The Risk Management Process

An Interagency Security Committee Standard

2024 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	11/2021	Document Update	ISC
4.0	07/2024	Document Update	ISC

Document Control

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

Message from the Interagency Security Committee Chair

The United States faces a dynamic threat environment. As captured in the 2024 Homeland Threat Assessment issued by the U.S. Department of Homeland Security, the threat of violence from individuals radicalized in the United States will "remain high…marked by lone offenders or small group attacks that occur with little warning." The Interagency Security Committee (ISC) plays an integral role in advancing efforts to mitigate risks to federal facilities through security best practices and standards.

A critical component of the ISC is the *Risk Management Process: An Interagency Security Committee Standard*. This foundational standard describes the principles and practices individuals responsible for federal facility security employ to achieve a level of protection commensurate with—or as near to—the level of risk. It provides an integrated, single source of physical security countermeasures for all federal facilities.

This edition categorizes the risk management process into a five-step methodology to ensure a comprehensive approach to meet federal facility security needs in today's threat environment. It also ensures a process by which organizations can plan and implement risk management strategies and identifies roles and responsibilities to improve clarity and accountability in the security framework.

This standard provides a clear approach to protect federal assets and personnel and showcases the exceptional leadership of the Standards Subcommittee and the collective collaboration of ISC members.

David Mussington, Ph.D., CISSP, CMMC-RP
Executive Assistant Director for Infrastructure Security
Cybersecurity and Infrastructure Security Agency

Updates

The Interagency Security Committee (ISC) has reviewed and updated *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*. Personnel engaged in the risk management process should read the entire document. Below is a summary of the most significant modifications:

- Consolidates and revises the Risk Management Process into a five-step methodology that better aligns with risk management practices and strategies and ensures a comprehensive approach to meeting federal facility security needs.
- Updates Facility Security Level (FSL) Matrix values to match other values within the risk management process.
- Limits use of the baseline Level of Protection (LOP).
- Implements recurring training requirements for tenants, security organizations, and owning/leasing organizations.
- Modifies facility security committee (FSC) meeting frequencies, voting and decision process.
- Offers additional information on resourcing security countermeasures.
- Expands guidance on the process associated with accepting risk.
- Specifies roles and responsibilities for agencies, security organizations, and owning/leasing organizations.
- Incorporates compliance reporting and compliance verification requirements.
- Revises and expands performance measurement approaches.
- Articulates protection from liability.
- Improves forms and templates.

Table of Contents

Figures

Tables

1.0 Introduction

The Risk Management Process: An Interagency Security Committee Standard (RMP) defines the criteria and processes for determining a facility's security level and corresponding security requirements. It utilizes a five-step methodology to enable organizations to make informed decisions, allocate resources effectively, and prioritize risk mitigation efforts in a dynamic threat environment. It helps organizations understand the potential impacts of risks, develop risk management strategies, establish a culture of risk awareness and resilience, and provides a standard for compliance.

The RMP is not a "one-time" exercise but an ongoing, iterative process that requires continuous monitoring, evaluation, and improvement. The standard has multiple integrated appendices that individuals responsible for a facility's security shall use in applying the ISC standard.

Appendix A: Design-Basis Threat Report (FOUO) creates a profile of the adversary's type, composition, and capabilities. The DBT is an estimate of the threat federal facilities face across a range of Undesirable Events (UEs). Appendix A correlates with *Appendix B: Countermeasures (FOUO)*.

Users may request access to FOUO appendices by sending an email to ISCAccess@hq.dhs.gov Include the following: Full Name, Agency, Position, reason for access and contact information.

Appendix B: Countermeasures (FOUO) establishes security countermeasures that correspond to levels of protection applied to all federal facilities subject to following the RMP.

Appendix C: Child-Care Centers Level of Protection Template, Implementation Guidance (FOUO) provides additional guidance for child-care centers based on their relationship to federal facilities including campus environments.

Appendix D: How to Conduct a Facility Security Committee (FSC) provides guidance on establishing and conducting a FSC when presented with security issues affecting the entire facility.

Appendix E: Security Performance Measures assists organizations with establishing or refining performance measurement programs which assess the effectiveness of security programs designed to enhance security and protection of federal facilities.

Appendix F: Forms and Templates provides commonly used fillable forms and templates to support the risk management process.

Appendix G: Resources provides a reference guide for all abbreviations, acronyms, initialisms, definitions and citations within this document.

Users of this standard must realize that there is no guarantee that even the greatest analysis or assessments, countermeasures and processes will protect federal facilities from all potential or evolving, threats. However, failing to adhere to ISC standards puts government agencies at risk of compromising the safety and resilience of their employees, visitors, facilities, and operations. This standard establishes a uniform, risk-informed strategy for developing, implementing, and assessing the protective measures that organizations use to improve the quality and effectiveness of security and protection at federal facilities. It does not supersede individual agency security policies that exceed the RMP Standards.

This standard supersedes any earlier ISC standards mentioned herein.

2.0 Background

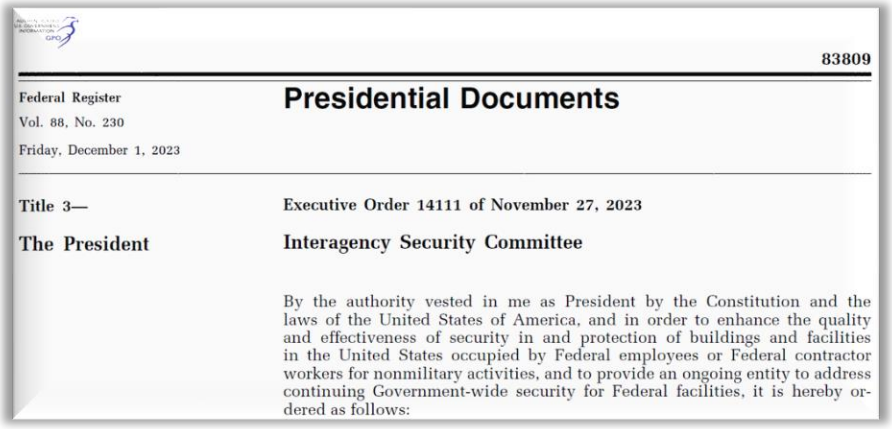
On April 19, 1995, at 9:02 a.m., a major explosion occurred in Oklahoma City. The source of the blast was a truck packed with explosives parked outside of the Alfred P. Murrah Federal Building. The blast destroyed the facility, which housed 14 federal agencies and The America's Kids Daycare Center. This tragedy remains the worst domestic-based terrorist attack against the United States government in our history. As a result, on October 19, 1995, the President signed Executive Order (EO) 12977 creating the "Interagency Security Committee" (ISC). EO 12977 required the ISC to enhance the quality and effectiveness of security in and protection of buildings and facilities in the United States occupied by federal employees for nonmilitary activities, and to provide a permanent body to address continuing government-wide security for federal facilities. In 2003, Executive Order 13286 transferred the Chair responsibilities of the ISC to the Secretary of the Department of Homeland Security (DHS).

In 2006, the ISC decided to update, expand, and clarify all security standards for protecting non-military Federal facilities. The goal was to create a single compendium of ISC standards. To achieve this, multiple working groups developed and published several key documents including:

- Facility Security Level Determinations for Federal Facilities (FSL), March 2008
- Use of Physical Security Performance Measures, June 2009
- Physical Security Criteria for Federal Facilities, April 2010
- Design-Basis Threat Report, April 2010
- Facility Security Committee Standard for Federal Facilities, July 2011

Next the ISC published *the Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*. Known simply as the RMP, this standard integrated all the previous publications, enabling a single-source comprehensive standard.

On Nov 27, 2023, the President signed EO 14111, *Interagency Security Committee* superseding EO 12977. EO 14111 reinforces the importance of the security of federal facilities in the face of persistent and emerging threats. It defines duties and responsibilities to establish the ISC's authority with the central responsibility agencies have for federal facility security. It also reduces ambiguity as to applicability and raises visibility of federal facility security to the highest levels of the government.



83809

Federal Register
Vol. 88, No. 230
Friday, December 1, 2023

Presidential Documents

Title 3—
The President

Executive Order 14111 of November 27, 2023

Interagency Security Committee

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to enhance the quality and effectiveness of security in and protection of buildings and facilities in the United States occupied by Federal employees or Federal contractor workers for nonmilitary activities, and to provide an ongoing entity to address continuing Government-wide security for Federal facilities, it is hereby ordered as follows:

Today the ISC chaired by the Cybersecurity and Infrastructure Security Agency (CISA) Executive Assistant Director for Infrastructure Security, consists of a permanent body of 66 departments and agencies.

3.0 Applicability and Scope

Pursuant to the Authority of the ISC in EO 14111, all federally owned or leased buildings, structures, and the land they reside on, in whole or in part, regularly occupied[1] by executive branch federal employees and/or federal contract workers for nonmilitary activities is subject to this Standard.

In accordance with EO 14111, *"nothing in this standard shall be construed to impair or otherwise affect the authority granted by law to an executive department or agency, or head thereof."*

The Department of Energy complies with the policies and standards of the ISC issued pursuant to EO 14111 to the extent such compliance is consistent with and does not impair or affect the Departments statutory obligation to protect national security assets consistent with the Atomic Energy Act of 1954, as amended and the Department of Energy Organization Act.

Title 41, Code of Federal Regulations (CFR), Part 102-81, Physical Security is applicable to "federally owned and leased facilities and grounds under the jurisdiction, custody, or control of General Services Administration (GSA), including those facilities and grounds that have been delegated by the Administrator of General Services." In 2022, the GSA amended 41 CFR § 102-81.25 "to clarify that federal agencies are responsible for meeting physical security standards at nonmilitary facilities in accordance with ISC standards, policies, and recommendations."[2] Additionally, per DoD Instruction, 2000.12, all DoD leased facility space or space in buildings owned or operated by the GSA not located on DoD property must comply with this standard.

40 United States Code (U.S.C.) § 1315, The National Security Memorandum on Critical Infrastructure on Security and Resilience codifies the U.S. Department of Homeland Security's (DHS) responsibility for protecting buildings, grounds, and property owned, occupied, or secured by the federal government; establish U.S. policy for enhancing the 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 National Security Memorandum on Critical Infrastructure Security and Resilience "advances our national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure."

[1] The responsible authority determines "regularly occupied." For single-tenant facilities, a single office designated by the organization (e.g., Director of Security) may make occupancy determinations ensuring consistency across the organization. An occupied facility is when there is federal, or contract employees permanently or regularly assigned.

[2] See 87 FR 51915

Dams, tunnels, bridges, and national monuments are examples of critical infrastructure. Various agencies classify these structures as "high-risk symbolic or critical infrastructure" or by other designations. Although the RMP does not focus on these structures, its processes and results may still be useful in protecting them. This standard primarily addresses human-made threats. Although many of the countermeasures listed will help to reduce the effects of natural hazards, the scope of this document does not address risks like earthquakes, fires, or storms, normally covered in relevant construction standards.

Further, this document presupposes that facility stakeholders, 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.), the Code of Federal Regulations (CFR), the Federal Management Regulations (FMR), the 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.

4.0 Key Definitions

Table 1: Key Definitions

TERM	DEFINITION
Facility Security Level (FSL)	A categorization based on the analysis of several security-related facility factors, which serves as the basis for the identification of preliminary countermeasures and recurring risk assessments.
Level of Protection (LOP)	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.
Responsible Authority[3]	Facility Security Committee (FSC), tenant representative for single-tenant facilities, or legal authority (i.e., courtroom where a judge exercises authority).
Risk	A measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence.
Risk Acceptance	The explicit or implicit decision not to take 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 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.
Senior Official	An organization's principle executive authority responsible for implementation and compliance with ISC Standards.

