necessary and otherwise reasonably unavoidable—risk acceptance.

Section 2.0: Background reviews foundational documents that codify the Department of Homeland Security's responsibility for protecting buildings, grounds, and property that are owned, occupied, leased, or secured by the federal government.

Section 3.0: Applicability and Scope outlines the ISC and the standard's authority.

Section 4.0: Facility Security Level Determinations for Federal Facilities supplies the information needed and process required when designating a federal facility's facility security level (FSL). The FSL is then utilized to establish a recommended baseline level-of-protection, and associated countermeasures, that should be customized to address site-specific conditions.

Section 5.0: Integration of Countermeasures provides an overview of how the application of physical security criteria is predicated on an FSL designation. Once an FSL has been determined, departments and agencies follow a decision-making process outlined in this section to identify an achievable level of protection that is commensurate with, or as close as possible to, the level of risk without exceeding the level of risk.

Section 6.0: The Risk Informed Decision-Making Process summarizes a process of identifying and implementing the most cost-effective countermeasure appropriate for mitigating vulnerability, thereby reducing the risk to an acceptable level.

Section 7.0: References provides references to other ISC documents for use in implementing this standard. These materials are For Official Use Only (FOUO) and must be obtained directly through the ISC.

Section 8.0: Acknowledgments identifies and thanks the individuals who contributed to the development of this standard and other documents related to implementing effective risk management processes.

Appendix A: Design-Basis Threat Report (FOUO) creates a profile of adversaries' types, compositions, and capabilities. Appendix A correlates with *Appendix B: Countermeasures*.

Appendix B: Countermeasures (FOUO) establishes a baseline set of physical security countermeasures to be applied to all federal facilities based on their designated FSLs. These baseline countermeasures provide comprehensive solutions under seven criteria of physical security.

Appendix C: Child-Care Centers Level of Protection Template (FOUO) specifies the customized level of protection to be incorporated as the basis for security planning for a child-care center.

Appendix D: How to Conduct a Facility Security Committee provides guidance on how to establish and conduct a Facility Security Committee (FSC) when presented with security issues that affect the entire facility.

Appendix E: Use of Physical Security Performance Measures provides guidance on how to establish and implement a comprehensive measurement and testing program.

Appendix F: Forms and Templates provides additional guidance to users.

Updates

Since the release of the 2016 edition of *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*, the ISC reviewed and updated the content of this document. Numerous review periods by ISC membership and by the ISC Standards Subcommittee helped update this standard. Most of the updates to the 2021 edition did not have any major effects on the processes and procedures contained therein. What follows is a list of significant changes and supporting information (if necessary):

- **Section 4.1**: Added footnote clarifying "routinely occupied" facilities.
- **Throughout**: Redefined the update timeline for the Risk Management Process (RMP).
- **Section 4.4.3**: Clarified the facility population factor and use of the peak number of visitors.
- **Section 4.6**: Added video surveillance system (VSS) to acronym list.
- **Throughout**: References to the security provider and the security organization were updated for appropriate context.
- **Figure 5-1**: Updated RMP chart to add "Measure Performance" as a separate step.
- **Section 5.2.6**: Included guidance for single and multi-tenant campuses.
- **Throughout**: Verbiage and terms were changed to reflect the Design-Basis Threat Report (DBT).
- **Glossary of Terms**: Added new terms and removed superseded information.
- **Section D.1**: Recommendation that FSC requirements be communicated in writing to tenant during lease acquisition process. New verbiage on FSC meetings and virtual options.
- **Section D.2.6**: Added ISC training options and recommendations for FSCs to retake training courses when significant updates to the RMP are made.
- **Section D.3** Included guidance on FSC charters.
- **Section D.3.1**: Clarified quorum and voting requirements.
- **Section D.3.1.1**: Included guidance on when to consider alternative proposals for disapproved countermeasures.
- **Section D.3.3**: Additional requirements for FSC member responsibilities were added.
- **Section D.3.4**: FSC training requirement was added.
- **Section D.3.5**: FSC training requirement was added.
- **Throughout**: Changed "Chief Security Officer" to "Senior Security Official."
- **Section D.6**: Changed timeframe of records retention to two assessment cycles. Added reference to the National Archives and Records Administration (NARA) guidance.
- **Appendix F**: Added recommendation to FSC Charter Template that FSC requirements be communicated in writing to tenant during lease acquisition process. New section on FSC meetings and virtual options. Added section on records retention. Added templates of FSC Meeting Agenda and Meeting Minutes.

Table of Contents

Figures

Tables

Appendices

1.0 The Interagency Security Committee *Risk Management Process*

The risk management process begins by outlining the approach necessary to identify, assess, and prioritize the risks to federal facilities. The process provides the method for determining the facility security level (FSL) based on the characteristics of each facility and the federal occupant(s) who inhabit that facility. The five factors quantified to determine the FSL are *mission criticality*, *symbolism*, *facility population*, *facility size*, and *threat to tenant agencies*. After using the five factors, the assessor may then consider any intangibles that might be associated with the facility. An adjustment to the FSL may be made accordingly, and a final FSL is determined.

A representative of the tenant for single-tenant facilities or the Facility Security Committee (FSC), consisting of representatives of all federal tenants in a multi-tenant facility, determines the FSL for the facility. More information on FSCs can be found in *Appendix D: How to Conduct a Facility Security Committee*.

Once this phase is complete, countermeasures are applied appropriately to mitigate an undesirable event's impact. *The Design-Basis Threat: An Interagency Security Committee Report* (DBT), which is reviewed annually and updated as required, provides the threat scenarios, baseline threat, analytical basis, target attractiveness, and outlook for undesirable events that range from theft to active shooter. Tenant(s) use this information as they begin to select and implement appropriate countermeasures. Using the DBT provides a wide-ranging review of undesirable events the facility faces and provides guidance to assess the risk. Management officials and security organizations should reference the most current edition of the DBT, unless a threat-assessment publication is available that addresses undesirable events and is current and agency-specific. More information on the DBT can be found in *Appendix A: The Design-Basis Threat Report*.

The tenant(s) are responsible for addressing the facility-specific security issues addressed in the risk assessment. The tenant agency representative or the FSC approves the implementation of the security countermeasures and practices the security organization recommends. The implementation may be a combination of operational and physical security measures based on the FSL and the level of protection (LOP) that is deemed both appropriate and achievable. More information on the security countermeasures can be found in (FOUO) *Appendix B: Countermeasures*.

Once a facility's FSL and appropriate countermeasures have been assessed and determined, the tenant(s) and the security organization should refer to *Appendix E: Use of Physical Security Performance Measures*. In this appendix, they will see performance measurement cycles and find examples of performance metrics for physical security.

2.0 Background

This standard creates one formalized process for defining the criteria and process that shall be followed while determining the FSL of a federal facility, determining risks in federal facilities, identifying a desired level of protection, identifying when the desired level of protection is not achievable, developing alternatives, and—when necessary—accepting risk. This standard supersedes all previous guidance contained in the Department of Justice's report *Vulnerability Assessment of Federal Facilities*, published in 1995, and previously published Interagency Security Committee (ISC) standards that are contained within this document.

40 United States Code (U.S.C.) § 1315, the Presidential Policy Directive (PPD-21), and the National Infrastructure Protection Plan (NIPP) are foundational documents that codify the U.S. Department of Homeland Security's (DHS) responsibility for protecting buildings, grounds, and property that are owned, occupied, or secured by the federal government; establish U.S. policy for enhancing protection and resilience of the Nation's critical infrastructure; and provide a framework for integrating efforts designed to enhance the safety of critical infrastructure.

- 40 United States Code (U.S.C.) § 1315 vests the DHS Secretary with the authority and responsibility to "protect the buildings, grounds, and property that are owned, occupied, or secured by the federal government (including any agency, instrumentality or wholly owned, or mixed-ownership corporation thereof) and the persons on the property."
- The Presidential Policy Directive (PPD-21) on Critical Infrastructure Security and Resilience "advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure…. The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure— including assets, networks, and systems—vital to public confidence and the Nation's safety, prosperity, and well-being."
- The overarching goals of the NIPP are to build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of a terrorist attack or natural disaster and to strengthen national preparedness, response, and recovery in the event of an emergency.

3.0 Applicability and Scope

Pursuant to the authority of the ISC contained in Executive Order (E.O.) 12977, October 19, 1995, "Interagency Security Committee," and as amended by E.O. 13286, March 5, 2003, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* is applicable to all buildings and facilities in the United States occupied by federal employees for nonmilitary activities. These buildings and facilities include existing buildings, new construction, or major modernizations; owned-, to be purchased-, or leased-facilities; stand-alone facilities, federal campuses, and where appropriate, individual facilities on federal campuses; and special-use facilities.

Additionally, in December 2012, the Department of Defense (DoD) voluntarily and officially adopted *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* and integrated it into Unified Facilities Criteria (UFC) 4-010-01, DoD Minimum Antiterrorism Standard for Buildings. This criteria applies to all off-installation leased space managed by DoD and all DoD buildings owned or operated by GSA.

EO 12977 also requires the development of a strategy for ensuring compliance with standards. To meet this requirement, the ISC published the *Interagency Security Committee Compliance Benchmarks* and developed the ISC-Compliance System (ISC-CS). ISC-CS is a web-based application that collects and analyzes benchmark responses. Departments and agencies must report information through the system on an annual basis.

Critical infrastructure such as dams, tunnels, bridges, and national monuments are not normally considered to be federal facilities as defined in this document; they are generally identified as "high-risk symbolic or critical infrastructure" or by other designations as determined by the departments or agencies responsible for their protection, in accordance with guidance provided under the NIPP. Although this standard was not written with these structures in mind, the methodology upon which it is based may be applicable.

The threats addressed by this standard are primarily manmade. Hazards such as earthquakes, fires, or storms are beyond the scope of this document and are addressed in applicable construction standards, although many of the countermeasures identified will contribute to mitigating natural hazards. Further, this document assumes facility owners and operators including, but not limited to, facility tenants, security managers, and security organizations will implement countermeasures in full compliance with applicable sections of the United States Code (U.S.C.), Code of Federal Regulations (CFR), Federal Management Regulations (FMR), American Barriers Act Acceptability Standards (ABAAS), Americans with Disabilities Act Amendments Act (ADAAA) requirements, Occupational Safety and Health Administration (OSHA) regulations, Fire and Life Safety codes, and all applicable Executive Orders and Presidential Directives.

All users of the standard should clearly understand that there are no guarantees that even the best assessments, countermeasures, and procedures will protect federal facilities from potential threats. However, non-compliance with these ISC standards has the potential to leave federal agencies exposed to risks in protecting their workforce, visitors, and federal facilities. This standard does not replace specific agency security policies; it was developed to establish a standard risk-informed approach for developing, implementing, and evaluating protective measures all federal facilities can use to enhance the quality and effectiveness of security and protection. In those instances where the standard conflicts with agency policy, the more restrictive measures should be enforced.

In order to keep pace with the changing nature of the threat to federal facilities, this standard will be reviewed annually and updated as needed. Users of this document should visit the ISC website for relevant information that may affect this standard and other ISC documents related to the security of federal facilities. The 2021 edition of this document is a new document that does not invalidate prior decisions but should be applied to new facilities as new or recurring assessments and reviews of current FSLs are conducted.

4.0 Facility Security Level Determinations for Federal Facilities

The Facility Security Level (FSL) determination directs the user to a set of baseline standards that may be customized to address site-specific conditions. It applies to all federal facilities whether those facilities are government-owned or -leased or are in the process of construction, modernization, or purchase. It serves as the basis for implementing protective measures under other ISC standards. It is critical that departments and agencies recognize the security decision process is an integral part of overall facility management and real-estate acquisition processes. The security decision process must be fully integrated into the decision-making process to be most effective.

4.1 Making the Facility Security Level Determination

The initial FSL determination for newly leased or owned space will be made as soon as practical, after the identification of a space requirement, including succeeding leases. The FSL determination ranges from a Level I (lowest risk) to a Level V (highest risk). 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.

Risk assessments will be conducted once every five years for Level I and II facilities and once every three years for Level III, Level IV, and Level V facilities.[1] The FSL will be reviewed and adjusted, if necessary, as part of each initial and recurring risk assessment.

The responsibility for making the final FSL determination rests with the tenant(s) who must devise a risk management strategy and, if possible, fund the appropriate security countermeasures to mitigate the risk:

- For single-tenant facilities owned or leased by the government, a representative of the tenant[2] agency will make the FSL determination in consultation with the owning or leasing department or agency and the security organization responsible for the facility.
- In multi-tenant facilities owned or leased by the government, tenants (i.e., the Facility Security Committee), will make the FSL determination, in consultation with the owning or leasing department or agency and the security organization responsible for the facility.

When the security organization and the owner/leasing authority do not agree with the tenant agency representative or FSC with regard to the FSL determination, the ISC, as the representative of DHS, will facilitate the final determination through discussion with all relevant parties. ISC facilitation will begin after initiation through either a regional ISC representative or through direct communication with the ISC headquarters element. The FSL determination shall be documented, signed, and retained by all parties.

[1] Facilities not routinely occupied by federal employees do not require recurring security assessments. These facilities include locations not classified as buildings, such as antenna towers, parking spaces (not including complete parking structures), freestanding restrooms, and other similar facilities that cannot be regularly occupied. However, nothing prevents agencies from conducting such assessments.

[2] The representative of the tenant agency approved by the department or agency to make such determinations (e.g., the Director of Security might make all determinations to ensure consistency).

4.2 Basis for the Factors and Criteria

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). These criteria are explained in Section 4.4 of this standard. Presidential Policy Directive 21[3] (PPD-21), issued in February 2013, advances the "national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure." PPD-21 has three strategic imperatives, including the "capability to collate, assess, and integrate vulnerability and consequence information with threat streams and hazard information to… aid in prioritizing assets and managing risks to critical infrastructure… [and] recommend security and resilience measures for critical infrastructure prior to, during, and after an event or incident."

In 2007, Homeland Security Presidential Directive 20 (HSPD-20)[4] identified eight National Essential Functions (NEFs), 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 and other essential functions, are a part of determining the "value" of a facility to the government.

Finally, the threat to facilities from criminal elements must also be evaluated. Consideration must be given to the risk from more common criminal acts, such as theft, assault, violent civil disturbances, workplace violence, and vandalism—acts that historically occur more frequently at federal facilities than acts of terrorism.

These concepts have been incorporated into determining the factors and criteria established in this standard.

4.3 Facility Security Level 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 the criteria used to evaluate each factor and assign points. However, the criteria cannot capture all of the circumstances that could be encountered. Thus, the standard includes a sixth factor—intangibles—to allow the assessor to consider other factors unique to the department or agency needs or to the facility.

Assessment-specific judgment has been reduced to the extent possible, but it may still be necessary. To that end, this document includes an explanation of why each factor was included, a description of its intended impact on the score, and examples to allow security professionals encountering conditions that do not clearly match those anticipated here to make an informed decision based on the same rationale used in the development of this process.

To use the FSL matrix, each of the factors is examined and a point value is assigned based on the provided scoring criteria. The points for all factors are then added 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, thus determining the final FSL. If an adjustment to the FSL is made, it must be documented accordingly.

---

[3] See https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, accessed 3 November 2015.

[4] National Security Council, Homeland Security Presidential Directive-20, Washington D.C.: Executive Office of the President, 2007.

Table 1: Interagency Security Committee Facility Security Level Determination Matrix

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

Note: For information on Level V facilities refer to Section 4.5.

4.4 Facility Security Level Scoring Criteria

4.4.1 Mission Criticality

The value of a facility to the federal government is based largely on the facility's mission, particularly as it may relate to NEFs and other examples of government activities listed below. As vital as it is for the government to perform these activities, it is equally attractive to adversaries to disrupt important government missions. The mission criticality score is based on the criticality of the missions carried out by federal tenants in the facility (not by the tenant agencies overall). In a multi-tenant or mixed multi-tenant facility, the highest rating for any federal tenant in the facility should be used for this factor. Continuity of Government (COG) and Continuity of Operations (COOP) documents are good sources of information

regarding the performance of essential functions. The security organization cannot determine the tenant's mission criticality on its own. This factor is decided by the tenant.

Table 2: Mission Criticality

Value	Points	Criteria	Examples
Very High	**4**	National leadership, seats of constitutional branches. Houses chief officials for a branch of government	White House, the US Capitol building, the Supreme Court building
		Communications centers that support national essential government functions	White House Communications Agency facilities
		Houses essential communications, workstations, electronic equipment, or hardcopy documentation necessary for defense or intelligence activities	Intelligence community facilities, including communications; Top Secret information, and weapons/munitions storage
		Houses individuals necessary to advance American interests with foreign governments.	U.S. Department of State headquarters
		Houses government officials of foreign nations	Foreign embassies and consulates in the United States
		Houses individuals or specialized equipment necessary to identify and analyze threats to homeland security. Conducts comprehensive criminal investigative work involving high profile crimes	U.S. Coast Guard, ports of entry, Joint Terrorism Task Force and Counter-drug Task Force activities, intelligence-gathering locations, Fusion Centers, etc.
		Houses personnel or specialized equipment necessary to identify or respond to large-scale or unique incidents or is an identified COG facility	Emergency operations centers, national response assets (e.g., Nuclear Emergency Support Teams), COG facility (as defined in Federal Continuity Directive-1)
		Houses personnel or specialized equipment essential to regulating national fiscal or monetary policy, financial markets, or other economic functions	U.S. Department of Commerce building, FEMA Emergency Operations Center
		Contains currency, precious metals, or other materials necessary to maintain economic stability	U.S. Mint facilities, Federal Reserve buildings
		Houses specialized equipment necessary to process or monitor financial transactions necessary for the Nation's economy	National financial centers

Value	Points	Criteria	Examples
Very High (Cont'd)	**4**	Houses personnel or specialized equipment necessary to detect or respond to unique public health incidents	Centers for Disease Control and Prevention
		Houses personnel, specialized equipment, or maintains operations affecting the strategic capability for the defense of the United States	Nuclear-related missions
		Houses material or information that, if compromised, could cause a significant loss of life, not limited to, but including production quantities of chemicals, biohazards, explosives, weapons, etc.	U.S. Department of Energy research reactor facilities, explosives storage facilities
		COG facilities	Federal Emergency Management Agency Emergency Operations Center
High	**3**	Original, irreplaceable materials or information central to the daily conduct of government	National Archives
		Houses personnel or material necessary for the development of defense systems	Facilities used to produce tanks, aircraft, etc. at which federal employees are assigned
		Designated as a shelter in the event of an emergency incident	Smithsonian museums
		Regional or headquarters policy and management oversight	GSA National Capitol Region headquarters, Social Security Administration headquarters, Census Bureau
		Biological/chemical/radiological/medical research or storage of research and development (de minimis) quantities of chemicals, biohazards, explosives, and similar items	Animal Disease Research Center
		COOP facilities for department and agency headquarters	GSA Central Office COOP facility

Value	Points	Criteria	Examples
High (Cont'd)	**3**	General criminal investigative work	Fraud, financial, non-terrorism-related crime
		Houses personnel, specialized equipment, or maintains activities affecting the tactical or operational capability for the defense of the United States	Special Operations, Deployment-related activities
		Judicial processes	Federal courts
Medium	**2**	District or State-wide service or regulatory operations	Agriculture Food Safety and Inspection Services District Office
		Houses personnel, specialized equipment, or maintains activity affecting the defense infrastructure of the United States	Financial or human resource operations, medical operations, Fisher House, Defense Industrial Activities.
		COOP facilities for other than national headquarters	GSA Regional Office COOP site
Low	**1**	The loss, theft, destruction, misuse, or compromise of activities or operations that would have an minimal impact on the defense of the United States; or would only affect defense missions on a regional level	Administrative support operations
		Administrative, direct service, or regulatory activities at a local level	Agricultural County Extension Office

4.4.2 Symbolism

The facility's symbolism is based on both its attractiveness as a target and the consequences of an event. The symbolic value is first based on external appearances or well-known/publicized operations within the facility that indicate it is a U.S. Government facility. Transnational terrorists often seek to strike at symbols of the United States, democracy, defense, and capitalism. Domestic extremist groups or individuals may seek to make a statement against government control, taxation, policies, or regulation.

Symbolism is also important because of the potential negative psychological impact of an undesirable event. Attacks at certain government facilities, particularly those perceived to be well-protected and central to the United States' safety and well-being, could result in a loss of confidence in the U.S. Government domestically or internationally.

Even if a mixed-tenant or mixed multi-tenant facility has no external appearances or contains no well-known operations of the U.S. Government, it may still be symbolic to terrorists. Facilities such as financial institutions, communications centers, transportation hubs, and controversial testing laboratories may be symbolic in the eyes of single-interest domestic extremist groups or international terrorist organizations, whose leaders have stated that strikes against the American economy are a high priority. The symbolism

of non-U.S. Department of Defense (DOD) federal facilities on a DOD campus should be assessed similarly.

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

Table 3: Symbolism

Value	Points	Criteria	Examples
Very High	**4**	Popular destination for tourists	Smithsonian museums
		A nationally significant historical event has occurred at the facility	Independence Hall
		Widely recognized to represent the Nation's heritage, tradition, or values	White House, U.S. Capitol, Supreme Court building
		Contains significant original historical records or unique artifacts that could not be replaced in the event of their damage or destruction	National Archives Museums, Smithsonian museums
		Executive department headquarters building	U.S. Department of Justice, Department of Transportation headquarters
		Other prominent symbols of U.S. power or authority	U.S. Circuit, District, or Bankruptcy Courthouses, Central Intelligence Agency headquarters
High	**3**	Well-known, regional U.S. Government facility	Oklahoma City Federal Building
		Agency/bureau headquarters	GSA Central Office, Environmental Protection Agency headquarters, Social Security Administration headquarters
		Houses large numbers of personnel (over 100) required to wear uniforms, representing the U.S. Government	Military or federal law enforcement personnel
		A facility that is perceived to be well-protected	Military installation

Value	Points	Criteria	Examples
High (Cont'd)	**3**	Located in a symbolic commercial financial building	International trade centers, regional or nationwide bank headquarters building
		Co-located with other non-governmental but highly symbolic facilities	Transportation hubs
Medium	**2**	Readily identified as a U.S. Government facility based on external features	Signage stating "Federal Office Building," Great Seal of the United States, seals of departments and agencies on exterior
		Readily identified as a U.S. Government facility based on the nature of public contact or other operations (even without external features)	Social Security Administration field office
		Readily identifiable, non-facility assets located at site	Large fleet of federal government vehicles, military equipment
		Dominant, single federal facility in a community or rural area	U.S. Department of Veterans Affairs clinic
		Non-governmental commercial laboratory or research facility symbolic to single-interest extremists	Animal testing facility
Low	**1**	No external features or public contact readily identifying it as a U.S. Government facility	Classified locations, small offices in leased commercial buildings

4.4.3 Facility Population

Many terrorist organizations aim to inflict mass casualties. Pre-operational surveillance reports recovered from terrorists include considerable details on when a facility's population is at its highest number. These reports do not distinguish between tenants and visitors. From a consequence perspective, the potential for mass casualties should be a major consideration.

Thus, the facility population factor is based on the number of personnel in federally occupied space, including occupants and visitors. This number should not include such transient influxes in population as an occasional conference (or similar event), unless the facility is intended for use in such a manner (such as a conference center) and the population is part of normal business. Transient shifts in population such as the occasional conference should be addressed by contingency security measures.

The average number of visitors in the facility at any given time not to exceed the facility's maximum capacity should be used to determine the visitor population. Ideally, visitor population would be achieved by providing a review of visitor logs or access control lists; however, it may necessitate an estimate or a short-term sampling of visitor traffic. Facilities such as standalone parking garages should be considered to have a scoring value of "low."

The sensitive nature of child-care centers (CCC) located in federal facilities requires every federal CCC or facility with a CCC to receive a facility population value of "very high."

If the non-federal population of a mixed-tenant or mixed multi-tenant facility contributes to the target attractiveness (e.g., creates a substantial population over and above the federal population), document the rationale and add 1 point, not to exceed the maximum of 4 points.

Table 4: Facility Population

Value	Points	Criteria
Very High	**4**	Greater than 750 people or facilities with CCCs
High	**3**	251 to 750 people
Medium	**2**	101 to 250 people
Low	**1**	Less than 100 people

4.4.4 Facility Size

The facility size factor is based on the square footage of all federally-occupied space in the facility, including cases where an agency with real property authority controls some other amount of space in the facility. If the entire facility or entire floors are occupied, gross square footage should be used (length multiplied by width); if only portions of floors are occupied in a multi-tenant facility, assignable or rentable square footage should be used. Size may be directly or indirectly proportional to the facility population. An office facility with a large population will generally have a correspondingly large amount of floor space; however, a large warehouse may have a very small population.

For a terrorist, an attack on a large, recognizable facility results in more extensive media coverage. However, large facilities require a more substantial attack to create catastrophic damage. The extensive preparation and planning required to execute a substantial attack could deter adversaries. From a consequence perspective, the cost to replace or repair a large facility is a major consideration. The NIPP considers the cost to rebuild a facility in determining the potential economic impact of a successful attack.

If the total size of a mixed-tenant or mixed multi-tenant facility beyond that occupied by the federal population contributes to the target attractiveness (e.g., creates a highly recognizable structure based on size alone), document the rationale and add one point, not to exceed the maximum of four points.

Table 5: Facility Size

Value	Points	Criteria
Very High	**4**	Greater than 250,000 square feet
High	**3**	100,001 to 250,000 square feet
Medium	**2**	10,001 to 100,000 square feet
Low	**1**	Up to 10,000 square feet

4.4.5 Threat to Tenant Agencies

The next factor in FSL calculation is the threat to tenant agencies, which includes the following considerations:

- Nature of federal tenant's contact with the public: Is the federal tenant's interaction with the public typically adversarial in nature?
- Nature of the federal tenant's mission at the facility: Is the federal tenant's mission at this facility controversial in nature and does it draw the attention of any type of credible threat?
- Past and current credible threats to the federal tenant(s) at the facility: What is the history of credible threats? Are there current credible threats to the federal tenant(s)?
- Past and current credible threats to any of the tenants in the facility that pose a threat to the federal tenant(s): What is the history of credible threats? Are there current credible threats to non-federal tenants? Do those threats affect the security of federal tenants?
- Crime statistics: Based on local, county, state, and federal crime statistics, is this facility located in a high, moderate, or low crime area?

With these five considerations in mind, the threat to tenant agencies is determined based on Table 6: Threat to Tenant Agencies. For a multi-tenant facility, the highest value of any one federal tenant should be used for the FSL calculation. For a mixed-tenant or mixed multi-tenant facility for which the threat to non-federal tenants affects any federal tenant, the value should consider that threat and use the highest applicable value.

When selecting a value, this factor should not be confused with any federal agency-specific threat levels. Although those threat levels may inform the selection of a value, they should not be the only criterion used for the FSL calculation.

When determining whether a facility is in a high, moderate, or low crime area, one should use the following guidelines for gathering and analyzing crime statistics:

- The crime statistics used should never be limited to only crimes committed at, on, or in the facility.
- When available, use crime statistics for the prior 24 months.

- For large cities and urban areas with a population exceeding one million, use crime statistics for a radius up to two miles from the facility.
- In smaller cities with a population exceeding 100,000 up to one million, use crime statistics for the entire city.
- In suburban and rural areas with a population less than 100,000, use crime statistics for the zip code, county, or other relevant criteria based on the availability of local statistics.

Table 6: Threat to Tenant Agencies

Value	Points	Criteria	Examples
Very High	**4**	Tenant mission and interaction with certain segments of the public is adversarial in nature	Criminal and bankruptcy courts, high-risk law enforcement, including those who routinely contact or attract the attention of dangerous groups (Federal Bureau of Investigation, Drug Enforcement Agency, Bureau of Alcohol, Tobacco, Firearms and Explosives, U.S. Courts (including administrative courts of federal agencies) hearing high profile, controversial, high threat or cases that impact a large number of individuals (i.e., Narcotics-trafficking, terrorism, potentially controversial matters, deportation).
		Tenant mission is controversial in nature and routinely draws the attention of organized protesters	Environmental Protection Agency, Department of Energy, Courthouses, World Banks
		Located in a high-crime area	As determined by a characterization established by local law enforcement
		Significant history of violence directed at or occurring in the facility. More than ten incidents per year requiring law enforcement/security response/investigation for unruly or threatening persons	As determined by security organization or tenant incident records
High	**3**	Public contact is occasionally adversarial based on the nature of business conducted at the facility	Non-criminal/administrative courts where privileges or benefits may be suspended or revoked, general law enforcement operations, National Labor Relations Board offices
		History of demonstrations at the facility	U.S. Department of State headquarters
		Located in a moderate-crime area	As determined by a characterization established by local law enforcement

Value	Points	Criteria	Examples
High (Cont'd)	**3**	History of violence directed at the facility or the occupants; five to ten incidents per year requiring law enforcement/security response/investigation for unruly or threatening persons onsite	As determined by security organization or tenant incident records
Medium	**2**	Generally non-adversarial public contact based on the nature of business conducted at the facility History of demonstrations against the tenant agency (not at the facility) Located in a low-crime area History of violence directed at tenant agencies/companies (not at the facility).	General/internal Investigations, inspection services for the U.S. Department of Agriculture, Department of State Passport Office U.S. Nuclear Regulatory Commission, U.S. Citizenship and Immigration Services As determined by a characterization established by local law enforcement Internal Revenue Service, Social Security Administration offices
Low	**1**	Generally little-to-no public contact No history of demonstrations at the facility Located in an area with very low crime No history of violence directed at the facility or the occupants	Government warehouses or storage facilities, Federal Trade Commission As determined by security organization or tenant incident records As determined by crime statistics analysis guidance above As determined by security organization or tenant incident records

4.4.6 Intangible Factors

It is impossible for this document to take into account all the conditions that may affect the FSL decision for all federal departments and agencies. Certain factors, such as a short duration of occupancy, may reduce the value of the facility in terms of investment or mission that could justify a reduction of the FSL. Such factors are in essence indicative of a reduced value of the facility itself and a corresponding reduction in the consequences of its loss.

Other factors may suggest an increase in the FSL, such as the potential for cascading effects or downstream impacts on interdependent infrastructure or costs associated with the reconstitution of the facility.

Accordingly, the FSL may be raised or lowered one level at the discretion of the deciding authority based on intangible factors. However, the intangible factors should not be used to raise or lower the FSL in response to a particular threat act. The FSL characterizes the entire facility; 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. For example, a weeklong conference may increase the population of a facility substantially during the conference, but it should not be considered in the FSL determination. On the other hand, if the facility is a conference center that normally holds such gatherings, the population during those conferences should be factored into the FSL.

Like all risk management decisions, it is important to document these intangible factors and the resulting adjustments made to the FSL score. The decision-making authority should document any intangible factors and the associated adjustment and retain this information as part of the official facility security records.

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.

4.5 Level V Facilities

Although the incorporation of additional factors and criteria makes this standard more useful to determine the FSL for special-use and other unique facilities, such as high-security laboratories, hospitals, or unique storage facilities for chemicals or munitions, some facilities may still not fit neatly into the criteria defined here. The mission's criticality or the facility's symbolic nature could be such that it merits a degree of protection above that specified for an FSL Level IV facility, even though the other contributing factors, such as population or square footage, might be scored lower.

For example, a research laboratory might receive lower score values for symbolism, square footage, and population size. However, the laboratory may be responsible for critical research and diagnostic activities vital to protecting the Nation's citizenry or animal and food products from disease agents accidentally or deliberately introduced into the United States. This mission, combined with the fact that it may be the only such laboratory in the country, would suggest the criticality factor would far outweigh lower score values in symbolism, population, and/or facility size, and thus the facility should be considered for a Level V designation. As a result, the criteria and decision-making authority for identifying Level V facilities are within the purview of the individual agency. As general guidance, agencies should consider a facility as potentially suitable for a Level V designation if it receives a "very high" score value for mission criticality or symbolism and is a one-of-a-kind facility (or nearly so).

4.6 Campuses, Complexes, and Federal Centers

A campus consists of two or more federal facilities located contiguous to one another that share some aspects of the environment (e.g., parking, courtyards, vehicle access roads, or gates) or security features (e.g., a perimeter fence, guard force, or onsite central alarm/video surveillance system [VSS] monitoring station). A campus may also be referred to as a "complex" or "federal center."

In the case of a campus housing a single tenant, such as the DHS headquarters campus or the Social Security Administration's headquarters campus, an overall FSL may be established. In multi-tenant campuses, all individual facilities in the campus will either be assigned an FSL in accordance with this

standard, or all tenants may agree to determine an overall FSL for the entire campus by treating the entire campus as though it were a multi-tenant facility (using the highest rating of any tenant in the facility for each factor).

4.7 Changes in the Facility Security Level

Changes in the environment at the facility, particularly when tenants move in or out, could result in changes in the scoring for the various factors. A small change to the population (such as an increase from 150 to 151 employees) could result in a change to the population score. The use of multiple factors in making the FSL determination somewhat dilutes the effect of any one factor and all but prevents a small change from causing a change in security level. However, the nature of the tenant (i.e., the criticality of the mission or risk associated with the agency itself) moving in or out may also affect the FSL.

It may be impractical to adjust the FSL every time a tenant moves in or out of a multi-tenant facility; instead, the FSL will be reviewed at least as part of the regularly recurring risk assessment and adjusted as necessary. Major changes in the nature of the tenants should merit consideration of whether to review and potentially adjust the FSL between the regularly scheduled assessments.

The requirement for recurring risk assessments may in some cases make the argument for a federal facility to install or retain temporary perimeter security measures rather than permanent installations, given that the risk may decrease later, particularly if the facility tenant mix is likely to change.

4.8 Co-location of Tenants with Similar Security Needs

Establishing an FSL that is agreeable to all the tenants in a multi-tenant facility is especially challenging when tenants do not have similar security requirements, such as when a high-risk law enforcement entity is located in the same facility as a low-risk administrative entity. For this reason, the ISC recommends that compatible tenants —those with similar security concerns and requirements—should be co-located whenever possible, and incompatible tenants should not. This principle should be applied by all agencies with real property authority.

The factors of mission criticality and threat to tenant agencies should be primary considerations in determining compatible tenants. Additionally, although it is not explicitly considered above, the volume of public contact for various tenants is also a concern, especially where visitor-screening may become a requirement.

Co-location has traditionally been a difficult issue in smaller communities where there is only one federal facility. Generally, small communities with only one federal facility results in the co-location of tenants with differing security requirements. When this happens, agencies with higher security requirements often request separate space where they can be the sole tenants. Although this decision may come at a great cost, it is a risk-management decision for the tenant agency. Locating a high-risk tenant in a separate facility reduces the threat to the other tenants, reduces the cost of security to all but the tenant that requires it, and ensures that the high-risk tenant can achieve the higher security posture it merits.

A tenant requiring a higher level of security should not be moved into a facility with a low security level. A pre-lease assessment should be conducted before a tenant moves into a new or existing facility. Such a move would result in either the higher-risk tenant accepting less security than it requires, or the lower-risk tenants having to accept and share the cost of a higher level of security than they require. Even if an alternative is to allow the higher-risk tenant to pay for any increased security measures required, the

operational impacts upon the other agencies have to be considered (e.g., the implementation of extensive visitor screening procedures may adversely affect a tenant with a high volume of public contact).

The onus is not just on the agency with real property authority that facilitates the relocation; it is shared by agencies seeking to relocate. By agreeing to occupy a space, the agency is agreeing to the level of security established for that facility and any operational or cost impacts associated with maintaining it, as well as any security language included in the lease.

5.0 Integration of Countermeasures

Note: ***Appendix B: Countermeasures*** **to this standard contains specific examples regarding the steps noted in this section, as well as the security criteria tables. Appendix B is marked For Official Use Only (FOUO) and is available upon request from and approval by the Office of the Interagency Security Committee at** ISCAccess@hq.DHS.gov.

The integration of *Appendix B: Countermeasures* is predicated on an FSL designation. Once an FSL is determined, departments and agencies will use the following decision-making process resulting in either:

- The application of the baseline LOP applicable to the facility's FSL; or
- The application of a customized LOP to address facility-specific conditions.

Integration of countermeasures to the risk management process ensures the use of a comprehensive approach to meet federal facility security needs in today's threat environment. Integration also ensures that the scope of security countermeasures is commensurate with the risk posed to a facility. Figure 5-1, Risk Management Process, depicts the steps required to apply the countermeasures and identifies the sections (5.1 through 5.1.13) that explain each step. The objective of this risk management process is to identify an achievable LOP commensurate with—or as close as possible to—the level of risk without exceeding the level of risk.

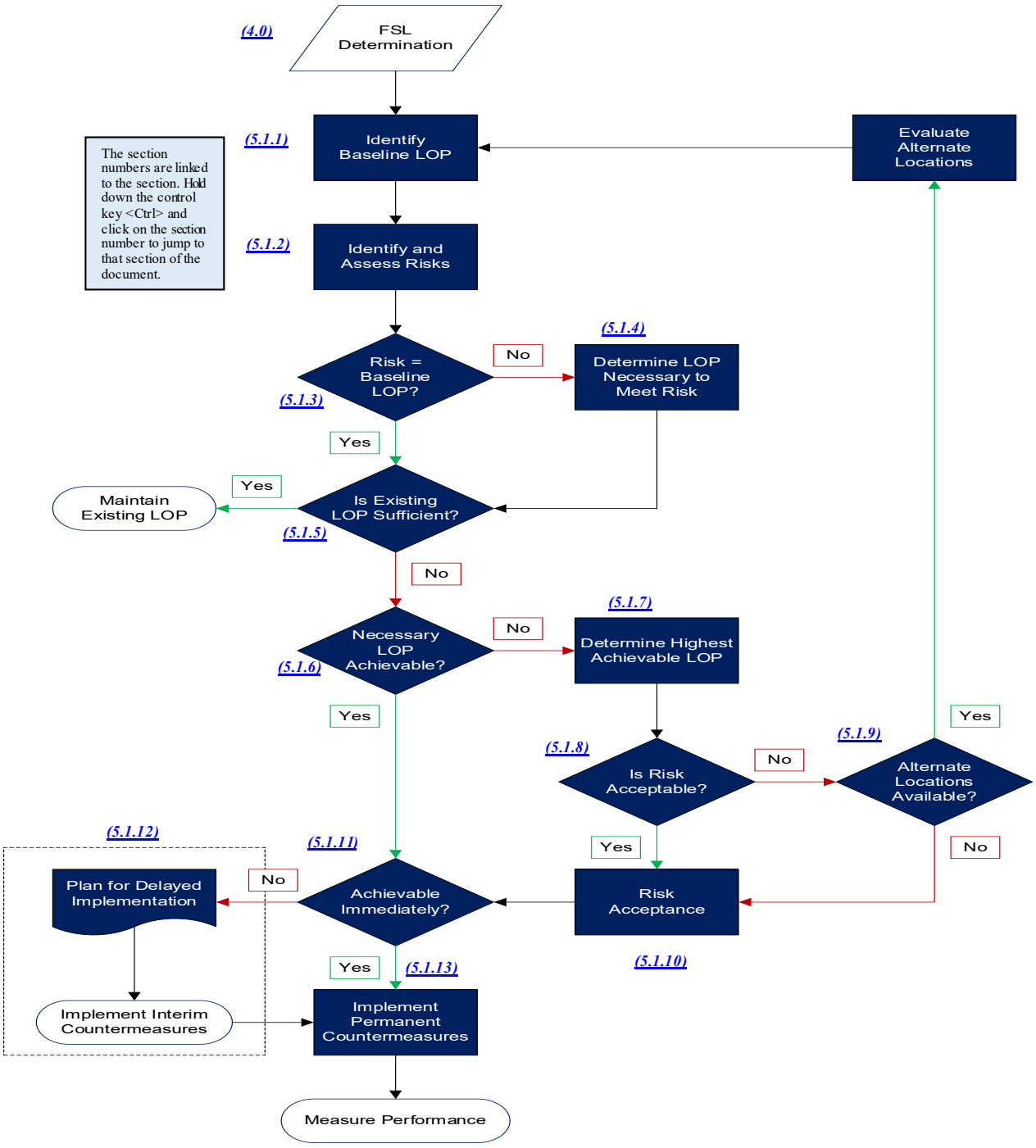

Figure 5-1: Risk Management Process

5.1 How to Apply Countermeasures

5.1.1 Identify Baseline Level of Protection

Each FSL corresponds to a level of risk that relates directly to an LOP and associated set of baseline security measures. Comparatively speaking, Level I facilities face a minimum level of risk, and thus the baseline LOP for a Level I facility is Minimum; Level II corresponds to Low; Level III to Medium; Level IV to High; and Level V to Very High (see Table 7 below).

Table 7: Relationship between Facility Security Level, Risk, and Level of Protection

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

Appendix B: Countermeasures (FOUO) contains the Security Criteria tables, which lists security measures for each level and criterion. Figure B-2 in *Appendix B: Countermeasures* provides an example of the columns containing countermeasures aligned to each LOP. By using the applicable countermeasures to a given FSL, a baseline LOP for a facility can be derived.

5.1.2 Identify and Assess Risks

The risks to a facility must first be identified and assessed in order to determine if the baseline LOP is sufficient or if customization is required.

Appendix A: The Design-Basis Threat Report provides a broad range of undesirable events that may impact federal facilities. Regardless of the level of effort involved in the identification and assessment of risk, the analysis must consider all of these undesirable events. In assessing actual risks at the facility, the variance of the risk from the baseline is identified as shown in *Appendix B: Countermeasures*, Figure B-4.