For a comprehensive list of definitions, refer to the Glossary of Terms in Appendix G.

[3] The definition of "Responsible Authority" does not include the term "Designated Official (DO)." 41 CFR § 102-74.230 establishes and defines specific responsibilities for the DO centered around the Occupant Emergency Program.

5.0 Roles and Responsibilities

Securing and protecting federal facilities requires collaboration from multiple entities. Each component involved in the risk management process fulfills specific roles and responsibilities to *"enhance the quality and effectiveness of security in and protection of buildings and facilities*[4]*…"*

5.1 Organizational Headquarters

Per EO 14111, "*each agency shall cooperate and comply with the requirements of this executive order and the policies and standards of the Committee issued pursuant to this order.*" The executive order requires each executive agency to:

"Provide such cooperation and compliance as may be necessary to enable the Committee to perform its duties and responsibilities" and "Designate a senior official, who shall be responsible for agency implementation and compliance with this order." Organizational Headquarters shall:

- Establish organizational policy to comply with EO 14111 and this standard.

- Designate the senior official in writing and provide the documentation to the Interagency Security Committee at ISC.DHS.GOV@HQ.DHS.GOV.
    - Higher-level headquarters organizations (e.g., Department of Homeland Security) may designate a single senior official for the entire organization to include sub-agencies, sub-organizations, and bureaus if their authority and resources provide them a means to achieve the senior official's responsibilities. When the senior official does not have the authority and resources to achieve these responsibilities for the entire organization, a suitable senior official should be designated for the sub-agencies, sub-organizations, and bureaus. In these instances, it is a good practice to document the boundaries of the Senior Official's responsibilities within the organization[5].

    - The documentation shall include:
        - Name of Senior Official
        - Office/Title
        - Email address and phone number

5.2 Senior Official

The senior official serves as the organization's principle executive authority responsible for implementation and compliance. Senior officials ensure their organizations provide such cooperation and compliance as may be necessary to enable the Committee to perform its duties and responsibilities. Senior Officials will:

[4] EO 14111, *Interagency Security Committee*

[5] In instances such as document approval, each primary member agency has only one vote. Organizations with multiple senior officials must designate one to register a single vote on behalf of the entire agency.

- Ensure agency implementation of ISC standards.
- Approve ISC documents, to include the Biennial Report, and provide strategic direction to Subcommittees and Working Groups (primary members only).
- Approve new Associate Members (primary members only).
- Ensure compliance reporting on an annual basis and participate in compliance verification.
- Ensure appropriate offices review and clear draft ISC documents.
- Share security related intelligence, as appropriate.
- Maintain a centralized list of the organization's risk acceptance for each facility and develop a mechanism/means to support prioritized funding.

Additionally, EO 14111 specifies the senior official *"Shall ensure their agency supports Facility Security Committees, as applicable, in the performance of their duties."* Senior Officials shall:

- Monitor/promote completion of FSC training for required personnel.
- Provide oversight to ensure FSCs operate effectively, efficiently and in accordance with established ISC policy and standards.
- Ensure FSC representatives receive voting guidance on financial issues.
- Provide 3rd level and final review in FSC decision making process, when invoked by FSC chair.

5.3 Organizational Security Element

The Organization Security Element (OSE) is the organizational security office's headquarters or regional component or equivalent. The OSE is associated with the facility tenants and is generally the entity that assists the senior official in ensuring organizational implementation and compliance of the ISC standards. The OSE and the security organization (section 5.4) are usually different. The OSE will:

- Establish and annually review a risk register (i.e., risk acceptance list) that informs and prioritizes all security risk at federal facilities within their organization.
- Track identified countermeasures not implemented at each facility, the reason for non-implementation, and maintain risk acceptance documentation.
- Ensure implementation of security performance measures and testing programs.
- Track approved funds and advise the responsible authority on which fiscal year the funds will be available.
- Monitor/promote completion of RMP training for personnel making or advising on risk management decisions at single tenant facilities.
- Maintain list of federal facilities occupied by the organization to include Facility Security Level (FSL) designations.
- Maintain active roster of FSC chairpersons and FSC member representatives.
- Identify additional ISC member representatives.
- Nominate subject matter experts to support ISC subcommittees and working groups.
- Provide guidance to responsible authorities and other organizational personnel regarding security policy, risk management strategies, and compliance.
- Provide documented decision to responsible authorities when an agency does not approve funds. The documentation must include the reason for denial and risk acceptance to the facility.
- Assist responsible authorities in selecting a security organization when one does not reside in a facility or otherwise assigned.
- Provide 2nd level review in FSC decision process when invoked by FSC chair.

5.4 Security Organization

The security organization is 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 and performs preliminary FSL determinations and initial or recurring risk assessments.

Security organizations are responsible for assessing risk by identifying and analyzing threats, vulnerabilities, and consequences. Based on this risk assessment, they must identify countermeasures that meet ISC requirements. The security organization must provide all relevant information to the responsible authority, enabling them to make informed decisions regarding the identified countermeasures.

A fundamental contrast between a security organization and organizational security element is that the security organization performs the required risk assessment for each assigned government facility.

Security organizations will:

- Ensure personnel performing risk assessments have completed an ISC certified risk management process and FSC training program.
- Ensure risk assessment methodology used meets the ISC standards.
- Conduct FSL analysis and present data to responsible authority for final determination.
- Consult on tenant's final FSL determination.
- Conduct risk assessments and provide responsible authorities with results to include supporting documentation.
    - For future construction: Conduct a project-specific risk assessment during the requirements definition phase.
    - For existing facilities: Conduct risk assessments in accordance with the frequency required by the FSL and identify required countermeasures and design features.
- Provide a scope of work[6] and cost estimates[7] for proposed countermeasure(s) to each tenant agency. This plan must include the following:
    - Estimated cost of countermeasure(s) to include life-cycle costs.
    - How the countermeasure(s) will mitigate the risks identified with specific credible threats to include operational procedures.

[6] The Federal Acquisition Regulation Subpart 36.302 states "The agency shall develop, either in-house or by contract, a scope of work that defines the project and states the Government's requirements. The scope of work may include criteria and preliminary design, budget parameters, and schedule or delivery requirements."

[7] The scope of work and cost estimate should be commensurate to the Planning, Programming, Budgeting & Execution (PPBE) process. Those used for planning and programming purposes or to obtain an initial decision may be budgetary estimates requiring refinement and improvement as the countermeasure moves into the project design phase.

    - How the countermeasure(s) meets the necessary LOP as determined in step 4 of the risk management process.
- Assist responsible authorities in developing risk mitigation strategies.
- Participate in market surveys to identify potential locations capable of meeting space requirements for the Government[8]. If the security organization cannot attend, they must provide notice to the responsible authority, owning/leasing authority, and organizational security element(s). The security organization will still be responsible for providing risk related data such as crime statistics.
- Provide technical assistance and guidance to the responsible authority as appropriate.
- Conduct performance testing for countermeasures for which responsible in accordance with *Appendix B: Countermeasures (FOUO)* and the necessary LOP.

5.5 Owning or Leasing Organization

The owning or leasing authority is an entity authorized to enter into a lease agreement with a person, co-partnership, corporation, or other public or private entity for the accommodation of a federal agency in a facility. The owning or leasing authority shall:

- Ensure personnel responsible for acquiring real property for agency tenants complete necessary risk management process and FSC training.
- Co-locate tenants with similar risk profiles whenever feasible.
- During the lease acquisition process, inform the proposed tenant in writing of their responsibility to either fill the responsible authority/FSC Chair position or provide a representative.
- Notify the security organizations and OSEs of pending new projects (to ensure participation in design phase).
- Invite the security organization and OSE to participate in market surveys with sufficient notice to encourage participation.
- Consult the responsible authority and security organization in making the FSL determinations.
- Coordinate with security organizations to ensure completion of risk assessments sufficiently in advance of the solicitation (request) for offer documents.
- Notify responsible authorities and security organizations of occupancy or mission changes to a facility that may affect the FSL or current risk acceptance.
- Act as a liaison between tenant(s) and owning organization to discuss implementing necessary countermeasures based on the risk and notify the responsible authority when the lessor does not approve a countermeasure proposal.
- Assist with vendor access to the facility when requested by the security organization.

[8] GSAM 570.301 requires a market survey to identify potential locations capable of meeting a space requirement for the Government. GSA Leasing Desk Guide, chapter 2 notes that a "market survey" refers to the process of gathering information about and physically touring specific properties in the market, usually accompanied by an agency representative, to determine whether suitable property is competitively available.

5.6 ISC Standards Subcommittee

The ISC Standards Subcommittee (SSC) is the coordination point for ISC policies, standards, and recommendations. The SSC will:

- Review the RMP standard on a regular basis and publish revisions and updates as appropriate.
- Review and provide comments and recommended resolution regarding disputes or implementation of this standard.

5.7 ISC Regional Advisors

ISC Regional Advisors provide federal facility security expertise to regional/field-level federal facility stakeholders and organizational officials to enhance the security and protection of federal facilities in their assigned regions. Regional Advisors will:

- Establish and maintain relationships with stakeholders.
- Advise stakeholders on the RMP and FSC operations.
- Deliver FSC training, seminars, workshops, etc.
- Provide ISC technical assistance, guidance, and subject matter expertise.
- Facilitate FSC discussions when an impasse occurs.
- Determine need-to-know and support release protocols for ISC For Official Use Only (FOUO) documentation.
- Facilitate FSL determinations when the responsible authority, security organization, and leasing authority do not agree.
- Conduct ISC compliance assistance visits.
- Consult with responsible authorities on annual compliance reporting and results.
- Support organizational and facility level compliance verification.

6.0 Training Requirements

Federal employees and contractors who participate in the ISC risk management process will complete required training within 90 days of assignment. FSC members (see Appendix D) or those making or advising on risk management decisions for single tenant facilities shall complete the training, at a minimum, every five years (retain proof of the training). The ISC recommends that those in higher risk facilities (e.g., FSLs III-V) take the training every three years to assist with their recurring risk assessment and risk management process participation. Required training courses can be found on Interagency Security Committee Training | CISA.

Security personnel conducting risk assessments should complete additional training specific to their organization's risk assessment methodology. The additional training should specify how to conduct a risk assessment and use of any tools that support it. Organizations should seek ISC certification for training courses, data tools, or applications used to support an ISC-compliant risk assessment.

To learn more about the ISC risk management tool or training certification, contact the ISC at ISC.DHS.GOV@HQ.DHS.GOV.

7.0 Financial Guidance

The decision to implement identified security countermeasures or accept risk at a facility will often contain a financial component. **Generally, it is the responsibility of the organizational headquarters to provide funds for countermeasures.** Funding requests for security countermeasures and upgrades often compete with other funding requests at the organizational headquarters level. Accordingly, responsible authorities coordinate with the headquarters for all funding actions (unless they have funding authority). Organizational headquarters must be prepared for countermeasure funding requests and ensure their annual budget requests consider the number of locations they occupy and projected requests for security countermeasure funding.

Security organizations provide written funding proposals to the responsible authority for consideration that includes:

- Total project cost for the facility.
- A cost analysis that indicates the cost effectiveness of the proposed countermeasure.
- Projected costs for subsequent fiscal years.

For additional details unique to the Facility Security Committee funding processes, see *Appendix D: How to Conduct a Facility Security Committee*.