Risk is a function of the values of threat, consequence, and vulnerability. The objective of risk management is to create a level of protection that mitigates vulnerabilities to threats and their potential consequences, thereby reducing risk to an acceptable level. A variety of mathematical models are available to calculate risk and to illustrate the impact of increasing protective measures on the risk equation.

For the purposes of this standard, the assumption is made at this step of the process that there are no countermeasures in place and complete vulnerability exists. In a new construction project, that is the case; for existing buildings, the existing LOP — and the remaining actual vulnerability — will be assessed in Section 5.1.5. This approach is necessary to ensure all security criteria will be considered as the process is completed. This approach also helps define the relationship between the level of risk and the LOP. The

level of risk must be mitigated by a commensurate LOP. A high level of risk, for example, must be mitigated by implementing a high LOP.

The assessment of risk in this step does not necessarily entail a comprehensive on-site risk assessment. For existing facilities, site visits are beneficial. For a new construction or a new lease, no facility may yet exist, and thus the assessment would be based on a conceptual facility design or set of requirements.

The ISC or implementation of countermeasures does not mandate the use of a specific risk assessment methodology. The methodology, software tools, training, and personnel requirements may be unique to the agency. The methodology chosen should adhere to the fundamental principles of a sound risk assessment methodology:

- The methodology must be credible and assess the threat, consequences, and vulnerability to specific acts.
- The methodology must be reproducible and produce similar or identical results when applied by various security professionals.
- The methodology must be defensible and provide sufficient justification for deviation from the baseline.

In practice, various methodologies provide varying outputs, from numbers and percentages to qualitative ratings such as "low" or "green." Each department or agency must determine what outputs from their respective methodologies correlate with each enumerated LOP.

The facility's security organization will conduct a risk assessment to identify risk(s). When a facility does not have an assigned security organization or federal tenant with a law enforcement or security element housed in the facility, the tenant agency representative or FSC shall select a federal department or agency to provide the services of the security organization. When a facility has one federal tenant with law enforcement or security function housed in the facility, this entity may be selected as the security organization for the facility. When a facility has two or more federal tenants with a law enforcement or security function, the tenant agency representative or FSC should select a lead federal tenant to serve as the security organization. Once risks have been identified and assessed, continue to Section 5.1.3.

5.1.3 Decision Point: Are Risks Adequately Addressed by the Baseline Level of Protection?

Levels of risk determined for each undesirable event should be mitigated by countermeasures that provide a commensurate LOP: the higher the risk, the higher the LOP. The FSL determination is an estimation of the level of risk at a facility. The baseline LOP is intended to mitigate that estimated risk.

The security organization should determine whether the countermeasures contained in the baseline LOP adequately mitigate known or anticipated risks to the facility. The baseline LOP may be too high (more stringent than necessary) or too low (leaving a vulnerability unmitigated), compared to the level of risk.

⇧ If the baseline LOP adequately addresses the risk(s), plan to implement all of the baseline countermeasures for the LOP. **Go to Section 5.1.5.**

- or -

⇩ If the baseline LOP does not appropriately address the risk (too high or too low), the necessary LOP must be determined. **Continue to Section 5.1.4.**

If, in assessing the risks of various undesirable events, it is determined the actual risks the facility faces are predominantly higher or lower than the FSL, the FSL determination should be re-examined.

5.1.4 Determine the Level of Protection Necessary to Adequately Mitigate Risk(s)

Variations in a facility's mission, location, and physical configuration may create unique risks or risks that are relatively higher or lower in some cases than at other facilities with the same FSL. The baseline LOP may not address those risks appropriately. It may provide too little protection (e.g., the baseline LOP is medium, but the assessed risk to theft is very high), thus leaving an unmitigated risk. Conversely, it may provide more protection than is necessary (e.g., the baseline LOP is medium, but the assessed risk to robbery is minimum), resulting in the expenditure of resources where they are not needed. Unnecessary expenditure might reduce the availability of resources that could be applied elsewhere.

Unmitigated risk and waste can be negated by determining the necessary LOP according to a risk assessment. Excess resources in one risk area can then be reallocated to underserved areas, thus ensuring the most cost-effective security program is implemented.

The tables in *Appendix B: Countermeasures* (FOUO) identify the countermeasures generally considered applicable to mitigate the risk from a particular undesirable event. The matrix identifies a generic set of undesirable events that may impact federal facilities and relates them to applicable security measures. An undesirable event is an incident that adversely impacts the facility's occupants or visitors, the facility's operation, or the agency's mission. Note that this is not a legal definition; rather, it serves to establish a conceptual scenario for consideration in identifying applicable countermeasures.

The list of undesirable events is not all inclusive. Unique facilities may face other mission-specific threats. For events not identified in the tables in the *Appendix B: Countermeasures* (FOUO), the ISC recommends agencies add customized undesirable events and either relate them to countermeasures in the tables or develop a specialized set of countermeasures for the additional events (in addition to those included in this standard). For example, a biological research laboratory may establish tables to address contamination events and identify corresponding containment measures.

For each undesirable event where the assessed risk is either less than or greater than the baseline LOP, the security organization must identify the appropriate countermeasures that will provide an LOP equivalent to the level of risk. Level I—Minimum countermeasures are typically less stringent but may also be less effective in mitigating higher risks, whereas Level V—Very High countermeasures are typically more stringent and generally more effective.

⇧ If the assessed risk is higher than the baseline LOP, select countermeasures from a higher LOP.

- or -

⇩ If the assessed risk is lower than the baseline LOP, select countermeasures from a lower LOP.

A minimum level of risk should be mitigated by countermeasures from the Level I-Minimum column, a low level of risk should be mitigated by countermeasures from the Level II-Low column, and so on. By determining the appropriate countermeasures applicable to the assessed risks and by identifying changes from the baseline LOP, the necessary LOP can be developed. **Continue to Section 5.1.5.**

5.1.5 Decision Point: Is the Existing Level of Protection Sufficient?

Once the LOP necessary to meet the risk is identified, an evaluation of current conditions must be made to identify the existing countermeasures. In the cases of new construction or of developing a lease specification in a new facility, there are no existing countermeasures to evaluate and thus no existing LOP. **Continue to Section 5.1.6.**

The existing LOP may be determined by site surveys, interviews, reviews of policies and procedures, "red team" testing, tabletop exercises, and so on to determine the countermeasures currently in place and their level of effectiveness. Current conditions may then be matched up against the countermeasure criteria tables in *Appendix B: Countermeasures* (FOUO). The existing LOP is then compared to the necessary LOP to determine if it adequately addresses the threat(s), or if vulnerabilities need to be addressed.

⇧ If the existing LOP aligns with the necessary LOP, current countermeasures should be maintained and tested on a regular basis. Conditions at the facility should be monitored for changes that may impact the effectiveness of countermeasures or the needed LOP.

- or -

⇩ If the existing LOP does not sufficiently address the risks, shortfalls must be identified and countermeasures must be considered for implementation to address those vulnerabilities. **Continue to Section 5.1.6.**

At this stage, several determinations are involved. These determinations are presented in order of production as follows: FSL/Baseline Risk; the Baseline LOP; Assessed Risk; Necessary Risk; and Existing LOP. Each of these determinations is meant to show the security posture of the facility.

5.1.6 Decision Point: Is the Level of Protection Achievable?

If the existing LOP is insufficient, the tenant(s) in coordination with the security organization and the owning/leasing entity must decide whether the LOP can be achieved. Specifically, they must decide if implementation of countermeasures is feasible and if the investment is cost-effective. Cost-effectiveness is based on the investment in the countermeasure versus the value of the asset. In some cases, investment in an expensive countermeasure may not be advisable because the lifecycle of the asset has almost expired. In addition, consideration should be given to whether other countermeasures may take priority for funding.

Cost-effective is a different determination than "cost-prohibitive." A countermeasure is cost-prohibitive if its cost exceeds available funding. Funding may exist for a countermeasure, but it may not be a sound financial decision to expend that money for little gain.

New construction—with few exceptions—is fully expected to meet the LOP. In some cases, site limitations may restrict standoff distances, or fiscal limitations may prohibit the implementation of some measures. Both examples illustrate why the security requirements should be identified as early in the process as possible (see Section 5.2.1). During the design process, there is a point where design changes are cost-prohibitive and make the LOP unachievable.

During the lease process, it may be decided available facilities in the delineated area cannot meet the requirements of the LOP. This decision may be determined by providing a market survey or when responses to a solicitation do not meet the requirements specified to meet the LOP. In an existing leased facility, the terms of the lease might not allow the implementation of certain countermeasures that impact the entire facility.

In an existing facility, physical limitations and budgetary restrictions may make the LOP unachievable. For example, additional standoff distance might not be available; upgrade of window systems to resist blast loads might require complete renovation of the façade so the window system will stay attached to the walls and thus be cost-prohibitive; or the current design of the air handling system could prohibit relocation of air intakes to a less vulnerable area.

Cost considerations could also be a primary factor in a decision not to implement a recommended countermeasure or a decision to defer a funding request until such time as the likelihood of obtaining funding is more favorable. This standard does not mandate the use of a specific cost-analysis methodology. However, all costs, including life-cycle costs, shall be considered in whatever cost-analysis methodology is used. In addition to direct project costs, costs associated with indirect impacts (e.g., business interruption, relocation costs, or road closures) should be considered. Any decision to reject implementation outright or defer implementation due to cost (or other factors) must be documented—including the acceptance of risk.

⇧ If the appropriate LOP is achievable, a timetable for implementation must be considered. **Go to Section 5.1.11**.

- or -

⇩ If the appropriate LOP is not achievable, the highest achievable LOP must be identified. **Continue to Section 5.1.7.**

5.1.7 Determine the Highest Achievable Level of Protection

If the tenant agency representative or FSC determines the necessary LOP cannot be implemented, the highest achievable LOP must be identified. Identification of the highest achievable LOP may require an iterative process of examining the countermeasures included in the next lower LOP, determining if that level is achievable, and, if not, repeating the process with the next lower LOP. This approach minimizes the amount of risk that might be accepted.

For example, an assessment may determine the risk of a hazardous substance being introduced into ground-level air intakes may be high. The associated Level IV High LOP may call for the air intakes to be relocated to the rooftop or a high wall. In an existing federal facility, the configuration of the air-handling system may make a retrofit cost-prohibitive or even physically impossible. In a lease process, it might be determined during the market survey that no facilities in the delineated area have such a configuration. The Level III Medium LOP calls for monitoring the ground-level air intakes with VSS and guard patrols. If technologically and financially feasible or available within the delineated market area, the Level III Medium LOP would be considered for implementation.. The project documentation must clearly reflect any reason why the necessary LOP cannot be achieved. **Continue to Section 5.1.8.**

5.1.8 Decision Point: Is the Risk Acceptable?

If the necessary LOP cannot be achieved, consideration must be given to the amount of risk that would be accepted given the highest achievable LOP. The difference between the protection afforded by the necessary LOP and the reduced protection afforded by the achievable LOP is the risk that must be accepted.

It is impossible to establish a rule-of-thumb identifying how many LOPs below the necessary LOP is acceptable. Specific conditions—site, budget, political— will dictate the achievable LOP in each situation.

The amount of risk to be accepted must be minimized through the deliberate process described here. Regardless of site conditions, the LOP implemented may never be less than Level I Minimum.

⇧ If the amount of risk left unmitigated by the highest achievable LOP is acceptable, **go to Section 5.1.10.**

- or -

⇩ If the amount of risk left unmitigated by the highest achievable LOP is not acceptable, **continue to Section 5.1.9.**

5.1.9 Decision Point: Are Alternate Locations Available?

If the necessary LOP cannot be achieved and the remaining risk at the highest achievable LOP is not acceptable, consideration must be given to identifying an alternate location where the necessary LOP can be achieved (including the possibility of a new lease construction or expanding the delineated area). Inherent in this process is an assessment in the potential facility to ensure it can meet the LOP. Factors to be considered when determining if an alternate location is an option include:

- Limitations on the delineated area;
- Mission needs;
- Market conditions;
- Timeframe;
- Budget; and
- Other operational requirements.

If alternate locations are available, they must be evaluated to determine if any different risks are inherent in that location and if the necessary LOP can be achieved. Although the original security requirements are still applicable, site-specific conditions must be evaluated to determine if there is a change in the nature of risks at the alternate facility. For example, an alternate facility might be in a higher crime area, which necessitates additional theft-prevention measure.

In many situations, an alternate location is not feasible. If the tenant is already in an existing building, for example, budgetary constraints may prohibit relocation. Similarly, available sites for new construction may have limitations. In many cases, the tenant's mission dictates the facility be located in a specific, delineated area that limits the availability of alternate sites.

⇧ If alternative locations are available, they must be evaluated to determine if any different risks are inherent in that location and if the necessary LOP can be achieved. **Return to Section 5.1.2 for each potential facility.**

- or -

⇩ If the alternate location is not feasible, some risk will have to be accepted, and a lower LOP must be implemented. **Continue to Section 5.1.10.**

5.1.10 Risk Acceptance

Risk acceptance is the explicit or implicit decision not to take an action that would affect all or part of a particular risk. It is an allowable outcome of applying the risk management process. Though made every

day in government, the decision to accept risk is not one to be taken lightly. The threat to federal facilities is real, and the decision to accept risk could have serious consequences. For that reason, decision-makers should obtain all the information they deem necessary to make a fully informed decision.

In some cases, risk acceptance is unavoidable. Competing requirements, standards, and priorities cannot always be reconciled. All budgets have some limitation and political and mission requirements cannot be ignored.

In all cases, the project documentation must clearly reflect the reason why the necessary LOP cannot be achieved. It is extremely important to completely document the rationale for accepting risk, including alternate strategies considered or implemented and opportunities in the future to implement the necessary LOP. See *Appendix F: Forms and Templates* for an example of how risk acceptance might be documented. Follow ISC Facility Security Committee guidance regarding retention and documentation of decision making.

Risk(s) accepted at the facility level may have an impact on agency-wide risk management efforts. Therefore, a copy of the facility-approved risk management strategy associated with risk acceptance shall be provided to the headquarters security office for awareness, along with any supporting documentation. In the instance of multi-tenant facilities, this documentation shall also be provided to the headquarters security offices of each tenant.

Once a credible and documented risk assessment is presented to and accepted by the decision-maker(s), the security organization has met its obligation in providing its best professional advice. This does not exempt the security organization from their accountability associated with the accuracy and completeness of the risk assessment itself or from implementation of countermeasures.

At this point, a customized LOP for the facility has been developed. Risks have been assessed, an achievable LOP has been identified, and risks that will be accepted have been documented. Now it is necessary to determine if the customized LOP is immediately achievable. **Continue to Section 5.1.11.**

5.1.11 Decision Point: Is the Level of Protection Achievable Immediately?

The amount of preparation required to implement a countermeasure may limit its immediate achievability. If a countermeasure is no-cost (such as a procedural change), can be incorporated into an ongoing or planned project (such as a lobby redesign), or if funding is available, the countermeasure can generally be implemented almost immediately. When countermeasures require advance budgeting or coordination with owners and outside authorities for approval, implementation may be delayed.

In the case of new construction, countermeasures will be integrated into the building-design and implemented during construction. In leases, some countermeasures may require coordination with the lessor and other non-governmental tenants. In existing buildings, delayed implementation is often necessary when the LOP requires funding not available within the current fiscal year budget resources, or coordination among multiple government tenants causes delay. See Section 5.2 for specific implementation under various circumstances.

⇧ If the necessary LOP is immediately achievable, the countermeasures should be implemented. **Go to Section 5.1.13.**

- or -

⇩ If the necessary LOP is not immediately achievable, the delayed implementation must be planned, and interim countermeasures shall be implemented to temporarily mitigate the risks. **Continue to Section 5.1.12.**

5.1.12 Implement Interim Countermeasures

Interim countermeasures shall be considered when risk is identified but the permanent countermeasures to mitigate it are not immediately achievable. Interim countermeasures may involve establishing temporary procedures, posting additional guards, or utilizing portable equipment. The temporary countermeasures may provide a similar or even equivalent LOP. For example, "Jersey barriers" or "K-rails" may meet vehicle barrier requirements but may ultimately be replaced by permanent barriers that match the facility design. In other cases, interim countermeasures may provide less protection but may still mitigate the risk to a reasonable degree until the full LOP can be achieved. For example, a visual inspection of identification badges may be implemented until an electronic access-control system can be installed.

The countermeasures identified as necessary and achievable, through the application of this standard, must ultimately, and as rapidly as possible, replace any interim countermeasures. A plan for permanent replacement must accompany any implementation of interim countermeasures. **Go to Section 5.1.13.**

5.1.13 Implement Permanent Countermeasures

Once the customized LOP is established, it must be implemented. The Details of Security Measures section in *Appendix B: Countermeasures* provides specific information regarding implementation.

5.2 Application to Project-Specific Circumstances

The following describes how the process defined in Section 5.1 is applied to various project-specific circumstances.

5.2.1 Application to New Construction

As with previous ISC standards, the implementation of this standard does not preclude new construction in urban environments, although it may require the acceptance of some risk. In these cases, risk-acceptability is balanced against the tenant's needs and how dependent the mission is on the facility's location.

For future construction (whether lease-construct or government-owned), this standard shall be applied as part of the requirements definition-process. The security organization will conduct a project-specific risk assessment during the requirements definition phase. The security organization will recommend countermeasures and design features to be included in the design specifications. The tenant agency representative or the FSC will determine whether the identified countermeasures will be implemented or whether risk will be accepted. Those countermeasures will become part of the facility's design program requirements to ensure required security measures are fully integrated into the configuration of the site and/or building design.

Site security requirements for new construction—particularly setback—must be identified before a site is acquired and the construction funding request is finalized. Identifying site security requirements from the fore may prevent the selection of a site that lacks necessary features and may help reduce the need for more costly countermeasures, such as blast hardening.

5.2.2 Application to Existing Federal Facilities

For existing federal facilities (leased or government-owned), this standard shall be applied as part of the periodic risk assessment process. The security organization will conduct a periodic risk assessment (at the frequency specified by the FSL determination) and recommend countermeasures and design features to be implemented at the facility. The tenant agency representative or the FSC will determine whether the recommended countermeasures will be implemented or if risk will be accepted.

For approved countermeasures that cannot be implemented immediately, a plan to phase in countermeasures and achieve compliance shall be instituted. In some cases, the implementation of countermeasures must be delayed until renovations or modernization programs occur.

Historic buildings are addressed in the same manner as other existing buildings. Compliance with Section 106 of the National Historic Preservation Act[5] is governed by U.S. Department of Interior regulations found in 36 Code of Federal Regulations Part 800[6] and must be coordinated with the State Historic Preservation Officer consistent with established agency/departmental implementing procedures. Design alternatives for incorporating the necessary security measures into the historic property should be fully explored with a design professional to balance historic preservation goals and security requirements.

5.2.3 Modernization and Renovation

When a renovation or major modernization of an existing facility is initiated, many of the countermeasures previously deemed not achievable due to facility limitations or funding considerations may now be achievable as part of the project. For buildings identified to undergo a renovation or major modernization, this standard shall be applied during the planning and prospectus development phase.

Specifically, the following applies:

- When an existing building is being renovated, the security organization will conduct a project-specific risk assessment during the requirements definition phase. Prior security assessments and delayed implementation plans shall be reviewed to identify countermeasures deferred because of facility constraints or cost considerations.
- When an existing building or space is to have a change in building occupancy type (e.g., a warehouse is converted to office space), the security organization will conduct a project-specific risk assessment representing the finished building or space during the requirements definition or concept phase.
- Additions to existing buildings shall be designed and constructed to comply with this standard. The security organization will conduct a project-specific risk assessment for the addition. If the addition is 50 percent or more of the gross area of the existing building, this standard shall be applied to the entire building (existing portions and the addition).

[5] Please see http://www.nps.gov/history/local-law/nhpa1966.htm, accessed 10 May 2013.

[6] Please see http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=36:3.0.6.1.1, accessed 10 May 2013.

In all cases, the tenant agency representative or the FSC will still determine whether the recommended countermeasures will be implemented as part of the modernization or the risk will continue to be accepted. Approved countermeasures will be incorporated into the project program and prospectus proposal.

5.2.4 Application to Lease Solicitations

As with previous ISC standards, the implementation of *Appendix B: Countermeasures* does not preclude leasing in urban areas.

Unless there is a change in tenant(s) or mission, this standard does not apply to renewals, extensions, expansions, superseding leases, and succeeding leases established other than through full and open competition but is recommended for each of those instances. If there is a change in tenant(s) or mission, this standard does apply (see Sections 5.2.5 and 5.2.6). Otherwise, for these types of leasing actions the FSL determinations and risk assessments will continue to be done in accordance with the schedule established for the facility.

For new lease acquisitions, lease-construction, and succeeding leases established through full and open competition, this standard shall be applied during the requirements definition, negotiation and build-out phases. The security organization will conduct a project-specific FSL assessment and risk assessment during the requirements definition phase, and recommended countermeasures and security design features will be included in the lease solicitation. Security requirements must be applied equally to all offers in the procurement.