7.1 Approval of Funds

When organizations approve funds, they must advise the responsible authority as to which fiscal year the funds will be available. The headquarters' security element tracks the funds and keep their responsible authority informed of changes relating to appropriation or authorization.

7.2 Disapproval of Funds

When an agency does not approve funds, the decision then results in risk acceptance. The organizational security element shall document the denial of funds and the risk acceptance to the facility and provide a copy of the documentation to the responsible authority. Additionally, the organizational security element enters the risk acceptance data into the organizational risk register.

7.3 Funding Documents

It is beyond the scope of this document to detail each method of transferring federal funds from one federal agency to another. The agency implementing the countermeasure must determine how the procurement funding will occur from participating organizations. FSC members must contact their respective financial authority for guidance on how to transfer funds and in what fiscal year the funds will be available. The owning/leasing authority or security organization implementing the countermeasure is responsible for providing each FSC representative with the necessary information on the specific method(s) to use for transferring federal funds.

8.0 The ISC Risk Management Process

The ISC Risk Management Process establishes a single, formalized process for specifying the standards and guidelines to follow when determining federal facility security requirements. The goal of the RMP is to provide a level of protection equal to the level of risk at the site-specific location. Agencies shall use the risk management process resulting in:

- The application of the baseline LOP until the security organization performs a risk assessment, as is the case with lease solicitation or new construction; **THEN**
- The application of the necessary LOP to address facility-specific conditions based on the required risk assessment, **OR**
- The application of a customized LOP (necessary and/or achievable) and the documented acceptance of risk.

Responsible authorities minimize the amount of acceptable risk through an iterative process. The LOP implemented may never be less than Level I-Minimum found in *Appendix B: Countermeasures (FOUO)*, regardless of site conditions.

The ISC RMP follows a five-step methodology to ensure a comprehensive approach to meet federal facility security needs in today's threat environment. This methodology ensures that the scope of security countermeasures is commensurate with the risk posed to the facility. It also ensures a process by which organizations can plan and implement their risk management strategy (see Figure 1).

Figure 1: The Five Steps of the Risk Management Process

The risk management process is continuous and begins with determining the FSL based on the individual characteristics of a facility and the federal occupant(s). The FSL leads the security professional to a baseline level of protection for facility planning purposes. The next step involves completing a risk assessment which leads to developing a risk management strategy by determining if the Necessary LOP is achievable and if not, implementing an alternate strategy. Once a risk management strategy is in place, the responsible authority, security organization, and owning or

leasing authority, supported by the various organizational headquarters, implement the risk management strategy. The fifth step of the process is to measure performance. Measuring performance is a continuous process in which the responsible authority and/or security organization may need to cycle back to step 2, or step 3 if the performance is not meeting expected standards. Organizations may return to step 1 if changes in the security warrant it (see section 8.1.6).

8.1 Step One: Determine the FSL and Baseline LOP

Figure 2: Determine the FSL and Baseline LOP Overview

Determining the FSL and baseline LOP is step one of the risk management process and serves a two-fold purpose.

1. Directs security professionals to a baseline LOP to ensure the initial stages of a security project (i.e., new construction or new lease) include security countermeasures.
2. Establishes the frequency for recurring risk assessments.

8.1.1 Making the FSL Determination

Responsible authorities make the initial FSL determination for newly leased or owned space as soon as practical after identifying a space requirement, including succeeding leases. FSL determination ranges from a Level I (lowest risk) to a Level V (highest risk). The responsible authorities make the FSL determination 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.

Security organizations perform risk assessments once every five years for Level I and II facilities and once every three years for Level III, Level IV, and Level V facilities. Each initial and recurring risk assessment will include reviewing the FSL and adjusting, if necessary[9].

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.

[9] Facilities not regularly occupied by federal employees do not require recurring risk 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. However, nothing prevents agencies from conducting such assessments if they feel the risk warrants it.

The tenant(s) make the final FSL determination, in consultation with the owning or leasing authority and the security organization responsible for the facility.

- **For single-tenant facilities** owned or leased by the government or federal contractor, a representative of the tenant agency will make the final FSL determination.
- **In multi-tenant facilities** owned or leased by the government, the tenants (i.e., through the Facility Security Committee) will make the final determination.

For single-tenant facilities, a single office designated by the organization (e.g., Director of Security) may make all final FSL determinations ensuring consistency across the organization.

When the security organization and the owning/leasing authority do not agree with the tenant(s) regarding the FSL determination, the ISC regional advisor may facilitate a final determination through discussion with all relevant parties. ISC facilitation will include the ISC organizational representative or designee of the organizational security element. If the FSL determination is not resolved following the facilitated discussion, the issue will be raised to the respective Senior Officials for resolution. All entities will document, sign, and retain the final FSL determination.

8.1.2 Facility Security Level Matrix

The FSL matrix comprises 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 the potential circumstances. Thus, the standard includes a sixth element - intangibles - to allow the assessor to consider other factors unique or specific to the facility.

The standard does not include every potential situation that an organization may face at a facility. Therefore, the standard includes an explanation of each factor, 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 rationale used in the development of the process.

To use the FSL determination matrix (see table 2), examine each factor and assign a point value based on the provided scoring criteria. The preliminary FSL is determined by the sum of the point values for the five factors. The security organization and responsible authority will consider and document intangibles that might be associated with the facility and adjust the FSL by either a one-level increase or a one-level decrease. Appendix F: Forms and Templates: Example Memorandum for Record-Facility Security Level Determination provides an example memorandum.

Table 2: Facility Security Level (FSL) Determination Matrix

Factor	Points				Score
	1	2	3	4	
Mission Criticality	MINIMUM	LOW	MEDIUM	HIGH	
Symbolism	MINIMUM	LOW	MEDIUM	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 Agency	MINIMUM	LOW	MEDIUM	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					**+/- 1 FSL**
					Final FSL
* Facilities with a child-care center (CCC) receives a facility population value of "high."					

8.1.3 Facility Security Level Scoring Criteria

8.1.3.1 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 National Essential Functions 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, use the highest rating for any federal tenant in the facility. Continuity of Government (COG) and Continuity of Operations Plan (COOP) documents are useful sources of information regarding the performance of essential functions. The facility tenant(s) determine the tenant's mission criticality when consulting with the security organization.

Table 3: Mission Criticality

Value	Points	Criteria	Examples
High	**4**	National leadership, seats of constitutional branches. Houses chief officials for a branch of government.	White House, the U.S. 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, Joint Terrorism Task Force and Counterdrug 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.
		Houses personnel or specialized equipment necessary to detect or respond to unique public health incidents.	Centers for Disease Control and Prevention.

Value	Points	Criteria	Examples
		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 reactors facilities, explosives storage facilities.
		COG facilities	Federal Emergency Management Agency Emergency Operations Center.
Medium	**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. occupied by federal employees.
		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, Census Bureau.
		Biological/chemical/radiological/medical research or storage of research and development (de minimis) quantities of chemicals, biohazards, explosives, and comparable items.	Animal Disease Research Center
		COOP facilities for department and agency headquarters.	GSA Central Office COOP facility
		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
Low	**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.

Value	Points	Criteria	Examples
		COOP facilities for other than national headquarters.	GSA Regional Office COOP site.
Minimum	**1**	The loss, theft, destruction, misuse, or compromise of activities or operations that would have a 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

8.1.3.2 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 evaluation includes non-U.S. Department of Defense (DOD) federal facilities on a DOD campus.

Adversaries may perceive a facility with a large amount of land/acreage associated with it as highly important. 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 4: Symbolism

Value	Points	Criteria	Examples
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/irreplaceable artifacts in the event of their damage or destruction	National Archives Museums, Smithsonian museums
		Executive department headquarters buildings	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
Medium	**3**	Well-known, regional U.S. Government facilities.	Oklahoma City Federal Building
		Agency/Bureau headquarters	GSA Central Office, Environmental Protection Agency 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 perceived to be well-protected	Military installations
		Located in a symbolic commercial financial building	International trade centers, regional or nationwide bank headquarters building
		Co-located with other non-government but highly symbolic facilities	Transportation hubs
Low	**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)	Agency field offices.
		Readily identifiable, non-facility assets located at site	Large fleet of federal government vehicles, military equipment

Value	Points	Criteria	Examples
		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
Minimum	**1**	No external features or public contact readily identifying it as a U.S. Government facility	Classified locations, small offices in leased commercial buildings

8.1.3.3 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. For federal occupants, this number is based on tenant input, assigned numbers according to the tenant(s) human resources office, and occupancy agreement. The visitor number is the average number of visitors in the facility **at any given time.** Ideally, organizations calculate the visitor population through a review of visitor logs or access control lists; however, it may necessitate an estimate or a short-term sampling of visitor traffic. The total population number cannot exceed the facility's maximum capacity. The facility population score does not include transient populations. An example of a transient population is an occasional conference at the facility. Organizations use temporary or contingency security measures to address increased risks during temporary population increases.

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 "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 5: Facility Population

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

8.1.3.4 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 an organization occupies the entire facility or entire floor, use the gross square footage (length multiplied by width); in a multi-tenant facility, if a federal entity only occupies a portion of a floor, use assignable or rentable square footage. 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.

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. For instance, the assessor may add one point for a federal campus with a single overall FSL determination.

Table 6: Facility Size

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

8.1.3.5 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 7: Threat to Tenant Agencies. For a multi-tenant facility, use the highest value of any one federal tenant.

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, the security organization should use the following guidelines for gathering and analyzing crime statistics:

- Do not limit the crime statistics to only crimes committed at, on, or in the facility.
- When available, use crime statistics for the prior 12 months.
- Use crime statistics for a radius up to one mile from the facility.
- In smaller cities with a population exceeding 100,000 up to one million, use crime statistics for the entire city.
- In rural areas with a population less than 100,000, organizations may need to consider crime statistics for the zip code, county, or other relevant criteria based on the availability of local statistics.

Table 7: Threat to Tenant Agencies

Value	Points	Criteria	Examples
High	**4**	Tenant mission and interaction with certain segments of the public is adversarial in nature.	Criminal and bankruptcy courts; high-risk law enforcement organizations, including those who routinely contact or attract attention of dangerous groups (e.g., Federal Bureau of Investigation; Drug Enforcement Agency; Bureau of Alcohol, Tabaco, Firearms, and Explosives) and U.S. Courts - including administrative courts of federal agencies, hearings for high-profile, controversial, high-threat or those cases that impact a large number of individuals (e.g., narcotics-trafficking, terrorism, potentially controversial matters, deportation, etc.
		Tenant mission is controversial in nature and routinely draws the attention of organized protestors.	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.

Value	Points	Criteria	Examples
		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.
Medium	**3**	Public contact is occasionally adversarial based on the nature of business conducted at the facility.	Non-criminal/administrative courts that may suspend/revoke privileges or benefits, 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.
		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.
Low	**2**	Generally non-adversarial public contact based on the nature of business conducted at the facility.	General/internal Investigations, inspection services for the U.S. Department of Agriculture, Department of State Passport Office.
		History of demonstrations against the tenant agency (not at the facility).	U.S. Nuclear Regulatory Commission, U.S. Citizenship and Immigration Services.
		Located in a low-crime area	As determined by a characterization established by local law enforcement.
		History of violence directed at tenant agencies/companies (not at facility).	Internal Revenue Service, Agency mission support offices.
Minimum	**1**	Generally little-to-no public contact.	Government warehouses or storage facilities, Federal Trade Commission.
		No history of demonstrations at the facility.	As determined by security organization or tenant incident records.
		Located in an area with very low crime.	As determined by crime statistics analysis guidance above.
		No history of violence directed at the facility or the occupants.	As determined by security organization or tenant incident records.

8.1.3.6 Intangible Adjustment

It is impossible for this document to consider all the conditions that may affect the FSL decision for all 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.

The responsible authority may raise or lower the FSL one level based on intangible factors. However, organizations will not use intangible factors to raise the FSL in response to a particular threat. Organizations address specific threats to facilities through risk assessments, the necessary LOP and customized countermeasure implementation.

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, organizations develop contingency plans to implement temporary countermeasures until the event has passed. For example, a weeklong conference may increase the population and risk at a facility during the conference but would not justify an intangible adjustment.

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

Do not use the FSL intangible adjustment for the purposes of reducing the baseline LOP. If a facility cannot meet the baseline or necessary level of protection, risk acceptance may be necessary.

8.1.4 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.

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. 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 "high" score value for mission criticality or symbolism and is a one-of-a-kind facility (or nearly so).

8.1.5 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). An organization may establish an overall FSL in a campus housing a single tenant (DHS headquarters, Social Security Administration's headquarters). In multi-tenant campuses, either assign all individual facilities in the campus an individual FSL, 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).

8.1.6 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 factors. A slight 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 slight 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.

The FSL review is part of the regularly recurring risk assessment and adjusted, as necessary. The owning or leasing authority must notify the security organization and responsible authority of major changes in the nature of the tenants. When this occurs, the responsible authority in consultation with the security organization considers whether to do a review of the FSL between the regularly scheduled risk assessments.

8.1.7 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 in the same facility as a low-risk administrative entity. For this reason, organizations with real property authority should strive to co-locate compatible tenants —those with similar security concerns and requirements whenever feasible, and incompatible tenants should not.

The factors of mission criticality and threat to tenant agencies should be primary considerations in determining compatible tenants. Additionally, 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 complicated 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 needs it, and ensures that the high-risk tenant can achieve the higher security posture it merits.

The security organization should provide a pre-lease risk assessment before a tenant moves into a new or existing facility. A tenant requiring a higher level of security should not move into a facility with a low security level. 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, consider the operational impacts upon the other agencies (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; but 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.

8.1.8 Identify Baseline LOP

The **baseline LOP** is the degree of security provided by the set of countermeasures for each FSL and **is only applicable until the security organization completes the risk assessment** (i.e., new lease solicitation or new construction).

Each FSL corresponds to an estimated level of risk that relates directly to an LOP and associated set of security measures. Comparatively speaking, FSL I designated facilities face a minimum level of risk, and thus the baseline LOP for a FSL I facility is minimum; FSL II corresponds to Low; FSL III corresponds to Medium: FSL IV to High; and FSL V to Very High (see Table 8 below).

Table 8: FSL Relationship to Baseline LOP

Facility Security Level	Estimated 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 list security measures for each baseline LOP associated with the FSL. Security planners use the baseline LOP for

security design purposes in new construction/leases prior to an actual risk assessment and the identification of the necessary LOP.

Figure 3 represents how a FSL III determined facility with an associated medium baseline LOP would mitigate the estimated risk from Undesirable Events (UE) prior to completion of actual risk assessment.

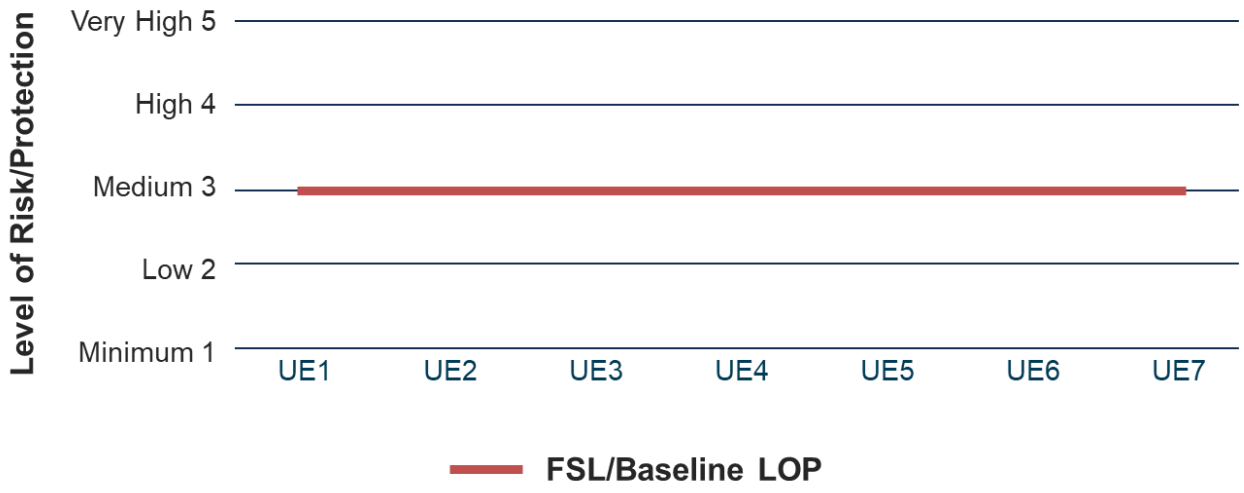


Figure 3: Example of Undesirable Events with Estimated Risk and Baseline Level of Protection

8.2 Step Two: Identify and Assess Risk

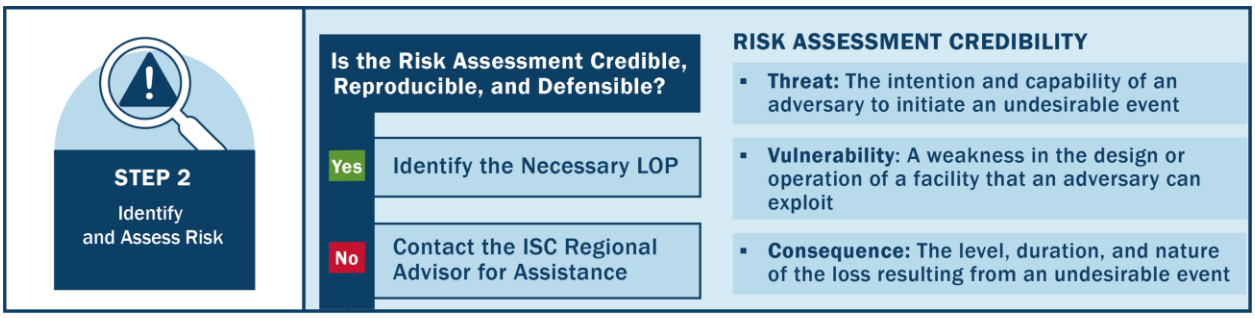


Figure 4: Identify and Assess Risk Overview

A comprehensive risk assessment of a facility has numerous benefits. First, it provides the specific risks corresponding to all UEs[10] associated with a facility. Second, it identifies the necessary LOP and whether the existing LOP will adequately mitigate the identified risk. Third, it provides decision makers with detailed information needed to develop and justify implementing identified countermeasures. Finally, it aids organizational headquarters with developing project priorities and budget submissions.

[10] See *Appendix A: Design-Basis Threat (DBT) Report (FOUO)*

Risk is a measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence.

The security organization conducts a risk assessment for each assigned federal facility. In doing so, the security organization uses *Appendix A: The Design-Basis Threat (DBT) Report (FOUO)* which supports the calculation of risk to a federal facility. The DBT provides a broad range of undesirable events (UE) with specific details on characteristics that may impact federal facilities. Each event supplies sufficient information for estimating the threat and contributes to the analysis of vulnerability and consequence when conducting a risk assessment. At a minimum, the risk assessment must consider all undesirable events in the DBT. The DBT report fills the void of threat information available to security professionals (especially in smaller agencies without access to current intelligence). Figure 5 shows how the assessed risk may compare or differ from the estimated risk associated with an FSL III facility with a medium baseline LOP.

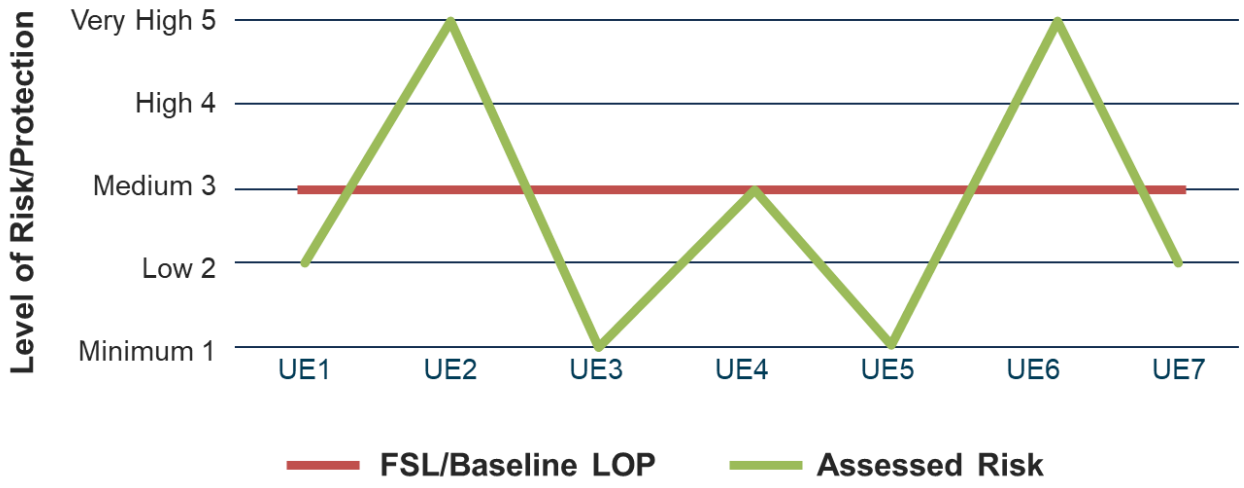


Figure 5: Example of Assessed Risk

The security organization **must** notify facility tenants of a pending risk assessment. Tenants may have first-hand knowledge of their surroundings that may be outside traditional reporting channels or other published sources available to the security organization. Tenants should inform their organizational security elements about upcoming risk assessments. Additionally, security organizations should engage organizational security elements in the risk assessment process to enhance collaboration and increase the opportunity for potential funding of identified countermeasures.

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 responsible authority will coordinate with their organizational headquarters element to select and coordinate security organization services.

Security organizations can gather preliminary data during the planning of a risk assessment; however, actual site visits by the security organization for existing facilities is the preferred method.

Once a risk assessment is complete, the baseline LOP is no longer applicable and is replaced by the necessary LOP.

8.2.1 Risk Assessment Methodology

Risk is a function of threat, vulnerability, and consequence and a variety of mathematical models are available to calculate risk and to illustrate the impact of increasing protective measures on the risk equation. The ISC Risk Management Process 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 must adhere to the fundamental principles of a sound risk assessment methodology:

- The methodology must be credible and assess the threat, vulnerability, and consequence to specific undesirable events.
    - **Threat**: The intention and capability of an adversary to initiate an undesirable event.
    - **Vulnerability:** A weakness in the design or operation of a facility that an adversary can
    - **Consequence**: The level, duration, and nature of the loss resulting from an undesirable event. (Commonly measure consequence in four ways: human, economic, mission, and psychological, but may also include other factors such as impact on the environment)

- The methodology must be reproducible and produce similar or identical results when applied by various security professionals.

- The methodology must be defensible. To be defensible, the methodology must:
    - Provide sufficient justification for deviation from the baseline threat ratings enumerated in the *Appendix A: Design-Basis Threat Report (FOUO)*.
    - Correlate directly with the levels of protection enumerated in *Appendix B: Countermeasures (FOUO)*.