Market surveys will provide the prospective tenant and the leasing agency (if different from the tenant agency) with information regarding whether the LOP can be achieved in the delineated area. Any additional risks and any additional countermeasures or design features identified by the security organization will be presented to the tenant(s) to determine whether to implement in the requirements of the solicitation or accept the risk. If the required LOP cannot be met in the delineated area, the prospective tenant(s) and leasing agency will determine whether to change the delineated area or have the tenant agency representative or the FSC reassess the minimum security requirements. As described in Section 5.1.9, other factors affecting the feasibility of altering the delineated area, such as mission needs, market conditions, timeframe, budget, and operational considerations, may be considered.

The security organization will evaluate the offerors' proposed security countermeasures for effectiveness in meeting the LOP required.

The security organization will update the risk assessment on offers in the competitive range to identify threats and vulnerabilities for the specific properties and recommend any additional security measures. The tenant(s) will determine the additional recommended security measures to be adopted or accept the risk. The leasing agency (if different from the tenant agency) will determine how the additional countermeasures will be implemented in the procurement. Major items may have to be included as an amendment to the solicitation. Minor items and quantitative changes may be able to be presented to the individual offerors prior to final proposal revisions, or included in the build-out phase post award.

Should none of the offers received meet the minimum security requirements of the solicitation, the prospective tenant(s) and leasing agency should consider expanding the delineated area or have the tenant agency representative or the FSC reassess the minimum security requirements. As described in Section 5.1.9, the feasibility of altering the delineated area may be considered.

During the build-out phase of the lease, the security organization will conduct an inspection of the leased space for proper installation and functionality of the security systems and countermeasures.

5.2.5 Tenant and Mission Changes in Occupied Buildings

Whenever consideration is given to moving new tenants (including out-leasing or backfilling vacant space) into a building already occupied by a government tenant, the potential for increasing security requirements—and impacts on the funding and operations of the existing tenants—must be a part of the decision process. Moving a higher-risk tenant into a facility already occupied by a government tenant with lower security requirements brings with it inherent challenges in funding, accepting risk, and implementation.

Changes to an existing tenant's mission brings with it even greater challenges in making decisions about risk acceptance and responsibility for implementation than moving in a new tenant does. The decision to change the mission of an existing tenant—and possibly increase the risks to the facility and the cost for increased security—is typically made solely by the tenant department or agency without input from or consideration for the other tenants.

Conversely, changing a tenant's mission to a lower-risk mission, or moving a high-risk tenant out of a facility, could reduce the risk to the remaining tenants. Some countermeasures could be decommissioned or reduced.

In these cases, the security organization must assess the entire facility with respect to the risk that would be created by the presence of a new tenant or by changing an existing tenant's mission of. The security organization should assess the overall FSL for the facility and make a new determination as necessary. If the FSL remains the same, the adequacy of the existing countermeasures should be reviewed, and appropriate security enhancements should be implemented. If the FSL changes, a new risk assessment and analysis of the baseline LOP is required, including customization analysis as outlined in Section 5.1. If new or increased risks are identified, recommended countermeasure upgrades must be considered prior to the change. Any recommended changes to security must be considered by the tenant(s), the prospective new tenant(s)— or tenant(s) with the mission change— and the leasing or owning agency.

A plan to phase in countermeasures and achieve compliance may be necessary, particularly where cost-sharing agreements must be developed.

5.2.6 Campus Environments

In a campus environment, site-specific conditions will dictate how campus-wide countermeasures impact individual facilities and exterior restricted areas. The tenant agency representative or the FSC should consider the campus security characteristics when the baseline security countermeasures are established for each facility within the campus.

For example, the characteristics of a facility located within the confines of a campus may require visitor vehicles to be screened prior to entering the parking garage. If visitor vehicles are screened prior to entering the campus, additional screening prior to entering the parking garage of a specific building is not necessary. Conversely, restricted areas within the campus, such as employee-only parking, utility buildings, and other buildings or improvements within the campus itself, may still require enclosures or other protective measures.

In applying the security criteria contained in this standard, the security organization should exercise sound judgment as they identify the security measures necessary at individual buildings. It may be more cost-effective to implement security measures at the perimeter, as it precludes the necessity to duplicate security measures at individual buildings or areas within the campus.

5.2.7 Purchases

For buildings to be purchased, this standard shall be applied as part of the requirements definition process. The security organization will conduct a project-specific risk assessment during the requirements definition phase. Recommended countermeasures and design features must be considered as part of the project cost and included in the scope of work needed to make the building suitable for occupancy.

The tenant representatives to the project team will determine whether the recommended countermeasures will be implemented or whether the risk will be accepted.

5.3 Security Criteria

The following list of tables, found in *Appendix B: Countermeasures* (FOUO) identifies the security measures to be applied as part of the baseline LOP or a customized LOP:

- Site—including the site perimeter, site access, exterior areas and assets, and parking;
- Structure—including structural hardening, façade, windows, and building systems;
- Facility Entrances—including employee and visitor pedestrian entrances and exits, loading docks, and other openings in the building envelope;
- Interior—including space planning and security of specific interior spaces;
- Security Systems—including intrusion-detection, access control, and VSS camera systems;
- Security Operations and Administration—including planning, guard force operations, management and decision making, and mail handling and receiving; and
- Cybersecurity—including device identification, network access control and maintenance, and incident response.

5.3.1 Format of the Tables

The tables are organized to provide a user-friendly cross-reference from the countermeasures and baseline LOPs to the undesirable events used for customization. The security organization should cross-reference each undesirable event (the right side of Figure 5-12) with the security criteria that mitigates it (the left side of Figure 5-12). Undesirable events marked with a "Y" (yes) and colored red (circled in blue) are generally mitigated by the corresponding countermeasure as shown on the left side of Figure 5-12; whereas those marked with an "N" (no) and shaded green are typically not considered criteria requiring mitigation (circled in yellow). This will allow the security organization the chance to build a general list of undesirable events applicable to the facility and the countermeasures used to mitigate those risks.

In many tables, the degree of applicability increases from a lower FSL to a higher FSL. The countermeasures are generally cumulative as the LOP increases (i.e., to achieve the Medium LOP, the countermeasures in Minimum, Low, and Medium must be implemented). However, when in conflict, the higher LOP supersedes the lower (e.g., if the Medium LOP requires a fence and the High LOP requires a wall, only the wall would be implemented).

In some cases, the security criteria may be "not applicable." For example, when no underground parking exists or there are no restricted areas on the outside of the building. In this case, documentation should reflect the parking criteria as "not applicable," not as "met" or "compliant."

Each table provides details on implementation and other considerations for each security criterion. While the application of security measures at the various levels is specific, this Standard does not recommend

specific technologies, systems, or manufacturer brands. Selection of individual systems and technologies is at the discretion of the department and agency security organizations.

5.3.2 Design-Basis Threat

Appendix A: The Design-Basis Threat (FOUO) report establishes a profile of the type, composition, and capabilities of adversaries. It is an estimate of the threat facing federal facilities across a range of undesirable events and is based on the best intelligence information, reports, assessments, and crime statistics available at the time of publication. In some instances, specific information about the threat may be required to determine which LOP to implement (e.g., when to deploy VSS cameras) or to develop a performance specification (e.g., the size of an explosive device to protect against). To support such determinations, and to maintain additional control of sensitive threat assessment information, the ISC developed this report.

The DBT report fills the void of threat information available to security managers in the field (especially smaller agencies without access to current intelligence) and dovetails with the ISC standards that allows for the customization of countermeasure packages based on risk. This is an incredibly important aspect of ensuring a common baseline on current threats and risks for all nonmilitary, federally-owned and leased facilities.

The DBT report was developed in cooperation with various government intelligence organizations. The document provides a basis for decision-making, including the assignment of threat ratings and the relative prioritization of threats.

5.3.3 Establishing Level of Protection Templates

Some departments and agencies construct or acquire similar facilities to accomplish identical missions in various locations. For example, GSA constructs child-care centers (CCC) across the Nation. CCCs generally face similar threats that can be mitigated by a similar LOP at each location. Instead of repeating the entire customization process for each CCC, a LOP template can be developed and applied to all CCCs.

The LOP template would serve as a boilerplate set of security requirements to be incorporated into the development of these facilities. In essence, the agency is creating a security design guide, starting with the selection of a common LOP. The LOP template avoids replication of the customization process, shortens the lead time required to identify security requirements when new projects are initiated, serves as the basis for cost-estimating, and encourages standardization across common facility types.

To create an LOP template, a common risk assessment must be developed that applies to all facilities in a common category. A customized LOP is then developed following the processes discussed in Section 5.1. The countermeasure selections in the customized LOP then become the LOP template. In all cases, a site-specific assessment should be conducted to ensure any additional risks not covered by the LOP template are appropriately mitigated by measures beyond those specified in the template.

Appendix C: Child-Care Center Level of Protection Template (FOUO) includes the boilerplate of undesirable events and the countermeasure requirements for CCCs in federal facilities and may be used as an example for further templates.

6.0 The Risk Informed Decision-making Process Summary

Security organizations are responsible for identifying and analyzing threats, vulnerabilities and consequences, and recommending appropriate countermeasures. The tenant agency representative or the FSC is responsible for the decision to either implement those recommendations or to accept risk as part of a risk management strategy. Together, the tenant agency representative or the FSC and the security organization are responsible for identifying and implementing the most cost-effective countermeasure appropriate for mitigating vulnerability, thereby reducing the risk to an acceptable level. Thus, the the tenant agency representative or the FSC plays a critical role in the decision-making process.

To make an informed risk-based decision regarding risk mitigation or risk acceptance, the security organization and the decision-making authority must collaborate. For any recommended countermeasure, the security organization must provide all information pertinent to the decision: the nature of the threat, the specific vulnerabilities that must be addressed, a complete understanding of the potential consequences, and the costs. The decision-makers need to know this information to make an informed decision.

Decision-makers must have authority, appropriate security clearance, and access to expert resources (e.g., security, facility, and finance) to gain a sufficient understanding of the relevant issues and render a sound decision. Sufficient understanding means not only an understanding of the security issues but also of the missions and priorities of those who occupy (or will occupy) the building, those of the agency(s) as a whole, and the associated cost implications.

Once a credible and documented risk assessment has been presented to and accepted by the decision-maker(s), the security organization is not accountable for any future decision regarding risk acceptance.

Decisions made pursuant to this risk informed decision-making process must be thoroughly documented from FSL determination and analysis of the LOP to the implementation of (or decision not to implement) countermeasures.

For further information on the role and responsibilities of the FSC, refer to *Appendix D: How to Conduct a Facility Security Committee*.

7.0 References

The following ISC documents, referenced above, support the ISC Risk Management Process. These documents are designated FOUO. Government users with an appropriate "need-to-know" may request access to the current edition of the documents by sending an email to ISCAccess@hq.DHS.gov with your full name and contact information, including email, the name of your agency, and the reason you need access.

- Interagency Security Committee, *Appendix A: Design-Basis Threat: An Interagency Security Committee Report,* Washington D.C.: U.S. Department of Homeland Security.
- Interagency Security Committee, *Appendix B: Countermeasures*, Washington D.C.: U.S. Department of Homeland Security.
- Interagency Security Committee, *Appendix C: Child-Care Centers Level of Protection Template*, Washington D.C.: U.S. Department of Homeland Security.

8.0 Acknowledgments

Interagency Security Committee

Daryle Hernandez
Chief

Bernard Holt
Deputy Chief

Anthony Evernham
RMP Update Facilitator

Lynn Enos
RMP Update Facilitator

Laura Robb
Analyst

TJ Cienki
Analyst

Standards Subcommittee

Risk Management Process for Federal Facilities:

An Interagency Security Committee Standard

2021 Edition

Mark Hartz, Chair
Administrative Office of the U.S. Courts

Michael Fluck
Internal Revenue Service

Michael Griffin
General Services Administration

Matthew Kurdziolek
Social Security Administration

Joseph Misher
Federal Protective Service

Charles King
Federal Trade Commission

Michael Brown
Federal Protective Service

Gean Alston
Department of Homeland Security

Matthew Chupka
Department of Defense

William Earl
General Services Administration

Dennis Ouellette
Internal Revenue Service

Dave Olsen
Federal Protective Service

Chad Hyland
Department of Justice

Lewis Monroe
Department of Energy

Joshua Freedman
Department of Defense

Wesley Faudree
Department of Justice

Charlotte Harding
Department of Justice

Lynn Enos
Interagency Security Committee

Jason Adams
United States Marshals Service

Emily Sprout
International Boundary and Water Commission

Michael Davenport
United States Marshals Service

Keith Earley
Railroad Retirement Board

Dan Handschin
Department of Homeland Security

Fred Jackson
Department of Defense

Anthony Evernham
Interagency Security Committee

Standards Subcommittee

Risk Management Process for Federal Facilities:
An Interagency Security Committee Standard
First Edition, December 2012

Brian Doto
Federal Bureau of Investigation

Mark Olberholtzer
Federal Aviation Administration

Bernard Holt
Interagency Security Committee

Michael Griffin
General Services Administration

David Olson
Federal Protective Service

Ashley Gotlinger
Interagency Security Committee

Facility Security Level Determination Working Group

Interagency Security Committee: Use of Physical Security Performance Measures

First Edition, June 2009

Everett R. Hilliard, Chair
Department of Justice

Jeffrey Barnhart Department of the Treasury	Calvin Byrd Nuclear Regulatory Commission
Dennis Chapas Department of Homeland Security	Wesley Carpenter Environmental Protection Agency
Joseph Gerber Department of Homeland Security	William Kmetz Federal Deposit Insurance Corporation
Robert Shaw General Services Administration	Mark Strickland Administrative Office of the U.S. Courts
Thomas Wood General Services Administration	Gwainevere Hess Interagency Security Committee

Security Performance Measures Working Group

Physical Security Criteria for Federal Facilities:
An Interagency Security Committee Standard

First Edition, April 2010

Mark Strickland, Chair
Administrative Office of the U.S. Courts

Joseph Gerber Department of Homeland Security	Gwainevere Hess Interagency Security Committee

Acknowledgement:

This working group acknowledges the work of Mr. Mark Harvey (Federal Protective Service) on the first draft of the Performance Measures document.

Physical Security Criteria Working Group

Physical Security Criteria for Federal Facilities:
An Interagency Security Committee Standard
First Edition, April 2010

Facility Security Committees: An Interagency Security Committee Standard
Second Edition, January 2012

Everett R. Hilliard, Chair
Department of Justice

Calvin Byrd Nuclear Regulatory Commission	Joseph Gerber Department of Homeland Security
William Hirano General Services Administration	Mark Strickland Administrative Office of the U.S. Courts
Thomas Wood General Services Administration	Gwainevere Hess Interagency Security Committee

First Facility Security Committee Working Group (2008-2010)

Mark Strickland, Chair
General Services Administration

Reginald Allen Office of Personnel Management	Mark Applewhaite Postal Inspection Service
Tommy Barnes Federal Deposit Insurance Commission	Bob Harding General Services Administration
Mark Harvey Department of Homeland Security	Thomas Holman Department of Labor
Charles Luddeke Department of Homeland Security	Ray Patterson National Aeronautics and Space Administration
Paul Raudenbush National Aeronautics and Space Administration	Sonya Rowe Department of State
Tom Thomas Central Intelligence Agency	Leslie Wiggins Department of State
Don Williams Department of Health and Human Services	Bernard Holt Interagency Security Committee

List of Abbreviations/Acronyms/Initialisms

CCC	Child-Care Center
COG	Continuity of Government
COOP	Continuity of Operations
DBT	Design-Basis Threat
DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department of Justice
E.O.	Executive Order
FSC	Facility Security Committee
FSL	Facility Security Level
GAO	Government Accountability Office
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
ISC	Interagency Security Committee
LOP	Level of Protection
NEF	National Essential Functions
NIPP	National Infrastructure Protection Plan
PPD	Presidential Policy Directive
RMP	Risk Management Process
RSF	Rentable Square Footage
U.S.C.	United States Code
VSS	Video Surveillance System

Glossary of Terms

Term	Definition
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 occur. Extended definition: Level of risk at which, given costs and benefits associated with risk reduction measures, no action is deemed to be warranted at a given point in time. Example: Extremely low levels of water-borne contaminants can be deemed an acceptable risk.
Adjacency	A building or other improvement that abuts or is proximate to a multiple building site, a specific building within a multiple building site, or a single building site.
Alteration	A limited construction project for an existing building that comprises the modification or replacement of one or a number of existing building systems or components. An alteration goes beyond normal maintenance activities but is less extensive than a major modernization.
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.
Buffer Zone	A tract of land between a facility or protected area. For example, a building owner/lessor may position a parking lot or a green space between the city street and a building.
Building	An enclosed structure (above or below grade).
Building Entry	An access point into, or exit from, the building.
Building Envelope	The outside surface and dimensions of a building, inclusive of the façade and roof.
Campus	Two or more federal facilities contiguous and typically sharing some aspects of the environment, such as parking, courtyards, private vehicle access roads, or gates and entrances to connected buildings. A campus also may be referred to as a "federal center" or "complex."
Consequence	The level, duration, and nature of the loss resulting from an undesirable event. Extended definition: Effect of an event, incident, or occurrence.

Term	Definition
	Annotation: Consequence is commonly measured in four ways: human, economic, mission, and psychological, but may also include other factors such as impact on the environment. See also: human consequence (health), economic consequence, mission consequence, psychological consequence, indirect consequence, and direct consequence.
Continuity of Government (COG)	A coordinated effort within each branch of government (e.g., the federal Government's Executive Branch) to ensure that NEFs continue to be performed during a catastrophic emergency.
Critical Areas	Areas that, if damaged or compromised, could have significant adverse consequences for the agency's mission or 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." Critical areas do not necessarily have to be within government-controlled space (e.g., generators located outside government-controlled space).
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
Customized Level of Protection	The final set of countermeasures developed as the result of the risk-based analytical process.
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 Federal Facility	A facility that has already been constructed or for which the design and construction effort has reached a stage where design changes may be cost prohibitive.
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	Space built or established to serve a particular purpose. The facility is inclusive of a building or suite and associated support infrastructure (e.g., parking or utilities) and land.

Term	Definition
Facility Security Committee	A committee that is responsible for addressing facility-specific security issues and approving the implementation of security measures and practices in multi-tenant facilities. The Facility Security Committee (FSC) consists of representatives of all federal tenants in the facility, the security organization, and the owning or leasing department or agency. In the case of new construction or pending lease actions, the FSC will also include the project team and the planned tenant(s). The FSC was formerly known as the Building Security Committee (BSC).
Facility Security Level	A categorization based on the analysis of several security-related facility factors, which serves as the basis for the implementation of countermeasures specified in ISC standards.
Federal Departments and Agencies	Those executive departments enumerated in 5 United States Code (U.S.C.) 101 and the Department of Homeland Security, independent establishments as defined by 5 U.S.C. 104(1), government corporations as defined by 5 U.S.C. 103(1), and the U.S. Postal Service.
Federal Facilities	Government leased and owned facilities in the United States (inclusive of its territories) occupied by federal employees for nonmilitary activities.
Facility Security Assessment	The process and final product documenting an evaluation of the security-related 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.
Federal Tenant	A federal department or agency that pays rent on space in a federal facility. See also: Single-tenant, multi-tenant, and mixed-multi-tenant.
Government-Owned	A facility owned by the United States and under the custody and control of a federal department or agency.
Interior	Space inside a building controlled or occupied by the government.
Lease Construction (Build-to-Suit)	A new construction project that is undertaken by a lessor in response to a specific requirement for the construction of a new facility for the government.
Lease Extension	An extension of the expiration date of a lease to provide for continued occupancy on a short-term basis.
Lease Renewal (Exercised Option)	The exercising of an option to continue occupancy based upon specified terms and conditions in the current lease agreement.
Level of Protection	The degree of security provided by a particular countermeasure or set of countermeasures. Levels of protection used in this Standard are Minimum, Low, Medium, High, and Very High.
Level of Risk	The combined measure of the threat, vulnerability, and consequence posed to a facility from a specified undesirable event.