8.2.2 Determine the Necessary Level of Protection to Adequately Mitigate Risk

The goal of the necessary LOP is to match or mitigate the assessed risk. Determination of the necessary LOP is included in step two because the security organization must identify the countermeasures that will provide an LOP equivalent to the level of risk as part of their risk assessment report. Assessment of a facility's threats, vulnerabilities, and consequences, may lead to risks that are relatively higher or lower in some cases than at other facilities with the same FSL. As a

result, the baseline LOP may not mitigate the risks found, therefore the baseline LOP is no longer applicable once the security organization has completed a credible risk assessment (e.g., the baseline LOP is medium, but the assessed risk of 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 of robbery is minimum), resulting in the unnecessary expenditure of resources. When performing the risk assessment, security organizations should consult subject matter experts in specialized areas to ensure identification of proper risk mitigation measures (see 8.3.5). The FSL remains applicable after the risk assessment, only the baseline LOP is replaced by the necessary LOP.

Determination and application of the necessary LOP negates both unmitigated risk and over-expenditure of resources. Excess resources to mitigate one risk area can be reallocated to underserved areas, thus ensuring the most cost-effective security program.

The security organization uses the risk assessment calculations to find the necessary LOP using the Security Criteria Tables found in *Appendix B: Countermeasures (FOUO)*. The tables identify the countermeasures generally considered applicable to mitigate the risk from a particular undesirable event. The matrix cross-references undesirable events that may affect federal facilities and relates them to applicable security measures.

The list of undesirable events is not all inclusive. Unique facilities may face other mission-specific threats. For events not found in the tables of the *Appendix A: Design-Basis Threat (DBT) Report (FOUO*), the ISC recommends agencies add customized undesirable events and either relate them to countermeasures in *Appendix B: Countermeasures (FOUO*) or develop a specialized set of countermeasures for the added 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.

The expectations are that new construction projects meet the necessary LOP, with few exceptions. In some cases, site limitations may restrict standoff distances, or fiscal limitations may prohibit the implementation of some measures. Both examples illustrate why security organizations must identify security requirements as early in the process as possible. During the design phase, there is a point where design changes are cost- prohibitive making the necessary LOP more difficult to achieve. Figure 6 illustrates how the necessary LOP corresponds with the risk assessment. It also demonstrates how following the baseline LOP may result in wasted resources or unmitigated risk.

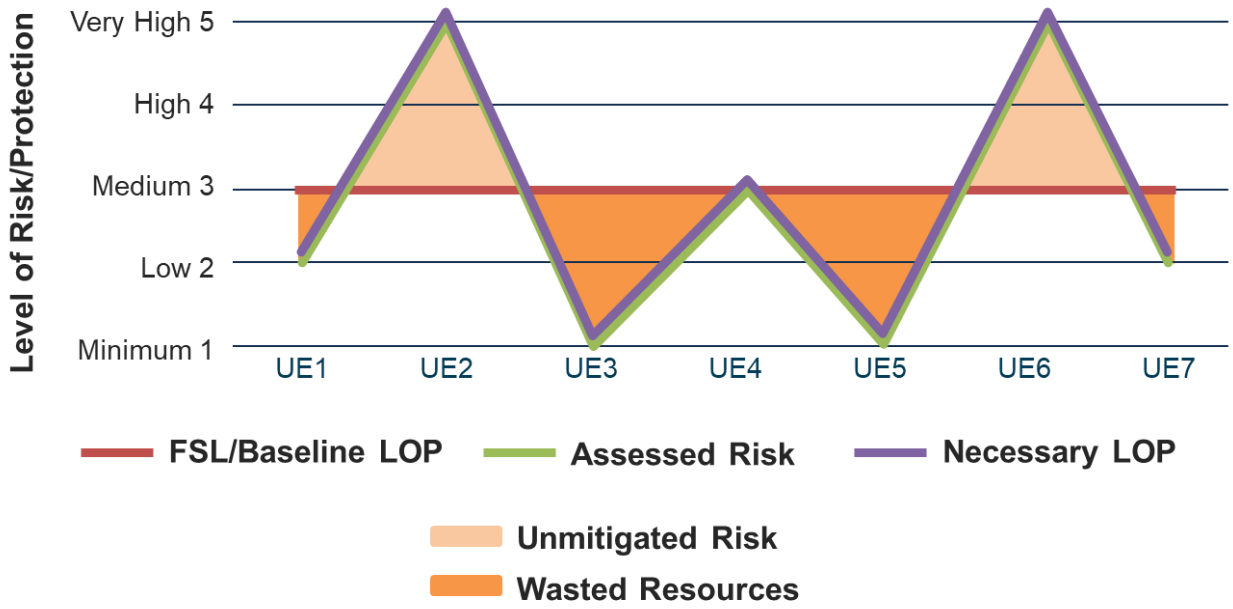


Figure 6: Example of Unmitigated Risk and Wasted Resources

8.2.3 Evaluate Existing Level of Protection

Organizations can find the existing LOP through 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.

The security organization evaluates the facility to determine whether the existing LOP is satisfactory and meets the necessary LOP. If the existing LOP does not match with the necessary LOP, the security organization identifies the difference between the LOPs and the countermeasures necessary to mitigate the existing vulnerability. However, if conducting a risk assessment for new construction, the security organization should consider construction design (e.g., setback) or security related features that may already exist (e.g., limited observation areas or avenues of approach) in determining vulnerabilities. In some situations, security planners may have to assume complete vulnerability. Figure 7 illustrates how the existing LOP may differ from the assessed risk and necessary LOP.

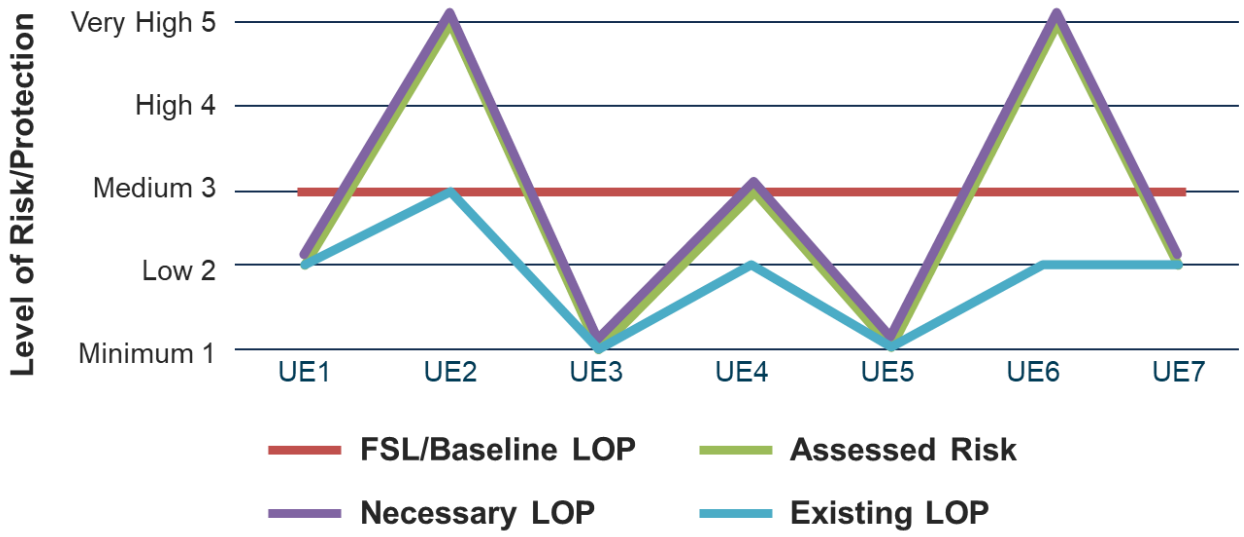


Figure 7: Example of Existing Level of Protection Compared to Necessary Level of Protection

8.2.4 Risk Assessment Report

The security organization will provide a written initial report or equivalent documentation and a verbal briefing of the risk assessment results to the responsible authority. The report must include the final FSL determination and any reference to an intangible adjustment/consideration, risk assessment using the DBT report, and countermeasures necessary to mitigate identified risks.

No later than 45 days after the initial report, the security organization will provide the final risk assessment report that:

- Provides a scope of work with estimated cost of each identified countermeasure.
- Provides written operating procedures for identified countermeasures.
- Identifies how each countermeasure will meet the necessary LOP to mitigate identified risk(s) to include any cost-saving benefits.
- Provides all documents requested by tenant agency representatives, their headquarters and/or funding authorities related to the implementation of any identified countermeasures.

Once the security organization presents a credible and documented risk assessment and the responsible authority accepts, it 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.

8.2.5 Responding to Risk Assessments and Identified Countermeasures

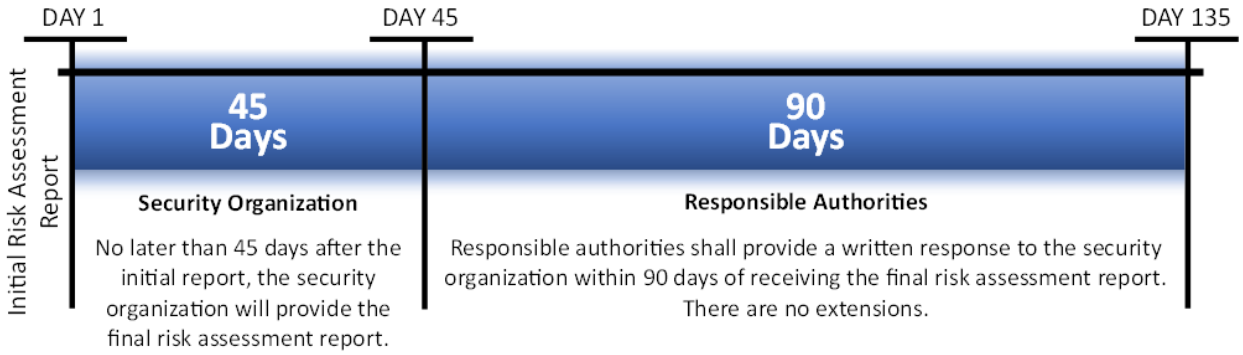


Figure 8: Risk Assessment Response Timeline

Responsible authorities shall provide a written response to the security organization within 90 days of receiving the final risk assessment report containing all documentation as outlined in section 8.2.4. This 90-day period includes *all* FSC deliberations and coordination **with organizational headquarters**; **there is no extension**. The response must contain decisions made regarding identified countermeasures needed to meet the necessary level of protection. The response may include plans to fully implement the identified countermeasures and plans to implement a lower LOP and/or risk acceptance. If accepting risk, organizations must document the risk acceptance as outlined in section 8.4.2. If the responsible authority disagrees with the identified countermeasure (e.g., the security organization recommends additional guards not required by Appendix B), they should note this in their response. FSCs develop responses supported by the voting process outlined in section D.3.5.