Term	Definition
Major Modernization	The comprehensive replacement or restoration of virtually all major systems, tenant-related interior work (e.g., ceilings, partitions, doors, floor finishes), or building elements and features.
Mixed-Tenant	A facility that includes exactly one federal tenant as well as one or more non-federal tenants (including commercial and state, local, tribal, and territorial tenants).
Mixed-Multi-Tenant	A facility that includes tenants from multiple federal departments and agencies AND at least one non-federal tenant.
Multi-Tenant	A facility that includes tenants from multiple federal departments and agencies but no non-federal tenants.
National Air Space	The region of the atmosphere above an area of land, especially the region above a nation over which it has jurisdiction (e.g., in the United States, airspace consists of classes A, B, C, D, E, and G.)[1] The NAS includes both controlled and uncontrolled airspace. Class A begins and includes 18,000 ft. MSL and continues up to 60,000 ft. MSL. It is the most controlled airspace and requires a pilot to carry an Instrument Flight Rating and proper clearance no matter what type of aircraft is being flown. Pilots are also required to change their altimeter settings to 29.92 in. to ensure all pilots within the airspace have the same readings in order to ensure proper altitude separation. Class B airspace extends from the surface up to 10,000 ft. AGL and is the area above and around the busiest airports (LAX, MIA, CVG) and is also heavily controlled. A side view of Class B airspace resembles an upside-down wedding cake with three layers becoming bigger toward the top. Class B's are designed individually to meet the needs of the airport they overlay. Pilots must also receive clearance to enter the Class B airspace, but Visual Flight Reference may be used. Class B airspace corresponds to the area formerly known as a Terminal Control Area (TCA). Class C airspace reaches from the surface to 4,000 ft. AGL above the airport which it surrounds. Class C airspace only exists over airports which have an operational control tower, are serviced by a radar approach control, and have a certain number of instrument flight operations. Class C is also individually designed for airports but usually covers a surface area of about 5 nautical miles around the airport up to 1,200 ft. AGL. At 1,200 ft. the airspace extends to 10 nautical miles in diameter which continues to 4,000 ft. Pilots are required to establish two-way radio communications with the ATC facility providing air traffic control service to the area before entering the airspace. Within Class C, Visual and Instrument pilots are separated.

Term	Definition
	Class D airspace exists from the surface to 2,500 ft. AGL above an airport. Class D airspace only surrounds airports with an operational control tower. Class D airspace is also tailored to meet the needs of the airport. Pilots are required to establish and maintain two-way radio communications with the ATC facility providing air traffic control services prior to entering the airspace. Pilots using Visual Flight Reference must be vigilant for traffic as there is no positive separation service in the airspace. This airspace roughly corresponds to the former Airport Traffic Area.
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.
New Construction	A project in which an entirely new facility is to be built.
New Lease	A lease established in a new location when space must be added to the current leased space inventory.
Non-Federal Tenant	For the purposes of entry control, employees of non-federal tenants who occupy other space in a mixed multi-tenant facility. The FSC (and lease agreement) would establish entry control requirements applicable to non-federal tenants passing through a federal entry control point (in accordance with established policies). See also: mixed-multi-tenant.
Nonmilitary Activities	Any facility not owned or leased by the Department of Defense.
Occupant	Any person who is regularly assigned to federally occupied space who has been issued and presents the required identification badge or pass for access. In multi-tenant facilities, the FSC establishes the thresholds for determining who qualifies for "occupant" status. Based on varying mission assignments, departments and agencies have the flexibility to determine what constitutes a "regularly assigned" person.
Organizational Security Element	A headquarters or field component of a facility tenant's internal security office, or equivalent.
Primary Tenant	The federal tenant identified by Bureau Code in Office of Management and Budget Circular No. A-11, Appendix C, occupies the largest amount of rentable space in a federal facility.
Risk	A measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence.

Term	Definition
	Extended definition: Potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences; potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence. Example: The team calculated the risk of a terrorist attack after analyzing intelligence reports, vulnerability assessments, and consequence models. Annotation: 1) Risk is defined as the potential for an unwanted outcome. This potential is often measured and used to compare different future situations. 2) Risk may manifest at the strategic, operational, and tactical levels.
Risk Acceptance	The explicit or implicit decision not to take an 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 Assessment Report	The documentation of the risk assessment process to include the identification of undesirable events, consequences, and vulnerabilities, and the recommendation of specific security measures commensurate with the level of risk.
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. Extended definition: Process of identifying, analyzing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level at an acceptable cost. Annotation: The primary goal of risk management is to reduce or eliminate risk through mitigation measures (avoiding the risk or reducing the negative effect of the risk), but also includes the concepts of acceptance and/or transfer of responsibility for the risk as appropriate. Risk management principles acknowledge that, while risk often cannot be eliminated, actions can usually be taken to reduce risk.
Risk Management Methodology	A set of methods, principles, or rules used to identify, analyze, assess, and communicate risk, and mitigate, accept, or control it to an acceptable level at an acceptable cost.
Risk Management Strategy	A proactive approach to reduce the usually negative impacts of various risks by choosing within a range of options that include complete avoidance of any risk that would cause harm or injury, accepting the risk, controlling the risk by employing risk mitigation options to reduce impacts, or transferring some or all of the risk to another entity based on a set of stated priorities.

Term	Definition
	Extended definition: Course of action or actions to be taken in order to manage risks; proactive approach to reduce the usually negative impacts of various risks by choosing within a range of options that include complete avoidance of any risk that would cause harm or injury, accepting the risk, controlling the risk by employing risk mitigation options to reduce impacts, or transferring some or all of the risk to another entity based on a set of stated priorities. Sample usage: Mutual aid agreements are a risk management strategy used by some emergency response authorities to respond to large scale incidents.
Risk Mitigation	The application of strategies and countermeasures to reduce the threat of, vulnerability to, and/or consequences from an undesirable event. Extended definition: Application of measure or measures to reduce the likelihood of an unwanted occurrence and/or its consequences. Measures may be implemented prior to, during, or after an incident, event, or occurrence. Example: Through risk mitigation, the potential impact of the tsunami on the local population was greatly reduced. Annotation: Measures may be implemented prior to, during, or after an incident, event, or occurrence.
Security Maintenance	The regularly scheduled or routine upkeep of equipment.
Security Organization	The government agency or an internal agency component either identified by statute, interagency memorandum of understanding /memorandum of agreement, or policy responsible for physical security for the specific facility.
Security Provider	The federal entity who oversees the conduct of security assessments; installation and/or maintenance of security countermeasures and components of countermeasures; or, contracts with federal agencies to provide security guard services and the personnel employed by them.
Security System(s)	Electronic system(s) that are designed to prevent theft or intrusion and protect property and life. Burglar alarm systems, access control systems, fire alarm systems, 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.
Single-tenant Facility	A facility that has exactly one federal tenant and zero non-federal tenants. This may include multiple components of a single federal department or agency.
Site	The physical land area controlled by the government by right of ownership, leasehold interest, permit, or other legal conveyance, upon which a facility is placed.

Term	Definition
Site Entry	A vehicle or pedestrian access point into, or exit from, the site.
Site Perimeter	The outermost boundary of a site. The site perimeter is often delineated by the property line.
Standoff	Distance between an explosive device and its target.
Special-Use Facilities	An entire facility or space within a facility itself that contains environments, equipment, or data normally not housed in typical office, storage, or public access facilities. Examples of special-use facilities include, but are not limited to, high-security laboratories, aircraft and spacecraft hangers, or unique storage facilities designed specifically for such things as chemicals and explosives.
Succeeding Lease	A lease established when the government seeks continued occupancy in the same space at the same leased location, whose effective date immediately follows the expiration date of the existing lease.
Suite	One or more contiguous rooms occupied as a unit.
Suite Entry	An access point into, or exit from, the suite.
Suite Perimeter	The outer walls encircling a suite.
Superseding Lease	A lease that replaces an existing lease, prior to the scheduled expiration of the existing lease term.
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.
Visitor	Any person entering the government facility that does not possess the required identification badge or pass for access or who otherwise does not qualify as an "occupant."
Vulnerability	A weakness in the design or operation of a facility that an adversary can exploit. Extended definition: Physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard; characteristic of design, location, security posture, operation, or any combination thereof, that renders an asset, system, network, or entity susceptible to disruption, destruction, or exploitation. Extended definition: Characteristic of design, location, security posture, operation, or any combination thereof, that renders an asset, system, network, or entity susceptible to disruption, destruction, or exploitation. Example: Installation of vehicle barriers may remove a vulnerability related to attacks using vehicle-borne improvised explosive devices.

Term	Definition
	Annotation: In calculating risk of an intentional hazard, the common measurement of vulnerability is the likelihood that an attack is successful, given that it is attempted.

Appendix A: The Design-Basis Threat Report (FOUO)

The Interagency Security Committee's *The Design-Basis Threat Report* is For Official Use Only (FOUO). Government users with a need to know may request access by sending an email to ISCAccess@hq.DHS.gov with your full name and contact information, including email, the name of your agency, and the reason you need access.

Appendix B: Countermeasures (FOUO)

The Interagency Security Committee's *Countermeasures* is For Official Use Only (FOUO). Government users with a need to know may request access by sending an email to ISCAccess@hq.DHS.gov with your full name and contact information, including email, the name of your agency, and the reason you need access.

Appendix C: Child-Care Centers Level of Protection Template (FOUO)

The Interagency Security Committee's Child-Care Centers Level of Protection Template is For Official Use Only (FOUO). Government users with a need to know may request access by sending an email to ISCAccess@hq.DHS.gov with your full name and contact information, including email, the name of your agency, and the reason you need access.

Appendix D: How to Conduct a Facility Security Committee

D.1 Introduction

The authority for federal departments and agencies to provide security for the facilities and employees is cited in various sections of the United States Code and the Code of Federal Regulations. Per their respective authority, each department or agency obtains funds to provide security. In single-tenant facilities, the federal department or agency with funding authority is the decision-maker for the facility's security and has the option to use these standards or other internal procedures to make security decisions. For facilities with two or more federal tenants with funding authority, an FSC will be established to make security decisions for the facility. It is recommended that the owning or leasing authority identify the requirement for an FSC and communicate that requirement in writing to the proposed tenant during the lease acquisition process.

FSCs should hold their meetings to maximize participation by tenant agencies, their funding authorities, and security personnel. FSC meetings do not need to be held in person, although at times in-person meetings may be desired (e.g, sensitive information). Technology can assist and can include conference calls for voice communication or voice and video/display, without impact to agency firewalls or data security. Technology also permits participation from individuals who are not able to travel to attend FSC meetings (i.e. funding authority, security organization or owning/leasing office).

Funding requests for security countermeasures and upgrades often compete with other funding requests at the agency headquarters level. Accordingly, FSC representatives are expected to assist the information flow between their respective headquarters and the FSC.

Each federal tenant that pays rent on space in the facility will have a seat and a vote on the FSC. Many decisions made by the FSC may have a financial impact. The headquarters element for each FSC representative is responsible for providing timely advice and guidance when needed. The facility security organization identifies security countermeasures to mitigate the risk of a credible threat for the facility. If an FSC makes the decision not to approve or provide funding for a countermeasure, this decision is the acceptance of risk.

In addition to decisions relating to the implementation or removal of countermeasures, FSCs are also responsible for the establishment and implementation of security operations and administration criteria in accordance with *Appendix B: Countermeasures*. Specifically, FSCs must develop and administer countermeasures, policies, and procedures related to security oversight and life, safety, and emergency procedures. This appendix is intended to be used in conjunction with *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*.

D.2 Facility Security Committees

The FSC, consisting of representatives of all federal tenants in the facility, the security organization (for example: Federal Protective Service for General Services Administration [GSA] owned and operated facilities), and the owning or leasing department or agency determines the FSL for the facility and determines the minimum standards (security countermeasures) for the facility. *Appendix B: Countermeasures* identifies the baseline LOP for a federal facility. *Appendix A: The Design-Basis Threat Report* establishes a profile of the type, composition, and capabilities of adversaries.

The facility's security organization will conduct a regular Facility Security Assessment (FSA) and, if necessary, provide feedback to the security organization to ensure information accuracy. The findings of the risk assessment determine whether the baseline LOP is adequate or if a customized LOP should be established. Any recommended countermeasures are reviewed by the FSC chairperson and the owning or leasing authority of the facility in advance of a scheduled FSC meeting.

At the FSC meeting, the security organization will provide documentation of risk assessment findings and recommendations for the countermeasures presented for consideration. Subsequent to the presentation, the FSC will meet to vote on the proposed countermeasure.

When voting on countermeasures, each FSC member votes to determine whether:

- The baseline LOP is used,
- Some of the baseline LOP is used and some risk is accepted,
- A lower LOP is used and some risk is accepted, or
- No countermeasures are used and all the risk is accepted.

To allow FSC members additional time to review the risk assessment findings, recommendations, and cost proposal prior to voting, the FSC chairperson may grant a review period, not to exceed 45 calendar days. During the review period, FSC representatives should consult their respective headquarters' security element if the FSC representative needs technical advice. If the FSC representative does not have funding authority, the FSC representative will consult their headquarters' financial element for guidance on votes that have a financial impact. The FSC representative votes to approve or disapprove proposed countermeasures and other security-related issues that come before the FSC.

D.2.1 Risk Mitigation or Acceptance

In general, risk is mitigated by lowering the vulnerability to exploitation of a potential weakness in the facility security posture. A common way to improve security is by adding or increasing the countermeasures to achieve a higher LOP. Some threats or vulnerabilities can be mitigated by applying a higher-level countermeasure and by changing or adding new physical security policies or procedures. Risk acceptance should be minimized; however, accepting risk may be the logical outcome of a rational decision process.

The federal facility's security organization shall identify each threat and the associated vulnerability for the facility. Each FSC shall document the chosen risk management strategy.

In some locations, federal tenants are responsible for funding security improvements through various means, such as rent increases or lump-sum funds. Frequently, the decision to implement a countermeasure has a financial component. To address this issue, the security organization must evaluate the cost effectiveness of the proposed countermeasure and present the analysis to the FSC. This analysis will follow the performance-measurement methodology outlined in *Appendix E: Use of Physical Security Performance Measures*.

When a countermeasure is recommended, the security organization shall inform the FSC members of the minimum standard for such countermeasures as outlined in *Appendix B: Countermeasures* for buildings with similar FSLs, as well as the threat as outlined in the most recent edition of *Appendix A: The Design-Basis Threat Report* (DBT). They shall also provide documentation indicating if the proposed countermeasure is above or below the standard set in the RMP for similar buildings.

D.2.2 Risk Acceptance

As stated in *The Risk Management Process for Federal Facilities*, the decision to forgo some available mitigation measures is a permissible outcome of applying the risk management methodology. For the purpose of this standard, risk acceptance is when a countermeasure suggested by the facility security organization is not used or a lower level of countermeasure is selected. For example, if funding is not available for a countermeasure, the FSC and security organization shall document the lack of funding availability and implement the highest-achievable countermeasure. The FSC shall document all aspects of the chosen risk management strategy and include this document in the meeting minutes.

D.2.3 Financial Authority

FSC members may or may not have the authority to obligate their respective organizations to a financial commitment. When funding issues are considered, each FSC representative without funding authority is allowed time to obtain guidance from their respective organization. Each FSC chairperson will establish a date for a vote on a decision item, while providing a reasonable period (not to exceed 45 calendar days from the date all requested documents and materials are provided to the FSC members to supply to their respective funding authorities) for FSC representatives to obtain guidance from their headquarters element.

If financial guidance is not provided to the FSC representative within this allotted time, the FSC chairperson may use the decision process, or other means as determined by the FSC, to reach a resolution.

D.2.4 Financial Commitment

An FSC vote to approve a countermeasure is a financial commitment by each federal tenant that pays rent for facility space. Each federal tenant is responsible for funding their prorated share of the cost of the approved countermeasure, regardless of how they voted. The prorated share of the cost is equal to the percentage of rentable square feet of space in the facility occupied by the federal tenant. (For General Services Administration [GSA]-controlled facilities please refer to Section D.3.1, paragraph 3.)

D.2.5 Selecting a Security Organization

When a facility does not have an assigned security organization or federal tenant with a law enforcement or security element housed in the facility, the FSC shall select a federal department or agency to provide the services of the security organization, as described in this document. When a facility has one federal tenant with law enforcement or security function housed in the facility, this entity should be selected as the security organization for the facility. When a facility has two or more federal tenants with a law enforcement or security function, the FSC should select a lead federal tenant to serve as the security organization.

D.2.6 Interagency Security Committee Training

Federal employees selected to be members of a federal FSC will be required to successfully complete a training course that meets the ISC's minimum standard of training. The ISC provides facilitated in-person and virtual training courses. Additionally, online training is available on the Homeland Security Information Network (HSIN) and the Federal Emergency Management Agency website. Completion of any of these training options will satisfy the training requirement. FSC members shall retain proof of completion for as long as they serve as a member of an FSC. Online training will minimally include:

- IS-1170 Introduction to the Interagency Security Committee and Risk Management Process
- IS-1171 Introduction to Interagency Security Committee Documents
- IS-1172 Interagency Security Committee Risk Management Process: Facility Security Level Determination
- IS-1173 Interagency Security Committee Risk Management Process: Levels of Protection and Application of the Design Basis Threat Report
- IS-1174 Interagency Security Committee Risk Management Process: Facility Security Committees

It is recommended that FSC participants retake the training courses when the RMP is significantly updated to ensure awareness of any changes that may impact their facility.

D.3 Facility Security Committee Procedures and Duties

Each FSC will have a chairperson. Each federal tenant that pays rent on space in a federal facility will have one representative with one vote on decision items before the FSC. The owning or leasing authority and security organization are members of the FSC with voting privileges, only if they pay rent on and occupy space in the federal facility. FSCs are encouraged to include the child-care center director (as applicable) as a non-voting member. Each federal department or agency headquarters shall provide guidance to its FSC representative. Meeting agendas must be published, and each agenda item must be identified either as a discussion or as a decision item. FSCs may adopt a charter identifying local operating procedures. These procedures should not contradict guidance outlined in this Standard. A charter template is provided in Appendix F. If a single federal tenant occupies a facility, they have the option to use this standard or other internal procedure to determine what security countermeasures are implemented, how funding is provided, and what risk is accepted. *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* details other functions where the FSC is expected to make decisions and provide guidance relating to the following items:

- 5.1.6 Determine the Highest Achievable LOP
- 5.1.9 Accept Risk
- 5.2.1 Application to New Construction
- 5.2.2 Application to Existing Federal Facilities
- 5.2.3 Modernization and Renovation
- 5.2.4 Application to Lease Solicitations
- 5.2.5 Tenant and Mission Changes in Occupied Buildings
- 5.2.6 Campus Environments
- Appendix B: Countermeasures

D.3.1 Voting Procedures

A vote is permitted only on agenda items identified as decision items. Each federal tenant has one weighted vote. The Office of Management and Budget (OMB) Bureau Code listed in Appendix C of OMB Circular No. A-11 shall be used to define each federal tenant and is located on both the OMB website and the ISC-HSIN website.

Each vote is weighted to the rentable square footage of assigned space (by percentage of total-square footage for the building) for each federal tenant. (see Table D-1).

Table D-1 illustrates how weighted voting is established based on the square footage of occupancy. It is common for a facility to have some joint use and vacant space. Depending on the amount of joint use and vacant space, the FSC may elect not to use the square footage for these areas to determine the pro rata voting share for each tenant. However, in facilities where the owning agency is paying vacant space charges to the security provider, vacant space will be added to the owning agency's pro rata voting share calculation as assigned space and that agency shall have a vote on proposed security countermeasures or changes in security procedures in accordance with *The Risk Management Process for Federal Facilities* security requirements. For example, in GSA facilities where GSA is paying vacant space charges to the Federal Protective Service, the GSA vote shall include that vacant space. To disallow the joint use and vacant space, the FSC can subtract the square footage of the joint use and vacant space from the total square footage of the facility and then recalculate the pro rata voting share for each tenant. Voting to eliminate joint use/vacant space should only be done once.

The FSC Chair can make these calculations for an entire facility by using the ISC Pro Rata Voting Share Calculation Tool located on the ISC HSIN website. **See Section D.7 for instructions on how to use the calculation tool.**

Table D-1: Tenant Voting Percentages Example

Agency Tenant	Agency/Bureau Code	Square Feet	% of total RSF	Pro Rata Voting Share
DOJ – Legal Activities and USMS (includes US Trustees, USMS and US Attorney)	011/05	14,514	28%	28%
DOJ – FBI	011/10	2,248	4%	4%
Courts - (includes Appellate, Bankruptcy, District Courts, Probation/Pretrial Services, Public Defenders)	002/25	25,982	50%	50%
Social Security Administration	016/00	3,522	7%	7%
VA – Benefits Programs	029/25	5,115	10%	10%
DHS – Immigration and Customs Enforcement	024/55	508	1%	1%
TOTAL		52,141	100%	100%

A quorum of the FSC members representing 50 percent of the RSF is required for a vote on a decision item. A decision item passes when more than 50 percent of the facility's tenant agencies' weighted votes are cast in favor of the recommendation. If FSC members representing more than 50 percent of the RSF

are not present for two consecutive meetings, the FSC chairperson may invoke an alternate process to proceed with the vote. If an FSC tenant agency is not able to attend, they may designate in writing that another tenant agency can cast their weighted vote. The meeting minutes must reflect the vote cast by the proxy member. The written designation of the proxy must be retained with the meeting minutes.

D.3.1.1 Decision Item Approval

When an agenda decision item is approved by the FSC, this vote must be recorded in the FSC meeting minutes. If the vote approves the implementation of a security countermeasure, this vote is a financial commitment by each federal tenant in the facility regardless of how each FSC representative voted. If a decision item is approved, all federal tenants in the facility shall provide their prorated share of the cost to fund the countermeasure. The FSC must also approve security countermeasures that are procedural in nature and have no funding implications.

- In a GSA-controlled facility, per the GSA Pricing Desk Guide, 5th Edition, a signature is not required to modify a tenant Occupancy Agreement (OA) when the FSC approves a security feature.
- The security organization, owning or leasing authority, and the organization implementing the security countermeasure should be prepared to accept funding from multiple sources and from mixed fiscal years, if applicable. Funding for a project approved by the FSC is detailed in Section D.4.2 of this document.
- If a facility owner, including GSA, determines that an approved countermeasure may inhibit the effective operations, maintenance, or management of a facility, the FSC may consider alternative proposals received from the owning or leasing authority following written notification from the facility owner that the approved countermeasure is not acceptable. If agreement on alternative proposals cannot be reached, this acceptance of risk will be documented in the FSC meeting minutes. The lessee's requirement to accept risk should be a consideration at the time of lease renewal.

D.3.1.2 Decision Item Disapproval

The meeting minutes must document each federal department or agency vote to approve or disapprove a recommended countermeasure. If a decision item is rejected, the meeting minutes must document the basis for risk acceptance or the alternative risk management strategy that was chosen. The meeting minutes shall be maintained by the FSC chairperson and the security organization as an historical document for the facility. Each member of the FSC and their respective security element at the organization headquarters level shall be provided a copy of the meeting minutes that document the chosen risk management strategy.

D.3.2 Facility Security Committee Chairperson

The FSC chairperson is the senior representative of the primary tenant. The senior person with the primary tenant may designate a senior staff member with decision-making authority to serve as the FSC chairperson; however, the senior representative retains the responsibility for the FSC. Should the senior person with the primary tenant decline to serve as the FSC chairperson, the FSC members shall select a chairperson by majority weighted vote. The FSC chairperson must represent a rent-paying federal department or agency. It is preferred to have an FSC chairperson who is an on-site employee or who regularly visits or works from the facility. He or she is responsible for the following:

- Setting FSC meeting agendas;
- Scheduling FSC meetings;
- Distributing FSC meeting minutes;
- Maintaining FSC meeting records;
- Maintaining training records for all FSC members;
- Coordinating with outside organizations;
- Assigning tasks to other FSC members for drafting plans;
- Maintaining a current list of federal tenant agency occupant status;
- Maintaining a current list of federal tenants' square footage;
- Serving as the point of contact for the FSC between meetings;
- Calling for votes on issues before the FSC;
- Establishing deadlines (not to exceed 45 days from the date all documents and materials are provided to the FSC members to supply to their respective funding authorities) by which each FSC member organization must provide guidance to their FSC representative;
- Casting votes for their organization;
- Facilitating dispute resolution between federal tenants and the security organization; and
- Interfacing with the ISC (i.e., ISC Staff, Standards Subcommittee, etc.) to facilitate a final determination relative to dispute resolution, as deemed appropriate.
- Completing required FSC training.

D.3.3 Facility Security Committee Members

FSC members shall be senior officials with decision-making authority for their organization, able to perform the functions of an FSC member, and able to provide an alternate member to participate if the primary member is unable to attend. Agency representatives will be responsible for making or conveying agency decisions on security measures and funding for their agency. If the FSC member does not have the authority to make funding decisions, the FSC member is responsible for making the appropriate request(s) to their organizational headquarters for funding authorization as well as for the following tasks:

- Representing organizational interests;
- Attending FSC meetings;
- Obtaining guidance on how to vote for issues with funding implications;
- Obtaining assistance from organizational security element; and
- Casting votes for their organization.

New facility tenants shall be included as FSC members no later than 60 days after occupying the facility.

D.3.4 Owning or Leasing Authority

The owning or leasing authority is a voting member of the FSC only if they pay rent for space in the facility. The responsibilities of the owning or leasing authority include the following:

- Completing required FSC training;
- Representing organizational interests;
- Attending meetings;
- Providing technical information;
- Assisting with vendor access to the facility when requested by the security organization; and
- Casting votes for their organization.

D.3.5 Security Organization

The security organization performs the FSL assessment and consults with the FSC and the owning or leasing authority to establish the FSL. Based on the FSL accepted by the FSC, the security organization evaluates the facility using the RMP to determine the baseline LOP and, if necessary, develops a customized LOP to be presented to the FSC for consideration. The security organization is a voting member of the FSC, only if the security organization occupies and pays rent for space in the facility, and is responsible for the following:

- Completing required FSC training;
- Advising the FSC;
- Performing the FSL assessment;
- Presenting the FSL assessment to the FSC;
- Preparing, presenting and distributing a facility security assessment (FSA) in accordance with the time intervals established by the ISC based on the FSL;
- Evaluating the facility to determine whether the baseline LOP is adequate, or whether a customized LOP is necessary;
- Presenting a written plan for proposed countermeasures that identifies how it will mitigate the risks identified with specific credible threats;
- Presenting written operating procedures for countermeasures;
- Presenting written cost impact for proposed countermeasures when requested;
- Providing technical assistance and guidance to the FSC as appropriate; and
- Casting votes for their organization.

D.3.6 Federal Department and Agency Headquarters

Federal department and agency headquarters shall provide funding guidance to FSC representatives as needed. When requested, the physical security element at the headquarters level shall advise and assist the FSC representative. If the FSC representative at a facility is unable to resolve a technical or financial dispute, then the respective security or financial headquarters element for each FSC representative shall assist in reaching a solution.

D.4 Facility Security Committee Operations

The FSC may be asked to consider many issues regarding their facility's physical security. Process charts are provided to aid each FSC when making decisions that will determine the facility's security posture.

If the FSC representatives are unable to resolve an issue, the decision process (see Section D.4.3) flow chart provides an outline for reaching resolution. The objective is for the facility occupants to make decisions for their respective facilities with regard to what countermeasures are implemented. When this is not possible, executive management at the highest level may become involved in the decision process.

D.4.1 Facility Security Committee Business Process

Figure D-1: FSC Business Process outlines the basic steps taken to address decision and discussion items on the meeting agenda. Discussion items allow the FSC to explore and document facility-related issues. If a decision item carries a funding impact, the funding decision process is used (see Figure D-2). If the decision does not carry a funding impact, each FSC representative has the option to request guidance on decision items.

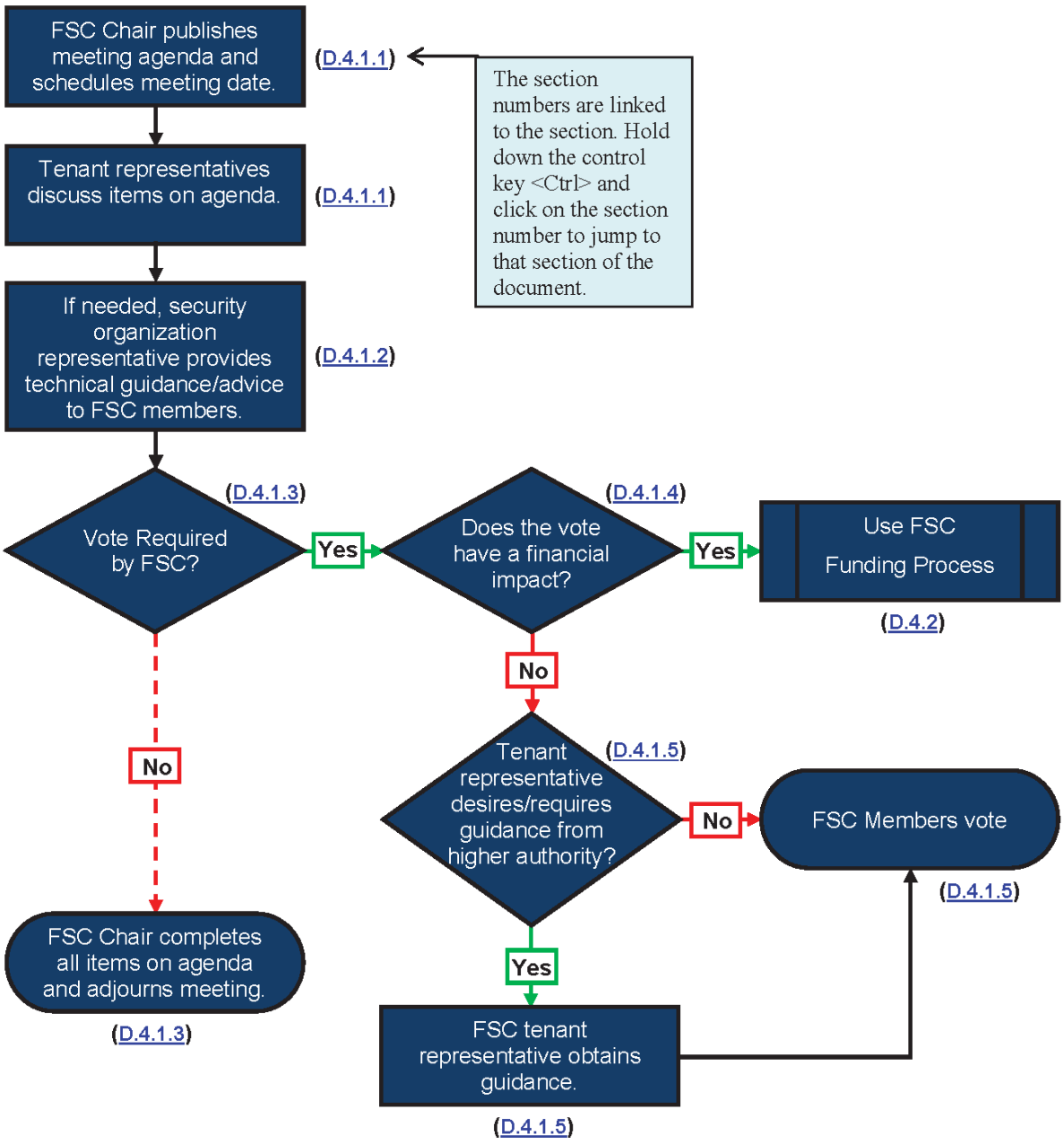

Figure D-1: FSC Business Process

D.4.1.1 Meeting Agenda and Discussions

The FSC chairperson sets and publishes the agenda and schedules the meeting. The FSC representatives review the agenda and agenda items are discussed.

D.4.1.2 Security Organization Guidance

FSC members are representatives for their organizations and may or may not have a physical security background. When the security organization proposes a change to the facility's security posture, the details and rationale of this change may require a technical brief to the FSC and the tenant's respective funding authority, so that each member fully understands the operational and funding impact to their respective operations. The security organization will provide technical assistance, guidance, and any requested documents to FSC members or their respective funding authorities.

D.4.1.3 Decision Point: Is a vote required by the Facility Security Committee?

A vote can be held on meeting agenda items marked as decision items. Discussion items relay information to FSC members and are documented in meeting minutes. A vote is permitted only on agenda items identified as decision items. Once all items on the agenda are addressed, the meeting is adjourned. The FSC voting procedures are detailed in Section D.3.1 of this document. Section D.4.2 of this document addresses processes for decision items that have funding impacts.

D.4.1.4 Decision Point: Does the vote have a funding impact?

A funding impact may be associated with a decision item. Section D.4.2 of this document provides guidance on how to address decision items with funding impacts. Section D.4.1 of this document provides details concerning decision items that do not have funding impacts.

D.4.1.5 Decision Point: Do Facility Security Committee members desire guidance from organizational authority?

FSC members may desire guidance from their respective organizational authority. The FSC chairperson will establish a date for a vote on a decision item, while providing a reasonable period for FSC representatives to obtain guidance from their organization (not to exceed 45 calendar days from the date all documents and materials are provided to the FSC members to supply to their respective funding authorities). If an organization does not provide guidance to the FSC representative within this allotted time, the FSC chairperson may use the decision process or other means as determined by the FSC to obtain a resolution. (see Figure D-3). All FSC votes are recorded in the meeting minutes and distributed to each FSC member and security organization.

D.4.2 Facility Security Committee Funding Process

The FSC will be asked to consider changes to their facility's security posture by adding new policies, changing existing policies, or by implementing or enhancing physical security countermeasures. Generally, policies and procedures do not require funding to implement or change. Countermeasures usually require funding to purchase, install, and maintain the countermeasure (e.g., purchasing of equipment or hiring of guards). When the FSC considers items that require funding, each FSC member is responsible for seeking guidance from their respective funding authority. The security organization or implementing agency is responsible for providing assessments, available supporting documentation, and cost estimates to funding authorities. Figure D-2 outlines the funding decision process.

The FSC chairperson shall establish a date for a vote on a decision item requiring funding, while providing a reasonable period for FSC representatives to obtain guidance from their respective authority (not to

exceed 45 calendar days from the date all documents and materials are provided to the FSC members to supply to their respective funding authorities).

If guidance is not provided to the FSC representative within this allotted time, the FSC chairperson may use the decision process, or other means as determined by the FSC, to obtain a resolution. The meeting minutes must document each federal department's or agency's vote to approve or disapprove a recommended countermeasure. If a countermeasure is not approved, the FSC accepts the associated risks related to that decision.

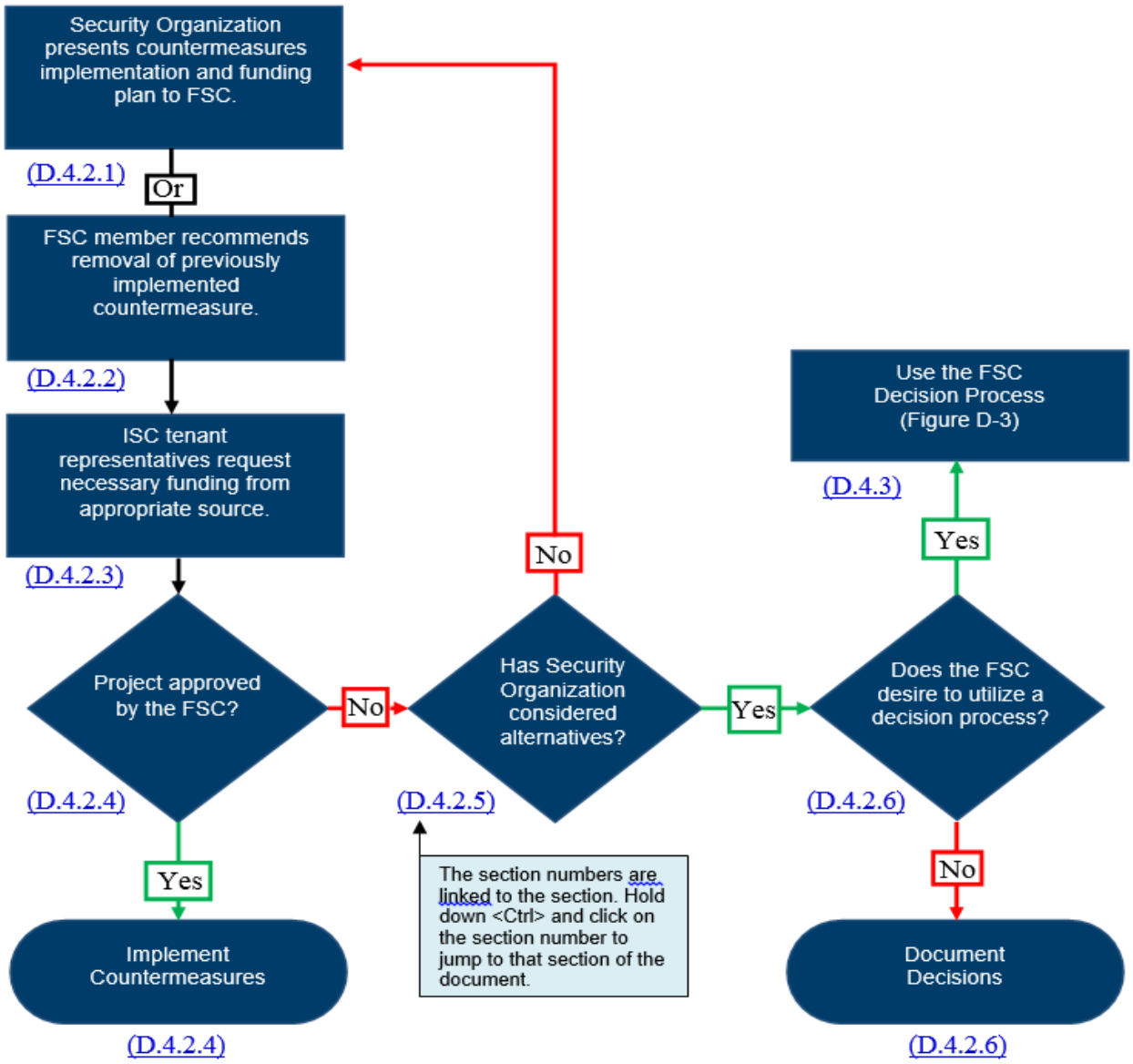

Figure D-2: FSC Funding Process .

If an FSC fails to provide a response on a countermeasure recommendation, the FSC should document the decision not to respond, as well as the justification for the decision, in the meeting minutes. If a countermeasure is not brought for vote, the FSC accepts the associated risk relating to that decision.

D.4.2.1 Security Organization Presents Countermeasures Implementation and Funding Plan to the Facility Security Committee

The security organization or implementing organization or agency will develop a proposal for each new or enhanced countermeasure. This plan must include the following elements:

- Estimated cost of countermeasure.
- How the countermeasure will mitigate the risks identified with specific credible threats to include operational procedures.
- How the countermeasure meets the necessary LOP as called for in the ISC's *Appendix B: Countermeasures* to include any cost-saving benefits.

D.4.2.2 Facility Security Committee Member or their Funding Authority Requests Removal of Previously Implemented Countermeasure

There are numerous facilities with security countermeasures in place that may or may not have been approved by a vote of the FSC. As these countermeasures may have financial impact on the tenant organizations, there shall be a mechanism to cancel or remove previously implemented countermeasures.

When a tenant organization is notified by their funding authority or headquarters security element that funding for a countermeasure is no longer available, or that the countermeasure is not required by the facility's baseline LOP or assessed risk, the tenant agency or their funding authority or security element will present an agenda item to remove the countermeasure to the chairperson of the FSC.

The decision to remove or discontinue the countermeasure will be based on a majority of the tenant agencies pro rata vote. Tenant organizations are responsible for all costs associated with removal. When removal of a countermeasure is approved, the agency responsible for the implementation shall cease or remove the countermeasure by the date specified by the FSC.

D.4.2.3 Facility Security Committee Members Request Guidance From Their Respective Funding Authority

An FSC member may or may not have the authority to obligate their respective organization to a funding commitment. When the member does not have funding authority, financial guidance from their respective funding authority is necessary.

The security organization or implementing agency shall provide a detailed description of work and cost estimates for the proposed countermeasure to each tenant agency or their respective security element or funding authority.

The FSC chairperson will establish a date for a vote on a decision item, while providing a reasonable period for FSC representatives to obtain guidance from their organization (not to exceed 45 calendar days from the date all documents and materials are provided to the FSC members to supply to their respective funding authority). If an organization does not provide guidance to the FSC representative within this alloted time, the FSC chairperson may use the decision process, or other means as determined by the FSC, to reach a resolution (see Figure D-3).

D.4.2.4 Decision Point: Did the Facility Security Committee vote to approve the proposed security proposal?

FSC members vote to approve or disapprove each proposed countermeasure based on the guidance provided by their respective authority. If approved, each countermeasure is implemented. Procedures for handling proposed countermeasures that are not approved are presented in Section D.5.2.2. When the FSC votes to deny the implementation of a security countermeasure(s) that exceeds the baseline standard for the LOP of a building of its specific FSL, the FSC will have accepted risk as an integral part of the committee's risk management strategy.

D.4.2.5 Decision Point: Has the security organization considered alternatives?

This decision point is an iterative loop for the purpose of facilitating technical discussions between the security organization and the security elements of the FSC members. Discussions help promote creative thinking and evaluate multiple countermeasures to mitigate risk. If certain risks are accepted, the FSC must document the basis for the chosen risk management strategy. See Section D.2.2 for more information on risk acceptance.

D.4.2.6 Decision Point: Does the Facility Security Committee desire to utilize a decision process?

When the security organization has explored alternatives and funding is not available for the countermeasure(s), the decision is either documented or the FSC chairperson can implement a decision process. For more information on the ISC's recommended Decision Process, see Section D.4.3 of this document.

D.4.3 Decision Process

Each FSC will face many decisions regarding their federal facility's security posture. FSC members have the best perspective to determine what the appropriate level of security should be for their facility. There will be times when FSC representatives require guidance from security and financial subject-matter experts at their respective headquarters. If the decision process is used on a countermeasure(s) that leaves the facility vulnerable, the risk for this vulnerability or vulnerabilities will be accepted until the final decision is reached.

The decision process example illustrated in Figure D-3 is a general guide. An FSC may adopt an alternate process to facilitate a decision. The organizational structure used by each federal department and agency may be different. FSC representatives are responsible for determining the appropriate management level to contact within their respective organization for guidance and assistance.