8.3 Step Three: Develop Risk Management Strategy

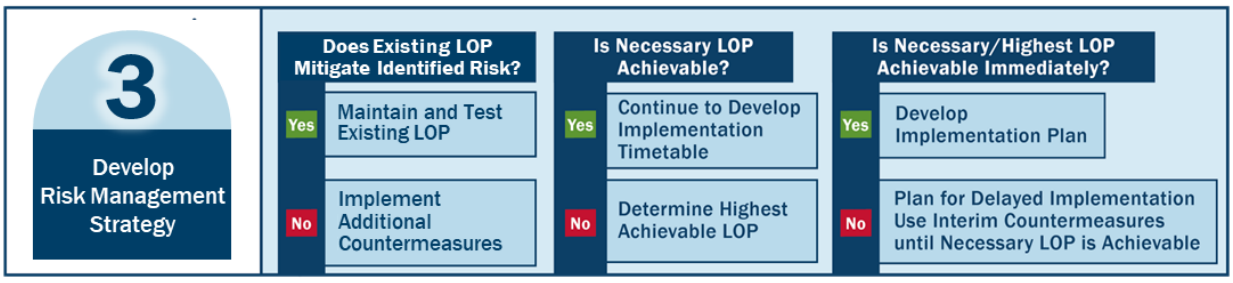


Figure 9: Develop Risk Management Strategy

In step three, the responsible authority develops a risk management strategy, in consultation with the security organization, owning or leasing authority, and in some instances the organizational security element.

- If the existing LOP aligns with the necessary LOP, retain current countermeasures and test on a regular basis. Monitor conditions at the facility for changes that may impact the effectiveness of countermeasures or the necessary LOP.

- or -

- If the existing LOP does not align with the necessary LOP, implement additional countermeasures to mitigate the risk. If the existing LOP exceeds the requirements for the necessary LOP, the organization should consider reducing the LOP to ensure allocation of resources to mitigate identified risk[11].

Key questions asked when developing the risk management strategy:

- If the existing LOP and necessary LOP do not match, is the necessary LOP achievable?
- If the necessary LOP is not achievable, what is the highest achievable LOP per UE?
    - Does the achievable LOP mitigate risk to an acceptable level?
- Is the identified countermeasure cost-effective?
- Is the necessary or highest LOP achievable immediately? If not, what are some compensatory or interim measures to mitigate risk?
- If the necessary LOP is not achievable, what is the amount of risk accepted?

8.3.1 Is the Necessary LOP 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 necessary LOP is achievable. Specifically, they must decide whether implementing 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 or the expected risk level mitigated. When a countermeasure's return on investment is not a practical security business decision, as would be the case with a lease that is soon to expire, investing in the countermeasure may not be fiscally responsible.

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 spend that money for little gain.

In an existing facility, physical limitations and budgetary restrictions may make the necessary 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 an identified 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, organizations should consider all costs, including life-cycle costs, direct project costs, and costs associated with indirect impacts (e.g., business interruption, relocation costs, or road closures).

[11] See Figure 6: Example of Unmitigated Risk and Wasted Resources

If the responsible authority rejects implementation outright or defers implementation due to cost (or other factors), document the decision — including the acceptance of risk.

- If the necessary LOP is achievable, develop an estimated timetable for implementation.

- or –

- If the necessary LOP is not achievable, identify the highest achievable LOP.

8.3.2 Determining the Highest Achievable LOP

If the responsible authority determines that it cannot implement the necessary LOP, they must identify the highest achievable LOP. Identification of the highest achievable LOP requires a continuous process of examining the countermeasures included in the next lower LOP, deciding if that level is achievable, and, if not, repeating the process with the next lower LOP. This approach minimizes the amount of risk accepted.

For example, an assessment may find the risk of a hazardous substance introduced into ground-level air intakes is high. The necessary LOP may call for the air intakes to be located on the rooftop. In an existing federal facility, the configuration of the air-handling system may make a retrofit cost-prohibitive or even physically impossible. During a lease process, the market survey might show that no facilities in the delineated area have such a configuration. As such the project team will consider the next lower LOP which calls for monitoring the ground-level air intakes with VSS and guard patrols. The documentation must clearly reflect any reason why the necessary LOP is not achievable.

8.3.3 Is LOP Achievable Immediately

The amount of preparation needed to implement a countermeasure may limit its immediate achievability. If funding is available, organizations can generally implement the countermeasure almost immediately. Delays may occur when countermeasures require advance budgeting or coordination with owners and outside authorities for approval. In these instances, consider first incorporating no-cost countermeasures (such as a procedural change) into an ongoing or planned project (such as a lobby redesign).

In the case of new construction, organizations integrate countermeasures into the building-design and implement 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, or coordination among multiple government tenants causes delay.

- If the necessary/highest achievable LOP is immediately achievable, then implement.

- or –

- If the necessary/highest achievable LOP is not immediately achievable, plan for delayed implementation, and use interim countermeasures to temporarily mitigate the risks and document risk acceptance.

8.3.4 Is the Risk Acceptable

The responsible authority considers the amount of risk accepted with the highest achievable LOP when it does not align with the necessary LOP.

Organizations must accept the risk that arises from the difference between the protection afforded by the necessary LOP and the reduced protection afforded by the highest achievable LOP.

Responsible authorities minimize the amount of risk accepted through the deliberate process described in this standard. **Regardless of site conditions, the LOP implemented may never be less than Level I Minimum** found in *Appendix B: Countermeasures (FOUO)*.

If the necessary LOP is unachievable and the remaining risk at the highest achievable LOP is not acceptable, consider an alternate location where the necessary LOP is achievable (including the possibility of a new lease construction or expanding the delineated area). Inherent in this process is an assessment of the potential facility to ensure it can meet the necessary LOP. When deciding if an alternate location is an option include consider:

- Limitations on the delineated area
- Mission need
- Market condition
- Timeframe
- Budget

If alternate locations are available, evaluate them to find if any different risks are inherent in that location and if the necessary LOP is achievable. Although the original security requirements are still applicable, evaluate site-specific conditions to determine if there is a change in risk at the alternate facility. For example, an alternate facility might be in a higher crime area that requires additional theft-prevention measures.

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 in a specific, delineated area that limits the availability of alternate sites. If an alternate location is not feasible, the tenant may have to implement a lower LOP and accept risk.

8.3.5 Application to Project-Specific Circumstances

The effective design and installation of security countermeasures depend on partnerships between the owning/leasing authority, physical security specialists, design professionals, facility engineers, and resource managers. Organizations must ensure close coordination with all stakeholders from the initial planning and requirement development phases, on any new construction project or addition or alteration of an existing building or campus. The coordination continues through design, contracting, and actual construction and installation. Consult with subject matter experts (i.e., blast mitigation) to ensure application of the right risk mitigation.

8.3.5.1 Application to New Construction

Organizations apply this standard for future construction (whether lease-construct or government-owned), as part of the requirements definition-process. The security organization will conduct a project-specific risk assessment during the requirements definition phase and identify design features and specifications.

8.3.5.2 Application to Existing Federal Facilities

Organizations apply this standard for existing federal facilities (leased or government-owned) as part of the recurring risk assessment.

Address historic buildings in the same manner as other existing buildings. U.S. Department of Interior regulations found in title 36 CFR Part 800[12] govern compliance with Section 106 of the National Historic Preservation Act.[13] Coordinate with the State Historic Preservation Officer consistent with established agency implementing procedures. Design alternatives for incorporating the necessary security measures into the historic property with a design professional to balance historic preservation goals and security requirements.

8.3.5.3 Modernization and Renovation

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

Specifically, the following applies:

[12] Please see https://www.ecfr.gov/current/title-36/chapter-VIII/part-800, accessed 8 August 2023.
[13] Establishes a national preservation program and a system of procedural protections, which encourage both the identification and protection of historic resources, including archeological resources, at the federal level and indirectly at the state and local level.

- When renovating an existing building, the security organization will conduct a project-specific risk assessment during the requirements definition phase. Review prior security assessments and delayed implementation plans to identify countermeasures deferred because of facility constraints or cost considerations.
- When an existing building or space is to have a change in building use or function (e.g., converting a warehouse 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.
- When designing and constructing additions to existing buildings, the security organization will conduct a project-specific risk assessment for the addition. If the addition is 50% or more of the gross area of the existing building, apply this standard to the entire federally owned, leased, or controlled space (existing portions and the addition).

The responsible authority decides whether to implement the identified countermeasures as part of the modernization or to continue accepting the risk in all cases. The project program and prospectus proposal incorporate approved countermeasures.

8.3.5.4 Application to Lease Solicitations

This standard applies for new lease acquisitions, lease-construction, and succeeding leases established through full and open competition. This includes during the requirements definition, negotiation, and build-out phases.

If there is a current risk assessment when renewing, extending, expanding, superseding, or establishing succeeding leases through means other than full and open competition, there is not a requirement for a new risk assessment. However, if anticipating a change in tenant(s) or mission, the security organization shall conduct a new risk assessment. Otherwise, continue with the risk assessment schedule established for the facility.

A new risk assessment during the renewal process provides an opportunity for the responsible authority and leasing organization to address risks previously accepted.

Conducting market surveys will provide the prospective tenant and the leasing agency (if different from the tenant agency) with information regarding whether the LOP is achievable in the delineated area. The security organization will present any additional risks and any additional countermeasures or design features to the tenant(s) to decide whether to implement them in the requirements of the solicitation or accept the risk. If the delineated area cannot meet the required LOP and it is not possible to implement other countermeasures to mitigate risk to an acceptable level, the prospective tenant(s) and leasing agency will decide whether to change the delineated area. Consider factors affecting the feasibility of altering the delineated area, such as mission needs, market conditions, timeframe, budget, and operational considerations.

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

The security organization will update the risk assessment on offers in the competitive range to identify threats and vulnerabilities for the specific properties and identify any additional security measures. The tenant(s) will decide which additional security measures to adopt or whether to accept the risk. If different from the tenant agency, the leasing agency will decide on the implementation of additional countermeasures in the procurement, incorporating major items as an amendment to the solicitation. Present minor items and quantitative changes to individual offerors before final proposal revisions or include them in the build-out phase post-award.

Should none of the offers received meet the LOP requirements of the solicitation, the prospective tenant(s) and leasing agency should consider expanding the delineated area. 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.

8.3.5.5 Campus Environments

In a campus environment, site-specific conditions will dictate how campus-wide countermeasures impact individual facilities and exterior restricted areas. The responsible authority should consider the campus security characteristics when establishing security countermeasures for each facility within the campus.

For example, the characteristics of a facility located within the confines of a campus may require screening of visitor vehicles prior to entering the parking garage. If the campus security screens visitor vehicles before entry, there is no need for additional screening before entering the parking garage of a specific building. 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.

8.3.5.6 Purchases

The security organization will conduct a project-specific risk assessment during the requirements definition phase. Consider required countermeasures and design features as part of the project cost and include them in the scope of work needed to make the building suitable for occupancy. The tenant representatives on the project team will decide whether to implement the necessary LOP or accept the risk.

8.4 Step Four: Implement Risk Management Strategy

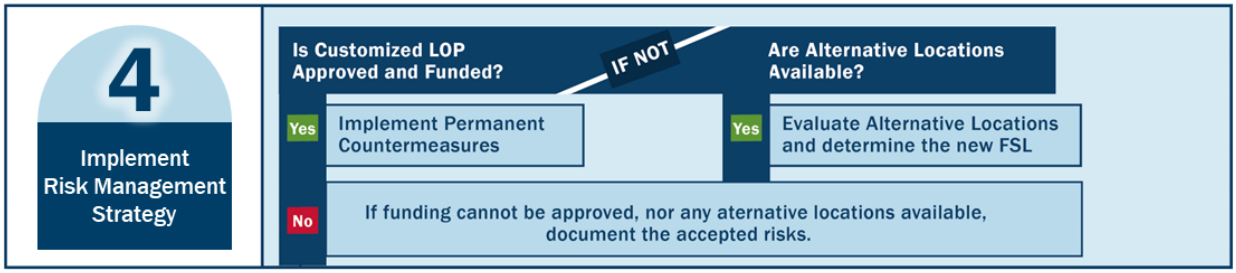


Figure 10: Implement Risk Management Strategy Overview

The responsible authority, the security organization and owning/leasing authority, supported by the tenant(s) organizational headquarters are responsible for implementing the risk management strategy once developed.

The strategy will consist of implementing a customized LOP to meet the necessary LOP, or as a last resort the achievable LOP with documented risk acceptance. The customized LOP is a final set of countermeasures developed as the result of the risk-based analytical process. Once established, implement the customized LOP. *Appendix B: Countermeasures (FOUO)* provides specific information regarding implementation.

8.4.1 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.

The threat to federal facilities is real, and the decision to accept risk could have profound consequences. For that reason, decision-makers should obtain all the information they deem necessary to make a fully informed decision.

In some instances, risk acceptance is unavoidable. It is not always possible to reconcile competing requirements, standards, and priorities. All budgets have some limitation, and it is not possible to ignore political and mission requirements.

8.4.2 Documenting Risk Acceptance

Once the responsible authority has considered and documented alternative risk mitigation strategies, accepting the risk is an allowable outcome of the risk management process.

For this standard, implementing a lower LOP than the necessary LOP results in risk acceptance. For example, if funding is not available for a countermeasure, the responsible authority and security organization shall document the lack of funding availability and implement the highest-achievable countermeasure. The responsible authority shall document all aspects of the chosen risk management strategy to include interim countermeasures and include this documentation in the risk acceptance documentation.

When an 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. The responsible authority shall receive a copy of this documentation.

The risk acceptance documentation **must clearly state the reason** why the necessary LOP is unattainable. Organizations **must document the rationale** for accepting risk, **including alternate strategies** considered or implemented and **opportunities** in the future **to implement the necessary LOP**. A fillable Risk Acceptance Template is in the Attachments. Follow ISC Facility Security Committee guidance regarding retention and documentation of risk acceptance.

Risk(s) accepted at the facility level may have an impact on agency-wide risk management efforts. Therefore, the responsible authority will provide the facility-approved risk management strategy associated with risk acceptance to the headquarters security office for awareness, along with any supporting documentation. In the case of multi-tenant facilities, the headquarters security offices of each tenant must receive this documentation.

Organizations shall establish and implement policies and procedures for reporting facility risk acceptance to the organizational headquarters.

Additionally, organizations should consider establishing policies regarding the level of approval and acknowledgement of risk(s) based on organizational tolerance for risk as well as mission. For example - the organizational headquarters must approve and acknowledge all risk that meets the following criteria:

- If any necessary Level of Protection (LOP) categorized as "very high" or "high" is not achievable, or
- Any achievable LOP that is two or more LOPs below the necessary LOP.

Although this kind of policy is easier to put in place at single tenant facilities, multi-tenant facilities should consider ways to include organizational headquarters engagement and incorporate it into their facility security committee by-laws.

8.4.3 Protection from Liability

Responsible authorities formally acknowledge the acceptance of risk and alternative strategies. For Facility Security Committees, the FSC Chair provides this acknowledgement and should include meeting minutes with votes from the FSC (See appendix D). In all cases, the responsible authority should coordinate the acknowledgement of risk, with the security organization, owning or leasing authority, and representatives of tenant organizational security elements.

Federal employees acting within the scope of their duties are protected from personal tort liability. *See* Federal Employees Liability Reform and Tort Compensation Act of 1988 (Westfall Act). For additional information seek advice from Agency legal counsel.

8.4.4 Implement Interim Countermeasures

Implementation of interim countermeasures is a risk mitigation strategy between risk identification and final countermeasure implementation or deployment. Consider interim countermeasures when identifying risk, but the permanent countermeasures are not immediately achievable. The risk mitigation or 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, temporary barriers that meet ASTM ratings may meet vehicle barrier requirements but permanent barriers that match the facility design may ultimately replace temporary barriers. In other cases, interim countermeasures may provide less protection but may still mitigate the risk to a reasonable degree until the full LOP is attainable. For example, implement a visual inspection of identification badges while waiting installation of an electronic access-control system.

The countermeasures identified as necessary and/or 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.

8.4.5 Establishing Level of Protection Templates

Some 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 at each location. The LOP template would serve as a boilerplate incorporating a set of security requirements into the development of these facilities instead of repeating the entire customization process for each CCC. In essence, the agency is creating a security design guide, starting with the selection of a common LOP. When initiating new projects, the LOP template avoids replication of the customization process, shortens the lead time required to identify security requirements, and serves as the basis for cost-estimating, and encourages standardization across common facility types.

Organizations develop a LOP template using the same processes discussed in Section 8.0 The ISC Risk Management Process. In all cases, conduct site-specific assessments to mitigate any additional risks not covered by the LOP template.

8.5 Step Five: Measure Performance

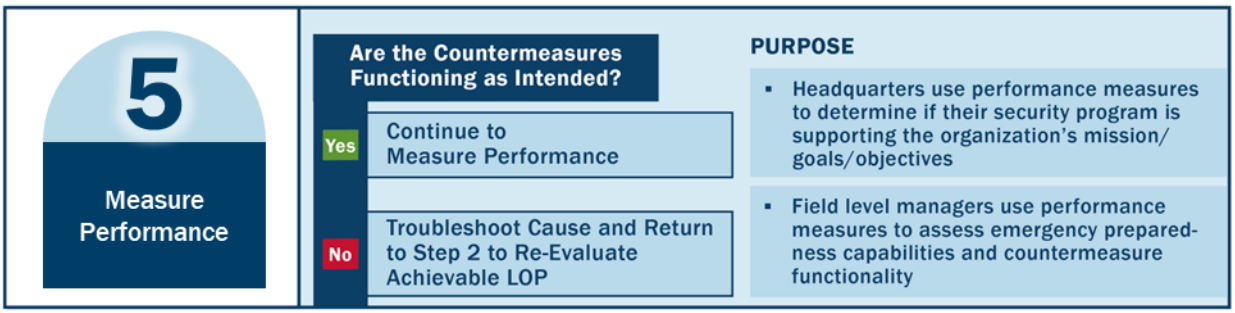


Figure 11: Measure Performance Overview

The fifth step of the risk management process is to measure performance. The purpose of this step is to ensure the implemented countermeasures or security programs are functioning as intended.

Performance measures are a useful tool for decision-makers at all levels of an organization. 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 indicate additional training. Ultimately, performance measures are critical in making resource allocation decisions. In accordance with OMB Memorandum M-21-27, Evidence-Based Policymaking: Learning Agendas and Annual Evaluation Plans, agencies are expected to use an evidence-based approach to further both mission priorities and organizational operations. This approach relies on evidence and data to strategically plan and make decisions at all levels of government.

8.5.1 Countermeasure Testing

The security organization will document and provide the completed countermeasure testing results to the responsible authority (see section 5.4).

For countermeasures not tested by the security organization, the organizational headquarters will consider testing as part of their required security performance measurement program.

8.5.2 Security Program Performance Measures

Performance Measurement is the ongoing monitoring and reporting of a program's progress and accomplishments, using pre-selected performance measures. Objective, unbiased information about accomplishments, 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 security programs and facility security countermeasures.

8.5.3 Headquarters and Field Level Interaction

Agencies must implement a performance measurement program that links the specific measures to organizations 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 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 identified 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 agency headquarters or field manager initiatives drive performance measures, 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.

The ISC does not specify how organizations document performance measurement. Organizations should use a standard format to ensure repeatability performance measurement development, customization, collection, and reporting activities. NIST SP 800-55 Rev. 1, Performance Measurement Guide for Information Security | CSRC (nist.gov), Table 2, *Measures Template and Instructions* and *Appendix A: Candidate Measures* offers a template. For additional information see Appendix E: Security Performance Measures.

9.0 Compliance and Verification

Executive Order EO 14111 requires the monitoring of compliance with the policies and standards of the Committee. Monitoring compliance shall consist, at a minimum, of the following:

- compliance benchmarks to measure compliance progress;
- periodic compliance reporting by all relevant agencies; and
- conducting risk-based compliance verification

Compliance with ISC policies and standards empowers agencies to make defensible, risk-based, and resource-informed decisions that enhance security across the federal community.

Verification confirms an agency's compliance and aligns with the Government Accountability Office's recommendations, enables the sharing of best practices across organizations, increases an agency's confidence in their compliance efforts, and provides defensibility in their compliance efforts.

For more information about compliance and verification go to Interagency Security Committee Compliance Program | CISA.

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

Appendix B: Countermeasures (FOUO)

Appendix C: Child-Care Centers Level of Protection Template Implementation Guidance (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.

Figure 12: RMP FOUO Appendices and Access Instructions

Appendix D: How to Conduct a Facility Security Committee (FSC)

D.1 Introduction

Facilities housing two or more federal tenants require an FSC to make security decisions for the facility. The owning or leasing authority is in the best position to determine this requirement and **shall** specify the need for an FSC and communicate this requirement in writing to the prospective tenants during the lease acquisition process. This includes determination and notification of the primary tenant.

Although optional, the ISC advocates that single-tenant facilities create a Facility Security Committee (FSC) or an equivalent entity to systematically address unique security concerns pertaining to the facility. At a minimum, single-tenant facilities must document internal procedures for making security decisions.

In addition to decisions relating to implementing or removing countermeasures, FSCs are also responsible for establishing and implementing security operations and administration criteria per *Appendix B: Countermeasures (FOUO)*. (Such as development of an OEP, FSP, etc.) Specifically, FSCs must develop and administer countermeasures, policies, and procedures related to security oversight and life, safety, and emergency procedures.

D.2 Facility Security Committees

The Facility Security Committee (FSC) comprises five major categories of members which include the chairperson, tenant representatives, security organization, owning or leasing authority and other supporting personnel. All FSC members must:

- Complete the required ISC training (section 6.0) within 90-days of assignment.
- Prepare for, attend, and actively participate in meetings.
- Interface with their respective headquarters.
- Vote on behalf of their agency if they represent a rent-paying federal tenant.
- Maintain required records.

Each FSC will have a chairperson preferably an on-site employee or one who regularly visits or works from the facility. Should the primary tenant[14] decline to provide an FSC chairperson, the FSC members may select a chairperson by majority weighted vote. The FSC chairperson must represent a rent-paying agency. In the event no other members accept the role of FSC chair, the primary tenant retains responsibility. The primary tenant will notify their organizational security element, who will then work towards a resolution. ISC regional advisors are available to assist upon request.

Each federal tenant that pays rent on space in a federal facility will have one representative with one weighted vote on decision items before the FSC. The owning or leasing authority and security organization are members of the FSC; however, they have voting privileges only if they pay rent on

[14] 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.

and occupy space in the federal facility. FSCs should include the child-care center director (as applicable) as a non-voting member. Within 60 days of occupying a facility, FSC members shall include new tenants.

D.2.1 Facility Security Committee Roles and Responsibilities

D.2.1.1 FSC Chairperson

The FSC chairperson shall be the senior representative of the primary tenant and serves as the FSC point of contact. The senior representative may delegate this authority to a senior staff member with decision-making authority to serve as the FSC chairperson; however, the senior representative retains the responsibility for the FSC and must document this delegation. The chair is responsible to:

- Establish the Facility Security Committee
- Schedule FSC meetings, set agendas, call for votes, and distribute meeting minutes.
- Maintain training records for all FSC members.
- Coordinate with outside organizations.
- Assign tasks to other FSC members for drafting plans.
- Maintain current list of federal tenant occupant status to include tenants' square footage.
- Invoke FSC decision-making processes, if required.