The ISC's Decision Process allows the FSC four opportunities to reach a decision. In the rare event an FSC is unable to reach a decision, the executive level of management for each federal department and agency at the facility will be presented with the information. Once a decision is made for the facility, the responsibility to implement and manage this decision is returned to the FSC members for action.

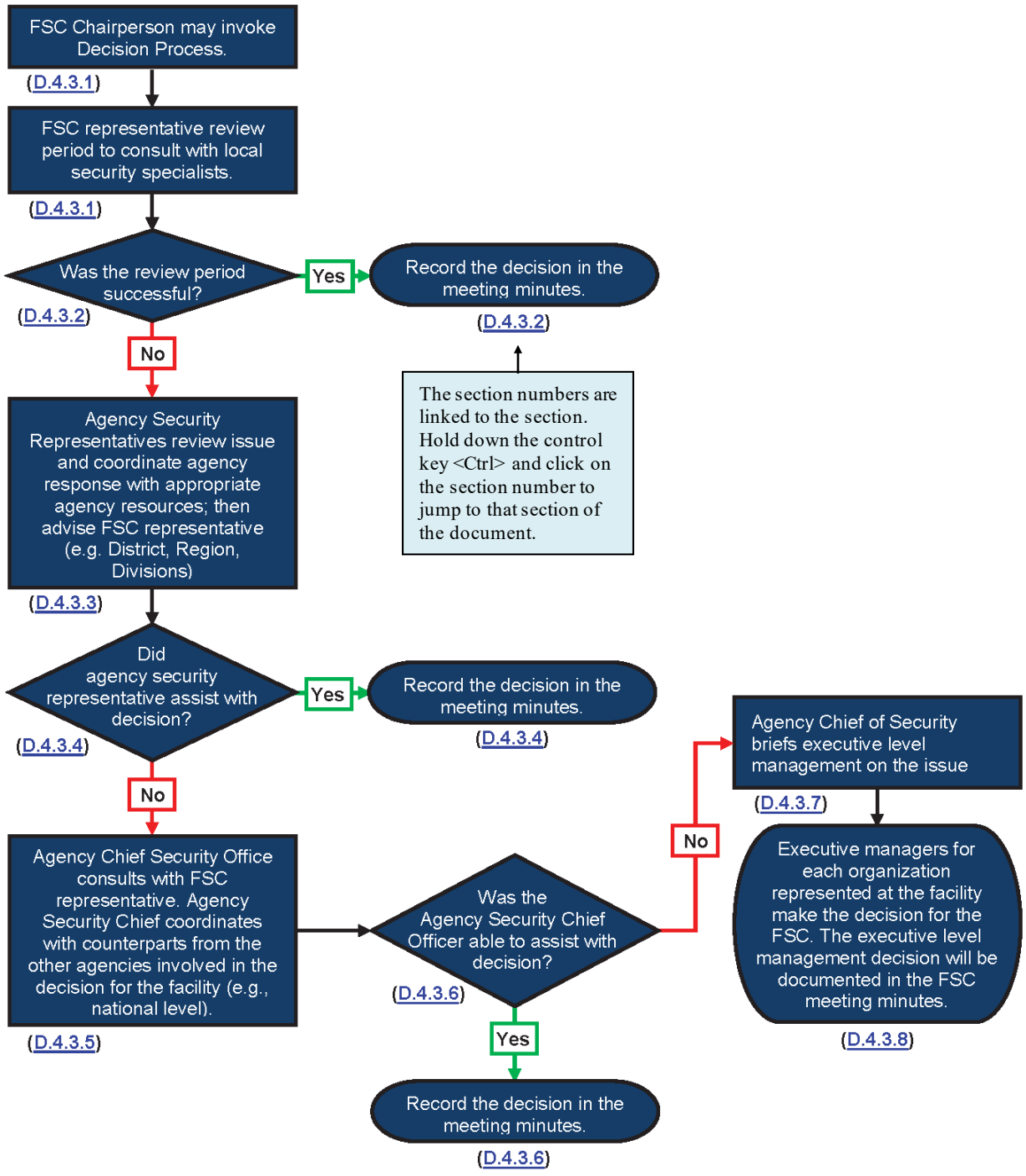

Figure D-3: Example Decision Process

D.4.3.1 Facility Security Committee Chairperson Invokes Decision Process

The FSC chairperson has the option to use the decision process should the discussions become unproductive. FSC representatives are allowed a review period to consult with their respective organizational security element for guidance when additional information is needed. Each FSC chairperson will establish a reasonable period (not to exceed 45 calendar days) for FSC representatives to obtain guidance from their organizations.

D.4.3.2 Decision Point: Was the review period successful?

If the review period was successful, the results are recorded in the meeting minutes. Votes are taken as required. If the review period was unsuccessful, then the FSC proceeds to the next step in the decision process.

D.4.3.3 Organizational Security Element Assistance

The physical security component from each of the facility's organizations participates in a review of the issue before the FSC does and provides guidance to the FSC representative. The physical security specialists for each organization should conduct an onsite review as a team. Security specialists evaluate the facility and the security organization's proposal and then look for ways to modify the proposal to an acceptable plan. If a modified proposal cannot be developed, the security representatives and the security organization will work together to develop alternative proposals and an FSC vote will be scheduled.

When the FSC representative contacts their respective organization and requests assistance, this step in the decision process must be completed within 30 calendar days of the initial contact. The FSC may vote to extend the 30-calendar-day timeframe. If a resolution is not reached in the agreed upon timeframe, the issue(s) in question shall be referred to each respective organizational senior security-official for action.

D.4.3.4 Decision Point: Did the organizational security element assistance resolve the issue?

If the review period was successful, the results are recorded in the meeting minutes. Votes are taken as required. If the review period was unsuccessful, then the FSC proceeds to the next step in the decision process.

D.4.3.5 Organizational Senior Security Official Review

The senior security-official from each of the facility's organizations will conduct an analysis of the issue in question, then work with representatives from the facility, their counterparts from the other represented organizations, and the organizational representatives from the facility to develop a plan that each organization finds acceptable. This plan is briefed to the organizational FSC representatives at the facility for their consideration and an FSC vote is scheduled.

This step in the decision process must be completed within 30 calendar days of being referred to each respective organizational senior security-official. The FSC may vote to extend the 30- calendar-day time frame. Should a resolution not be reached in the agreed upon time frame, the issue(s) in question shall be referred to each respective organization's executive level management for action.

D.4.3.6 Decision Point: Were the Senior Security Officials able to resolve the issue?

If the review period was successful, the results are recorded in the meeting minutes. Votes are taken as required. If the review period was unsuccessful, the FSC proceeds to the next step in the decision process.

D.4.3.7 Organizational Senior Security Official Briefs Executive-Level Management

The senior security-official for each organization represented at the facility briefs their organizational executive level management on the issue in question. The executive level management for each organization represented at the facility will work with representatives from the facility, their counterparts from the other represented organizations, and organizational representatives from the facility to make a decision on behalf of the facility.

This step in the decision process must be completed within 30 calendar days of being referred to each respective organizational executive level management. The FSC may vote to extend the 30- calendar-day-decision process. Should a resolution not be reached in the agreed-upon timeframe, the FSC can request assistance from the ISC Steering Committee, or the risk can be accepted.

D.4.3.8 Executive Level Management for Each Organization Represented at the Facility Agrees on a Decision for the Facility

Organizations have four opportunities to resolve an issue with facility-level input before the issue reaches the executive level for resolution. Should an issue rise to executive level for resolution, a final decision will be made and the facility will implement this decision. The executive-level management decision will be documented in the FSC meeting minutes.

D.5 Funding

Federal departments and agencies will be asked to provide funds for security countermeasures for federal facilities. The funding and security functions should work together when funding requests are considered. The decision to provide funding or accept risk should be based on the FSL, a risk assessment, and the baseline or customized LOPs.

D.5.1 Funding for a Non-Unanimous Vote

If the FSC votes to approve a countermeasure, federal tenants are required to fund their prorated share of the cost, even if their FSC representative voted to disapprove the countermeasure.

D.5.2 Facility Security Committee Member Funding Authority

A voting FSC member may or may not have funding authority. If an FSC member does not have funding authority and a decision item requires funding, the FSC representative shall seek guidance from their respective security and funding authority. The headquarters' security function and funding authority shall work together to provide guidance to the organizational FSC representative.

D.5.2.1 Approval of Funds

When funds are approved, each federal department or agency must advise their FSC representative as to which fiscal year the funds will be available. When funds are sought from a future appropriation year, the headquarters' security element must track the funds and keep their FSC representative informed of changes relating to appropriation or authorization.

D.5.2.2 Disapproval of Funds

Should a federal department or agency not approve funds, but the FSC votes to approve a countermeasure, the federal department or agency is responsible for providing funds for their prorated share of the cost of the approved countermeasure.

When a federal department or agency does not approve funds, the decision then results in risk acceptance. The headquarters' security element shall document the denial of funds and the risk acceptance to the facility. A copy of this documentation shall be provided to the organizational FSC representative. The FSC representative shall provide a copy of the denial of funding and risk acceptance documentation to the chairman of the FSC in order for the information to be included in the FSC meeting minutes.

D.5.3 Funding Documents

Transferring funds from one organization to another may be accomplished in several ways. It is beyond the scope of this document to detail each method of transferring federal funds. The agency implementing the countermeasure must determine how the countermeasure will be procured. Each FSC member must contact their respective financial authority for guidance on how to transfer funds and in what fiscal year the funds will be available. The agency implementing the countermeasure is responsible for providing each FSC representative with the necessary information on the specific method(s) to be used for transferring federal funds.

D.5.4 Funding Impact to Occupant

When the facility security organization presents a plan to the FSC for consideration, a written funding plan must be provided to each FSC member. This funding plan will include the project cost for the facility, and the cost per square foot to each federal tenant will be calculated.

The decision to implement security countermeasures or accept risk at a facility contains a financial component. To address this area, the security organization must provide a cost analysis that indicates the cost effectiveness of the proposed countermeasure and include projected costs for subsequent fiscal years. This analysis will follow the performance-measurement methodology outlined in the *Appendix E: Use of Physical Security Performance Measures*.

D.5.5 Occupancy Agreement

Federal tenants may have the option to work with their owning or leasing authority to fund security countermeasure projects by means of rent increases. A rent increase usually requires a change to the occupancy agreement to adjust the amount of rent paid to the owning or leasing authority.

D.6 Record Keeping

Meeting minutes, and other documents or information the FSC deems important, shall be retained as building-specific records. All FSC decisions shall be documented in the meeting minutes. Vote tabulation shall be recorded in the meeting minutes. Project funding approval, disapproval, and risk acceptance information shall be documented in both the meeting minutes and the Facility Security Assessment. It is recommended that the FSC and the security organization maintains copies of records for a minimum of two assessment cycles.

The National Archives and Records Administration (NARA) provides guidance on records retention for FSCs in its General Records Schedule 5.6.[7]

D.6.1 Purpose

Building and occupant-specific information shall be retained to provide a historical record of each FSC decision.

D.6.2 Format of Records

Records shall be maintained electronically, whenever possible, and subject to the E-Government Electronic Records Management Initiative.

D.6.3 Access to Records

All FSC members, and their funding authority and security element, will have access to meeting records. Additional access to FSC records held by other agencies will require the FSC's approval. Records containing National Security Information (NSI) or sensitive information shall only be released to appropriately cleared personnel with the need-to-know.

D.7 The ISC Pro Rata Voting Share Calculation Tool

The FSC chairperson may determine each federal agency tenant's pro rata voting share by using the ISC Pro Rata Voting Share Calculation Tool, which is located on the ISC HSIN web-site. The following instructions outline how to complete the necessary calculations.

1. List the total Rentable Square Footage (RSF) obtained from the owning/leasing authority.
2. List separately each agency tenant who is an occupant of the facility as listed in Appendix C of OMB Circular 11A.
3. Enter the rentable square footage of each separate agency tenant's assigned space.
4. Finally, to calculate the agency's share of the vote, click in the Pro Rata Voting Share column for each separate agency tenant. (The tool will automatically make the calculations and populate the Pro Rata Voting Share column. As each separate agency tenant is either added to or deleted from the tool, the tool will automatically recalculate all pro rata voting shares.)

[7] NARA guidance can be found here: https://www.archives.gov/files/records-mgmt/grs/grs05-6.pdf

Table D-2: Example of the Pro Rata Voting Share Calculation Tool

Agency Tenant	Agency/Bureau Code	Square Feet	% of total RSF	Pro Rata Voting Share
Social Security Administration	016/00	3,522	41%	41%
VA – Benefits Programs	029/25	5,115	59%	59%
TOTAL		8,637	100%	100%

Appendix E: Use of Physical Security Performance Measures

E.1 Introduction

Performance measurement data is essential to appropriate decision-making about the allocation of resources. Objective, unbiased information about what is being accomplished, what needs additional attention (management focus and resources), and what is performing at target expectation levels is vital to decisions regarding resource allocation. Security countermeasures must compete with other program objectives for limited funding. Performance measurement tools offer security professionals a way to measure a program's capabilities and effectiveness and can help demonstrate the need to obligate funds for facility security.

E.1.1 Cautionary Note

Although performance measurement and testing are necessary for effective management and oversight, they can become burdensome if senior management does not use them properly. The Government Accountability Office (GAO) observed in study GAO-6-612 that "agencies face obstacles in developing meaningful, outcome-oriented performance goals and in collecting data that can be used to assess the true impact of facility protection efforts." The GAO noted further that "in some programs, such as facility protection, outcomes are not quickly achieved or readily observable or its relationship to the program is often not clearly defined."[8] Without consistent management support, performance measurement and testing are counterproductive and could evolve into ends in themselves rather than serving as a means of ensuring program success.

Overcoming these obstacles will require sustained leadership, long-term investment, and clearly-defined performance goals, metrics, and data. The costs associated with developing the initial requirements, particularly to establish performance databases, will require significant front-end funding. At the agency level, leadership must communicate the mission-related priority and commitment assigned to performance measurement actions. Management attention will also be required at the facility level to ensure buy-in and cooperation among facility operators, security managers, building occupants, and other stakeholders. If management can meet these challenges, the physical security performance measures will help to ensure accountability, prioritize security needs, and justify investment decisions to maximize available resources.

E.1.2 Policy

Pursuant to Section 5 of Executive Order (E.O.) 12977, the following policy is hereby established for the security and protection of all buildings and facilities in the United States occupied by federal employees for nonmilitary activities. Federal departments and agencies shall take the necessary action to comply with the following policies as soon as practicable:

- Federal departments and agencies shall assess and document the effectiveness of their physical security programs through performance measurement and testing;
- Performance measures shall be based on agency mission goals and objectives; and

[8] Please see: http://www.gao.gov/new.items/d06612.pdf, accessed 24 Feb 2015.

- Performance results shall be linked to goals and objectives development, resource needs, and program management.

E.2 Guidance

This guidance is provided to assist departments and agencies with establishing or refining a comprehensive measurement and testing program for assessing the effectiveness of their physical security programs. Within large agencies or departments, security performance measurement and testing might best function at the major component organizational level (bureau, directorate, or office) and its field locations rather than at the senior management headquarters level. Nonetheless, senior management—the senior security official or equivalent—should ensure the consistent application and testing of performance measures throughout the agency or department.

E.3 Performance Measures

Performance measures can be categorized into three basic groups: input/process measures, output measures, and outcome measures. For consistency in the assessment of physical security programs' effectiveness, the following definitions apply.

E.3.1 Input/Process Measures

Inputs are the budgetary resources, human capital, materials and services, and facilities and equipment associated with a goal or objective. Process measures are the functions and activities that are geared toward accomplishing an objective.

E.3.1.1 Input/Process Measures Examples

The following are examples of input measures, including descriptions explaining how they relate to program assessment:

- **Asset Inventory**: This measure may encompass the entire facility asset inventory or a subset. For example, program managers could measure only those assets that have been (or need to be) assessed to those whose level of risk is acceptable. The inventory measure could also reflect various classifications to establish priorities, such as the facility security level (FSL) designations, or other mission-driven criteria. Depending on the status, program managers should establish intermediate and long-term target objectives for the asset inventory for tracking and achieving long-term goals. An example of this is a measure indicating whether all assets have an acceptable risk rating.
- **Number of Countermeasures in Use**: Similar to the inventory of facilities, this measure provides a baseline for the number of countermeasures (by type) requiring maintenance, testing, or scheduled for replacement. This number may increase or decrease as the asset inventory fluctuates, or recurring risk assessments indicate the need for additional security equipment. As the number of countermeasures in use increases and the number of tested and repaired or replaced countermeasures increases, the acceptable risk rating should also increase for your asset inventory as suggested in the first example.
- **Resource Requirements**: These measures track the resources required to accomplish the security program mission:
    - Full-Time Equivalent (FTE) employees, contract support, and training;

- FSL determinations and risk assessments;
- Countermeasure installation, maintenance, testing, evaluation and replacement; and
- Overall Security Program Management (salaries, information technology cost, administrative cost).

Tracking the resources applied to physical security efforts provides program managers with an understanding of the necessary resources, including expenditures and personnel, required for effective physical security program operations. Program managers can use this information to determine program growth, increases in cost, efficiency gains, and output costs. Essentially, this information provides an overview of the resources required to achieve program goals and to accomplish overall program mission goals. When considered in conjunction with output and outcome measures, they help determine the benefit of using various resource levels. Moreover, program managers should use this information to plan and justify resource requirements for future efforts.

E.3.2 Output Measures

Outputs are the products and services the organization produces that generally can be observed and measured. Efficiency is a measure of the relationship between an organization's inputs and outputs.

E.3.2.1 Output Measures Examples

The following are examples of output measures and how they relate to assessing program effectiveness:

- **Security Assessments Completed Versus Planned**: A core component of a physical security program is the scheduling of initial and recurring risk assessments and the accompanying FSL determination. Every agency or department should have an established schedule for assessing each facility. Tracking and measuring the percentage of completed assessments versus what was planned for the year, by quarter, or other period indicates management's commitment to maintaining an organized and efficient physical security program. More importantly, risk assessments performed on a regular schedule provides a means of effectively addressing changes in threats and vulnerabilities, and corresponding countermeasure needs. A typical target objective would be to complete a specific number of assessments annually, based on a planned schedule.
- **Countermeasures Deployed**: This measure reflects how well the deployment of countermeasures is managed throughout the procurement, installation, and acceptance cycle. Once funding has been made available, target dates (e.g., a specific date, month, or quarter) should be established. This target date is then compared with the actual deployment "date." If there is no existing data available for projecting a reasonable target date, a baseline should be established using representative countermeasures to determine the typical time frame for deployment of various kinds of countermeasures. This enables the manager to reasonably project target dates for future countermeasures. A typical target objective for this measure may be to deploy all fully-funded countermeasures on time (on or prior to the scheduled date) 95 percent of the time. The five percent margin of error allows for unforeseen events or circumstances that could not have been reasonably anticipated when the target dates were initially established. Once actual results are achieved, incremental improvement target dates may be necessary until the processes, planning, and scheduling procedures can be refined to ensure successful deployment 95 percent of the time. Note: This measure encompasses capital investments, facility enhancements and equipment, new process changes, and countermeasure activities. Separate reporting is encouraged for each of

these categories since the responsibility for each may differ, and corrective process improvements vary, among the organizational elements involved.

- **Countermeasures Tested**: This measure focuses on accomplishing an established schedule for testing[9] countermeasures to determine how well they are working. Testing encompasses such elements as determining whether or not equipment is calibrated properly, security guards are knowledgeable in post order procedures, and intrusion detection systems are activating properly. For critical infrastructure, testing may include planned exercises to breach security to ensure existing countermeasures are capable of securing the facility against the most sophisticated attempts to illegally access the facility. All testing should be based on an established set of testing protocols. As individual facilities may have numerous countermeasures in place, it is unrealistic to attempt to test all countermeasures annually. Random sampling may be necessary for larger facilities.

- **Incident Response Time**: This measure is suitable for a number of security-related requirements, but only when the security manager has operational control over response capability, or has negotiated a service agreement with a response provider. Use of this type of measure usually requires a baseline assessment of existing average response times. This average should be compared with a benchmark or desired standard. If there is a high volume of incidents within a given facility inventory and there is no automated time recording database available, random sampling of incidents may be necessary. Sampling should be large enough to reflect normal operational circumstances. Incremental performance target objectives may be necessary to guide development of improved procedures and future funding needs.

E.3.3 Outcome Measures

Outcomes or results represent the organization's upon its customers. Results are often classified in terms of the achievement of a desired condition, the prevention of an undesired condition, or user satisfaction. Effectiveness is a measure of the relationship between an organization's processes and results.

E.3.3.1 Outcome Measures Examples

Outcome measures are used to assess the cumulative results of output activities in achieving objectives. These measures indicate how well individual tasks or target objectives contribute to the accomplishment of broad-based security program goals. Outcome measures may support more than one program objective or goal. Examples include:

- **Facility Asset Inventory Secured (Strategic Goal)**: This measure reflects the cumulative impact of reducing individual facility risk levels through the deployment of security countermeasures throughout the asset inventory. The strategic goal is to achieve and sustain an acceptable risk rating for all facilities. Tracking this strategic goal is a multi-year process. The risk rating is reflective of countermeasures in place and working properly throughout the inventory. An acceptable risk rating may be defined based on a scoring system for evaluating the perimeter,

[9] Testing - Encompasses those procedures used to assess the performance of security equipment, security guards, and emergency planning and response. Security equipment testing includes, but is not limited to, alarm/detection systems testing, examining equipment calibration, detection of training weapons and other simulated contraband, and appropriate positioning of surveillance equipment.

facility envelope, and interior security features of an asset, or it could be simply defined as being ISC standard compliant.

- **Emergency Preparedness (Strategic Goal)**: This measure focuses on the degree to which employees and senior management are trained and perform up to expectations in emergency training exercises. It reflects the cumulative results of Continuity of Operations Plan (COOP) activation training exercises, Occupant Emergency Plans (OEP) drills, and other emergency exercises. Assuming all output measure target objectives are met, a typical strategic outcome goal for this measure might be to achieve an overall 98 percent success rate in accordance with expected behaviors.

- **Program Efficiency (Program Goal)**: This outcome measure is intended to capture the cumulative effect of individual process efficiency initiatives (outputs). A typical long-term goal might be to limit overall security program cost increases to a variable percentage per year. The results of individual efficiencies must be tracked, recorded, and summed.

E.3.4 Note on the Examples

The examples included above are provided for agencies as they develop or refine their performance measurement program. They may be adopted or modified to meet their particular mission and program needs. Departments and agencies should utilize only those measures suitable to and supportive of their particular physical security program. Variances within department or agency components in both number and content may also be appropriate due to program or budgetary constraints. In short, the examples below are provided to assist departments and agencies, and their components, in developing the measures that best suit their needs. Additional comments can be found in *Appendix B: Countermeasures* (FOUO).

E.3.5 Performance Measurement Process Chart

The following chart (Table E-1) illustrates how performance measures tie to mission, goals, objectives, specific actions (outputs), and outcomes. This hypothetical example is based on the mission of securing all facilities and a goal of ensuring all facilities comply with Interagency Security Committee (ISC) security standards within 36 months. To achieve the goal, two program objectives were established. The first objective was to assess all 100 hypothetical agency facilities within 18 months; the second objective was to deploy all approved security measures within 18 months after the last assessment is completed. The chart identifies several tasks or actions required to accomplish the objectives, but they should not be viewed as all-inclusive. In the example, the results indicate some delay, but overall the delay in approving all recommended countermeasures did not adversely affect the accomplishment of the goal within the target timeframe. The bottom portion of the process chart shows how the input, output, and outcome measures support each phase of the process. Ultimately, the goal of ensuring all facilities are compliant with the ISC or a comparable Agency Standard within 36 months was achieved.

Table E-1: Performance Measurement Process Chart

MISSION: Secure Facilities		
GOAL: Ensure all [agency] facilities are ISC compliant within 36 months.		
Objectives	**Actions**	**Results**
1. Assess all 100 [agency] facilities for compliance within 18 months.	1. Complete all scheduled risk assessments on time (quarterly schedule). 2. Obtain consensus/approval on recommended countermeasures within 45 days of risk assessment.	100 percent of risk assessments completed on time. Eighteen (18) facilities compliant. 90 percent of recommended countermeasures approved within 45 days (Remaining 10 percent approved within 60 days).
2. Implement corrective measures as needed within 18 months of last assessment [date].	1. Identify priority countermeasures; coordinate as appropriate with facility managers. 2. Award contract(s) for countermeasures installation by [date]. 3. Conduct post-deployment ISC compliance inspection.	250 Countermeasures identified as needed to make facilities ISC compliant. Five contracts awarded to install 250 countermeasures in 82 facilities within 18 months of last risk assessment [date]. All countermeasures installed and validated by [date].

Inputs	Outputs	Outcome
1. Necessary travel and support funding budgeted.	1. 100 approved assessments.	1. All 100 [agency] facilities are ISC compliant within 36 months.
2. Quarterly risk assessment schedule developed with dates.	2. Approved countermeasures prioritized.	2. Goal achieved.
3. Estimated countermeasure purchase and installation funding budgeted.	3. Countermeasures deployed within 18 months of last risk assessment [date].	3. Goal achieved.
4. Countermeasure installation plan developed and approved (Multiple contracts).	4. Post countermeasure deployment inspection reports completed.	4. Goal achieved.

E.4 Performance Measurement Implementation

Performance measures are a useful tool for decisionmakers at all levels. Program managers, at the agency headquarters level, use performance measures to determine if their security program is accomplishing or supporting the agency's mission, goals, and objectives. Field level managers may use performance measures to demonstrate program effectiveness to stakeholders, assess emergency preparedness capabilities, oversee security-equipment maintenance and testing programs, and determine the adequacy of resources to support operational security requirements. Physical-security-related performance measures provide valuable information used to support funding requests, accomplish program goals and identify areas for improvement, and process change or additional training.

E.4.1 Headquarters and Field Level Interaction

Implementing a performance measurement program at the agency level is required to link the specific measures to the agency's established goals. Generally, a strategic plan contains one or more goals, which impacts or requires the direct support of the physical security program operations over a multi-year time span. Therefore, performance measurement initiatives at the agency headquarters level are also generally multi-year efforts with phased implementation aligned with the agency strategic plan. At the field level, performance measurement activities must support the agency level goals and objectives. However, they may include measures aimed at assessing and demonstrating the effectiveness of the security program at the local level in ways different from the agency program measures. These field performance measures may be short-term or multi-year initiatives.

The Performance Measurement Process Chart (Table E-1) illustrates the implementation of an agency headquarters level goal [ensure all facilities are ISC compliant within 36 months] with two supporting objectives [assess 100 facilities within 18 months and implement corrective measures within 18 months of the last assessment]. These two objectives support the goal of achieving ISC compliance with a three-year timeframe for the entire organization. At the field level, the security program manager may be heavily involved in conducting the risk assessments and, once funding is available, implementing the approved countermeasures. The security program manager may also be involved in measuring the time and resources needed to complete individual assessments or the time required to obtain full approval of recommended countermeasures. This information may be helpful in justifying additional resource requirements necessary to meet the headquarters assessment schedule or to initiate process changes to reduce approval timeframes. The security program manager may track the accuracy of countermeasure deployment costs compared to the budget provided by headquarters. This will provide valuable information in developing input measure data for preparing a future budget submission.

The field manager may also establish local objectives. For example, the manager may establish a performance objective to develop and issue revised guard orders addressing the use of the new security equipment recommended in the required risk assessments. This output measure could be based on measuring the planned versus actual issuance date, using the date of countermeasure deployment as the planned date. Another example of a field manager establishing a performance measure is testing existing countermeasures to ensure they are working properly, such as setting a goal of 99 percent effectiveness. Testing confirms the reliability, or lack thereof, of maintenance programs, ensures credibility with facility occupants, and provides empirical data to support countermeasure replacement if necessary, all of which would be essential to support the conclusion that all facilities are ISC compliant. Whether the performance measures are driven by agency headquarters goals or field manager initiatives, all performance measures should provide a basis for assessing program effectiveness, establish objective data for resource and process improvements, and lead to overall security program effectiveness.

Goals and objectives established at the headquarters or field level illustrate the effective use of performance measures that requires a collaborative effort. The team should be led by the security professional, but should include budget, procurement, and facility management officials and, where appropriate, human resource and training officials. Each participant should be fully briefed and share a common understanding of the measurement initiative, including an understanding of the actual measures, definition of terms, data sources, and most importantly, a commitment to utilize the results to improve program performance.

E.5 Conclusion

The guidance in this document provides the foundation for a measurement program that will endure, both in terms of the metrics themselves and in the use of performance measurement as a management tool. The use of performance measurement and testing is one of six key management practices the ISC is promoting within the federal physical security community. Combined with future ISC management documents, ISC membership seeks to achieve consistent, professional, and cost-effective management of physical security programs across the federal government that will improve the protection of and security within federal facilities.

Table E-2: Quick Reference Guide

Type	Category	Example	Purpose
Input/ Process Measures	Asset Inventory	Number of facilities, number assessed, number at acceptable level of risk	Program scope identification
	Countermeasures in Use	Countermeasure Inventory by type: guards, VSS, magnetometers, x-rays, canines, blast protection, vehicle barrier protection, etc.	Program scope, resource development, countermeasure repair/replacement cost base, testing inventory
	Resources Requirements	FTE (number and salary), FSL and risk assessment workload, countermeasure procurement, installation, maintenance, and testing costs; database expense; contract support; training; travel; contract security guards; equipment	Oversight, program management, efficiency targets, trends/projections
	Process Governing Approval of Facility Security Assessment (FSA)	Track time and costs from initial completion to final approval of the FSA recommendations	To maximize efficient use of resources (human capitol)
Output Measures	Security Assessments Completed	Percentage of planned assessments completed within the timeframe	Program management (annual target objective), stakeholder communication
	Level of Risk	Number/Percentage of facilities at acceptable risk levels (e.g., ISC compliant), annual target/incremental improvement	Program management, stakeholder communication
	Countermeasures Deployed	Installation/deployment schedule, (percentage of planned completed by target date); track procurement, installation, and acceptance progress	Program management, stakeholder communication
	Countermeasures Needed (backlog)	Inventory of new and replacement countermeasures (annual backlog reduction target)	Program management
	Countermeasures Tested	Testing schedule, (percentage passing vs. failed) annual target leading to long-term performance objective	Program management, assessment validation

Type	Category	Example	Purpose
Output Measures (Cont'd)	Response Time	Time required for responders (guard, law enforcement, emergency response technician) to arrive/initiate response protocol	Program management, response readiness, stakeholder's trust/confidence
	Emergency Exercises	OEP, COOP exercises (actual vs. expected behaviors); after action report assessment	Emergency response enhancement, program management, stakeholder communication
	Stakeholder Satisfaction	Tenant or customer satisfaction assessment (survey); annual improvement targets	Program assessment, stakeholder confidence, identification of areas needing improvement
	Development and Training	1. Staff development (scheduled training vs. actual) 2. Customer training (crime awareness, security training) planned vs. actual	Program development, stakeholder communication and feedback
Outcome Measures	Inventory Secured	All facilities are protected to an acceptable risk level rating and are ISC compliant	Strategic goal accomplishment, facilities equipped with adequate countermeasures
	Security Measures Working	Security countermeasure inventory working at strategic goal level	Strategic goal accomplishment, security measures are effective
	Emergency Preparedness	Employees, contractors, senior management trained and prepared to response to emergency incident	Strategic goal accomplishment, OEP, COOP Plans validated, and employees prepared based on successful training
	Incident Reduction	Security violations, thefts, vandalism reduced	Strategic goal accomplishment, inventory experienced fewer security violations, etc.
	Program Efficiency	Physical Security program operating more efficiently	Strategic goal accomplishment, mission accomplished within resources/more cost-effective delivery

Appendix F: Forms and Templates

NOTE: Document becomes FOR OFFICIAL USE ONLY (FOUO) when filled in.

Example of a Risk Acceptance Justification Form:

Person Completing Form:			Date:
Organization:			Title:
Email:			Phone:
Facility Profile			
Facility Name:			Identifier/Bldg #:
Address:			
City:		State:	Zip:
Facility Security Level			
FSL		Date of FSL	Previous FSL
Factor	**Score**	**Rationale**	
Mission Criticality			
Symbolism			
Facility Population			
Facility Size			
Threat to Tenant Agencies			
Preliminary FSL			
Intangible Adjustment			
Risk Assessment Information			
Site Visit Start Date		End	Date of Report
Conducted By			Title
Organization			Phone
Email			Cell
Software or Methodology			

Risk Acceptance

For Each Recommendation that will not be fully implemented:

1. Summarize the recommendation, including the undesirable event being addressed.
2. Identify the necessary level of protection that the recommendation would provide.
3. Summarize any alternative measure being instituted in lieu of the recommended measure.
4. Identify the LOP the alternative measure will provide.
5. Provide the justification for why the recommended measure will not be implemented. If applicable, note rationale from choices, and include details as necessary. **Use additional paper as necessary to completely describe justification for accepting risk.**

Possible Rationales for Risk Acceptance:

1. Physical site limitations
2. Facility structural limitations
3. Historical/architectural integrity
4. Building system configuration
5. Adjacent structure impact
6. Funding priorities
7. Short-term occupancy
8. Facility to be excessed
9. Facility to be disposed (provide date)
10. End of lease (provide date)

Recommendation	Necessary LOP	Alternative Measure	Achievable LOP	Rationale	FSC Chair's Signature

Example of a Memorandum for Record—Facility Security Level Determination

NOTE: Document becomes FOR OFFICIAL USE ONLY (FOUO) when filled in.

MEMORANDUM FOR: THE RECORD

FROM: [FULL NAME]

SUBJECT: [Facility Security Level Determination]

PURPOSE:

The purpose of this Memorandum for Record is to document the security organization's input to assist in determining the Federal Security Level (FSL) for [insert building identification here].

BACKGROUND:

The responsibility for making the final FSL determination rests with the tenant(s) of the building/facility, who must either accept the risk via a risk management strategy or fund security measures to reduce the risk.

For single-tenant government-owned or -leased facilities, a representative of the tenant agency will make the FSL determination in consultation with the owning or leasing department or agency and the security organization(s) responsible for the facility.

In multi-tenant government-owned or -leased facilities, federal tenants; (i.e., the Facility Security Committee [FSC]) will make the FSL determination in consultation with the owning or leasing department or agency, and the security organization(s) responsible for the facility.

Based on available information, the security organization has evaluated the facility in accordance with the criteria for FSL determinations established by the Interagency Security Committee (ISC).

During this review, the security organization evaluated each of the factors for determining the FSL. Following are the scores for each factor according to the security organization analysis:

FACTOR		SCORE
Mission Criticality		
Symbolism		
Facility Population (including onsite contract employees and visitors)		
Facility Size		
Threat to Tenant Agencies		
TOTAL SCORE		

Based on this score, and consideration of any applicable intangible factors, the security organization recommends that the FSL for this facility should be: [Insert FSL Score].

This is [insert outcome (ex. Increase, Decrease, etc.] from the previous level that was determined using ***The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard***.

This input was presented to the following officials to assist with the FSL determination on:

[Insert Date]

This is a preliminary determination for the facility. The ISC standards establish a baseline level of (Minimum, Low, Medium, High, and Very High) with the understanding the customized level of protection could raise or lower certain elements of countermeasure protection within the base line level.

Property Manager's Name: _____

FSC Chair's Name: _____

The security organization recommends that the FSC formally document the final FSL determination for its records and transmit that determination to the security organization and the Property Manager.

Signed: _____

Inspector's Name: _____

Example of an FSC Charter

Facility Security Committee Charter

[Facility Name]

[Address]

Mission

The Facility Security Committee (FSC) provides a standing body to address facility-specific security issues to ensure the protection of federal employees, essential functions, and government property.

Objective

The Facility Security Committee will perform the following functions in accordance with Interagency Security Committee (ISC) Standards:

- Establish the Facility Security Level (FSL) in conjunction with the security organization and the owning or leasing agency
- Determine the appropriate Level of Protection (LOP) for the facility

---

Bylaws

Membership

The FSC will have a chairperson. The chairperson is the senior representative of the primary tenant. The senior person with the primary tenant may designate a senior staff member with decision-making authority to serve as the chairperson; however, the senior representative retains the responsibility for the FSC. Should the senior person with the primary tenant decline to serve as the chairperson, the FSC members shall select a chairperson by majority vote. The FSC chairperson must represent a rent paying federal department/agency and is responsible for the following:

- Setting FSC meeting agendas,
- Scheduling FSC meetings,
- Distributing FSC meeting minutes,
- Maintaining FSC meeting records,
- Maintaining training records for all FSC members,
- Coordinating with outside organizations,
- Assigning tasks to other FSC members for drafting plans,
- Maintaining a current list of federal tenant agency occupant status,
- Maintaining a current list of federal tenants' square footage,
- Serving as the point of contact for the FSC between meetings,
- Calling for votes on issues before the FSC,

- Establishing deadlines by which each FSC member organization must provide guidance to their FSC representative, and
- Casting votes for their organization.

Each tenant agency shall designate its representative. Tenant representatives shall be senior officials/individuals with decision-making authority for their organization. If the FSC member does not have authority to make funding decisions, the FSC member is responsible for making the appropriate request(s) to their organizational headquarters for funding authorization as well as for the following tasks:

- Representing organizational interests,
- Attending FSC meetings,
- Obtaining guidance on how to vote for issues with funding implications,
- Obtaining assistance from organizational security element, and
- Casting votes for their organization.

New facility tenants shall be included as FSC members no later than 60 days after occupying the facility.

The security organization performs the FSL assessment and consults with the FSC and the owning or leasing authority to establish the FSL. Based on the FSL being accepted by the FSC, the security organization evaluates the facility using the ISC standards to determine the baseline LOP and, if necessary, develops a customized LOP to be presented to the FSC for consideration. The security organization is a voting member of the FSC if the security organization occupies and pays rent for space in the facility and is responsible for the following:

- Performing the FSL assessment;
- Presenting the FSL assessment to the FSC;
- Evaluating the facility to determine whether the baseline LOP is adequate, or whether a customized LOP is necessary;
- Presenting a written plan for proposed countermeasures that identifies how it will mitigate the risks identified with specific credible threats;
- Presenting written operating procedures for countermeasures;
- Presenting written cost impact for proposed countermeasures;
- Provide technical assistance and guidance to the FSC as appropriate; and
- Casting votes for their organization.

The security organization and Owning/Leasing Authority are voting members of the FSC if they pay rent for space in the facility. The responsibilities of the owning or leasing authority include the following:

- Identifying the requirements for an FSC and communicating that requirement in writing to proposed tenants during the lease-acquisition process (recommended).
- Representing organizational interests,
- Attending meetings,
- Providing technical information,

- Assisting with vendor access to the facility when requested by the security organization, and
- Casting votes for their organization

Other organizations may be added with the concurrence of the FSC Chair by formally requesting membership through the FSC.

MEMBERS		
Name	**Agency**	**Function**
Joseph Smith*	Department of Justice	FSC Chair
Sam Jones*[10]	Federal Protective Service	Security Organization
Randy Rent	General Services Administration	Owning/Leasing Agent
Shirley Marks*	Department of Defense	Tenant Representative
Tom Thomas*	Department of the Interior	Tenant Representative

* Voting member

Procedures

FSC meetings shall be held in accordance with processes and procedures outlined in *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, Appendix D: How to Conduct a Facility Security Committee*. This includes procedures for voting and funding requirements.

All FSC members shall execute their respective responsibilities as outlined above. The FSC Chair will coordinate the committee's activities. Meetings shall be held at the call of the FSC Chair. Notification of meetings and an agenda will be distributed to members of the FSC in advance of the meeting.

When necessary, the FSC may establish additional rules/protocols and internal procedures for conducting business.

The FSC shall retain records of all official business and make those records available to all FSC members upon request. Records shall be stored in accordance with the National Archives and Records Administration (NARA) best practices or the policy of the FSC Chair's organization.

Training

Federal employees selected to be members of the FSC are required to successfully complete a training course that meets the minimum standard of training established by the ISC. The training is available on the Homeland Security Information Network (HSIN) and/or Federal Emergency Management Agency websites. The training will minimally include:

- IS-1170 Introduction to the Interagency Security Committee and Risk Management Process
- IS-1171 Introduction to Interagency Security Committee Documents

[10] The security organization is a voting member of the FSC if they pay rent on space in the facility.

- IS-1172 Interagency Security Committee Risk Management Process: Facility Security Level Determination
- IS-1173 Interagency Security Committee Risk Management Process: Levels of Protection and Application of the Design Basis Threat Report
- IS-1174 Interagency Security Committee Risk Management Process: Facility Security Committees

Termination

The FSC shall remain active until no longer required in accordance with ISC standards.

Example of an FSC Meeting Agenda

DATE: _____

TIME: _____

LOCATION: _____

DISCUSSION ITEMS:

- [Item 1]
- [Item 2]
- [Item 3]

DECISION ITEMS:

- [Item 1]

Example of FSC Meeting Minutes

DATE: _____

TIME: _____

LOCATION: _____

ATTENDANCE:

FSC Chair:	[Name]
Security Organization:	[Name]
Tenant Agency Representatives:	[Name(s)]
Owning or Leasing Authority:	[Name]
Other Personnel:	[Name]

QUORUM PRESENT FOR MEETING? Y/N

QUORUM PRESENT FOR VOTE? Y/N

DISCUSSION ITEMS:

- [Item 1]
- [Item 2]
- [Item 3]

DECISION ITEMS:

- [Item 1]:
    - [Recorded vote of each voting member]
    - DECISION ITEM PASS/FAIL

ACTION ITEMS:

- [Item 1]