D.2.1.2 Facility Security Committee Members

FSC members shall be management level 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. FSC members are 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. FSC member tasks:

- Represent organizational interests.
- Obtain guidance on how to vote for issues with funding implications.
- Obtain assistance from the organizational security element.

D.2.1.3 Owning/Leasing Authority

In addition to responsibilities outlined in section 5.5, the owning/leasing authority is responsible to advise the FSC on real estate or building related matters, and to assist the FSC with reporting compliance information.

D.2.1.4 Security Organization

In addition to responsibilities outlined in section 5.4, the security organization is responsible for the following:

- Advise the FSC on security or protection related matters.
- Perform and present preliminary FSL assessment to the FSC.
- Conduct, present, and distribute a risk assessment in accordance with the time intervals established by the ISC based on the approved FSL.

- Provide all documents requested by tenant agency representatives, organizational headquarters and/or funding authorities related to the implementation of identified countermeasures.
- Advise the FSC chairperson on their progress in obtaining the funding necessary from each tenant agency for approved countermeasures.
- Provide technical assistance and guidance to the FSC as appropriate.
- Assist FSC with reporting compliance information.

D.2.1.5 Other Supporting Personnel

FSCs can benefit from "non-voting" support personnel that can provide subject matter expertise. Agency headquarters are responsible for providing timely advice and guidance when needed. Additionally, the headquarters element for each FSC representative must budget for countermeasure requests from the facilities it occupies. When requested, the physical security element at the headquarters level must advise and assist the FSC representative. If the FSC representative at a facility cannot resolve a technical or financial dispute, then the respective security or financial headquarters element for each FSC representative shall assist in reaching a solution.
Some other examples include:

- Expert resources: Cost analysts, facility engineers and technicians, and subject matter experts (e.g., Mail Program Managers, ISC Regional Advisors, Organizational Security Elements).
- Non-Federal Entities: Property managers, other non-federal lessors, lessees, local authorities, child-care center directors.

D.3 Facility Security Committee Procedures

D.3.1 Facility Security Committee Charter

The FSC shall develop a charter to formally establish the FSC. At a minimum, the charter will consist of facility location, mission statement, objective statement, list of member agencies (voting and non-voting), and each member FSC function. Refer to Appendix F: Forms and Templates for a sample charter.

D.3.2 Bylaws

FSCs should develop by-laws as an addendum to the charter. The bylaws provide guidance on such areas as meeting frequency, alternate voting procedures, training specifications, local expectations of FSC members. The bylaws should not contradict guidance outlined in this Standard. In the event an FSC charter's bylaws conflict with this Standard, this Standard shall supersede the bylaws and govern to the extent necessary to resolve the confliction.

D.3.3 Facility Security Committee Meetings

At a minimum, FSCs shall hold semiannual meetings. However, the ISC encourages FSCs to hold quarterly meetings. To effectively forecast and submit a budget request to their funding authorities, tenant agencies should dedicate one FSC meeting during the first or second quarter of the fiscal year to budgeting decisions. The FSC chairperson publishes the agenda far enough in advance of the meeting for the FSC members to assess or seek additional guidance on topic items or receiver higher headquarters guidance on voting related issues.

D.3.4 Risk Assessments

The security organization regularly conducts risk assessments of the facility (refer to Section 8.2). The FSC chairperson and the owning or leasing authority review identified countermeasures in advance of a scheduled FSC meeting.

At the FSC meeting, the security organization will provide documentation of risk assessment findings and countermeasure requirements. As part of the risk assessment presentation, the security organization will indicate if the identified countermeasure matches with the necessary LOP or if a vulnerability will remain. The FSC should invite the tenant organizational security elements to FSC meetings when there is the presentation of risk assessment results. This will aid in voting, funding, and development of alternative risk reduction strategies. After the presentation, the FSC will meet to vote on the proposed countermeasure. When voting on countermeasures, each FSC member votes to determine whether to:

- Use the necessary LOP.
- Use some of the necessary LOP and accept some risk.
- Use a lower achievable LOP and accept some risk.
- Accept all identified risks without employing any countermeasures.

Unacceptable level of risk may be occurring while waiting for a decision on whether to fund and implement and identified countermeasure.

FSCs shall provide a written response to the security organization within 90 days of receiving the final risk assessment report as required in section 8.2.5. FSCs develop responses supported by the voting process outlined in section D.3.5. If an FSC does not vote on a required countermeasure, document the associated risk relating to that decision. Meeting minutes and risk acceptance documentation are inspectable items by higher Headquarters and/or the ISC through the compliance and verification process.

During the review period, FSC representatives will consult their 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 organizational security element and financial element for guidance on votes that have a budgetary impact. The FSC representative votes to approve or disapprove proposed countermeasures and other security-related issues that come before the FSC. The FSC will follow guidance outlined in section 8.4.1 to document accepted risk. The meeting minutes document any voting delays and why (e.g., lack of information provided by a stakeholder organization).

D.3.5 Voting Procedures

To ensure adequate time for review and consultation, voting is only permitted on agenda items identified as decision items. The FSC chair should schedule the first vote within 45 days of receiving the final risk assessment report but no later than 90 days (see section 8.2.5) 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 the OMB website. The RSF of assigned space (by percentage of total square footage for the building) for each federal tenant weights each vote. (See Table 9).

For a valid vote, a quorum of 50 percent of the FSC tenant organizations, representing at least 51 percent of the RSF must cast a vote on a decision item. A decision item passes when the proposal receives more than 50 percent of the FSC weighted votes. If an FSC member cannot attend a meeting, they may submit a vote on an agenda item in advance. The meeting minutes must reflect the vote provided ahead of time. FSCs should discourage abstention voting, as it will count as a "no" vote due to the potential outcome of risk acceptance if a security measure fails to pass. The minutes must include the reason for any "no" or "abstention" votes.

FSCs must document the result in the meeting minutes if the necessary condition for a valid vote is not present. The FSC Chair may then schedule another time for the vote or immediately **submit the matter to a second level review** (Figure 15).

Table 9 illustrates weighted voting 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, add vacant space 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.[15]

The FSC Chair can make these calculations for an entire facility by using the ISC Pro Rata Voting Share Calculation Tool.

Table 9: Example of FSC Weighted Votes

Agency Tenant	Agency/Bureau Code	Square Feet	% of Total RSF	Pro Rata Voting Share
DOJ – Legal Activities and USMS (includes U.S. Trustees, USMS and U.S. 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%

[15] To exclude 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.

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%

D.3.5.1 Decision Item Approval

When the FSC approves an agenda item decision, the meeting minutes shall reflect the decision. If the vote approves the implementation of a security countermeasure, this represents a financial commitment by each federal tenant in the facility regardless of how each FSC representative voted. All federal tenants in the facility shall provide their prorated share of the cost to fund the approved countermeasure.

Notification of the decision to the security organization, owning/leasing authority, or implementing agency is through their FSC meeting participation and receipt of the meeting minutes. They shall also be responsible for reporting to the FSC chair their progress in obtaining funding necessary to implement the countermeasure(s).

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, GSA does not require the FSC to provide a signature for an approved security feature to modify a tenant Occupancy Agreement (OA).
- The security organization, owning/leasing authority, or the organization implementing the security countermeasure should be prepared to accept funding from multiple sources and from mixed fiscal years, if applicable.
- 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 there is not an agreement on alternative proposals, then document this acceptance of risk in the FSC meeting minutes. The lessee's requirement to accept risk should be a consideration at the time of lease renewal.

D.3.5.2 Decision Item Disapproval

The meeting minutes must document each agency's vote to approve or disapprove an identified countermeasure. If the meeting participants reject a decision item, the minutes must document the basis for risk acceptance, or the alternative risk management strategy chosen. The FSC chairperson shall maintain meeting minutes as an historical document for the facility. Provide each member of the FSC and their respective security element at the organization headquarters level with a copy of the meeting minutes documenting the chosen risk management strategy. The security organization will maintain documentation of the decision, as well.

D.3.6 Facility Security Committee Funding Process

This section supplements *Section 7.0, Financial Guidance*. The FSC considers changes to their facility's security posture by adding new policies, changing existing policies, or by implementing or enhancing 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). Funding requests for security countermeasures and upgrades often compete with other funding requests at the organizational headquarters level. Accordingly, FSC representatives must facilitate the information flow between the FSC and their headquarters (unless the representative has funding authority). Organizations must be prepared for countermeasure funding requests and ensure their annual budget requests consider the number of locations they occupy and the projected requests for security countermeasure funding.

The FSC chairperson shall establish a date for a vote on all decision items requiring funding, while providing a reasonable period for FSC representatives to obtain guidance from their respective organization (up to 90 calendars days after receiving all documents and materials necessary to supply respective funding authorities).

If organizations do not provide guidance to the FSC representative within this allotted time, the FSC chairperson may use the FSC decision process, or other means as determined by the FSC, to obtain a resolution. The meeting minutes must document each agency's vote to approve or disapprove a required countermeasure.

Step 1: Security Organization Presents Countermeasures Implementation and Funding Plan to the Facility Security Committee or Facility Security Committee Member or their Funding Authority Requests Removal of Previously Implemented Countermeasure.

Facilities may have numerous security countermeasures in place, and the FSC may or may not have approved them by vote. As these countermeasures may have budgetary impact on the tenant organizations, there shall be a mechanism to cancel or remove previously implemented countermeasures that are no longer necessary.

When a funding authority or headquarters security element notifies an FSC that funding for a countermeasure is no longer available the tenant agency FSC member 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 pro rata vote of the tenant agencies. Tenant organizations are responsible for all costs associated with removal. When there is approval for the removal of a countermeasure, the agency responsible for the implementation shall cease or remove the countermeasure by the date specified by the FSC.

Step 2: Facility Security Committee Members Request Guidance from Their Respective Funding Authority.

Step 3: Vote - Did the Facility Security Committee vote to approve or disapprove the security proposal?

- Approved: Implement countermeasures
- Disapproved: Consider alternative strategies as noted in section 8.3. This decision point is an iterative loop for the purpose of facilitating technical discussions between the security organization and the organizational security elements of the FSC members. Discussions help promote creative thinking and evaluate multiple countermeasures to mitigate risk.

Figure 13: FSC Funding Process

Step 4: 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.

D.3.6.1 Financial Commitment

An FSC vote to approve a countermeasure is a financial commitment by each federal tenant that pays rent for facility space.

Should an agency vote not to approve a countermeasure, but the FSC votes to approve the countermeasure, the agency is responsible for providing funds for their prorated share of the cost of the approved countermeasure, regardless of their vote. 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 D.3.5.1 Decision Item Approval.) The security organization, owning/leading authority, or implementing authority shall coordinate with each tenant agency funding authority on the transfer of that agency's pro rata share of the funds. Organizations must provide written estimates for when funding will be available.

D.3.7 Risk Acceptance

If an FSC makes the decision not to approve or provide funding for a countermeasure, this constitutes risk acceptance. The FSC representative shall provide a copy of the denial of organizational funding and risk acceptance documentation to the chairperson of the FSC for inclusion in meeting minutes.

D.4 Facility Security Committee Operations

The FSC may consider many issues regarding their facility's security. This standard includes process charts to aid each FSC when making decisions that will determining the facility's security posture.

If the FSC representatives are unable to resolve an issue, the decision process (see section D.4.2 FSC Decision Process) flow chart provides an outline for reaching resolution. The objective is for the FSC to make decisions for their respective facility regarding countermeasures to implement at the lowest level. 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 14 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, use the funding process (see Figure 13). If the decision does not carry a funding impact, each FSC representative has the option to request guidance on decision items.

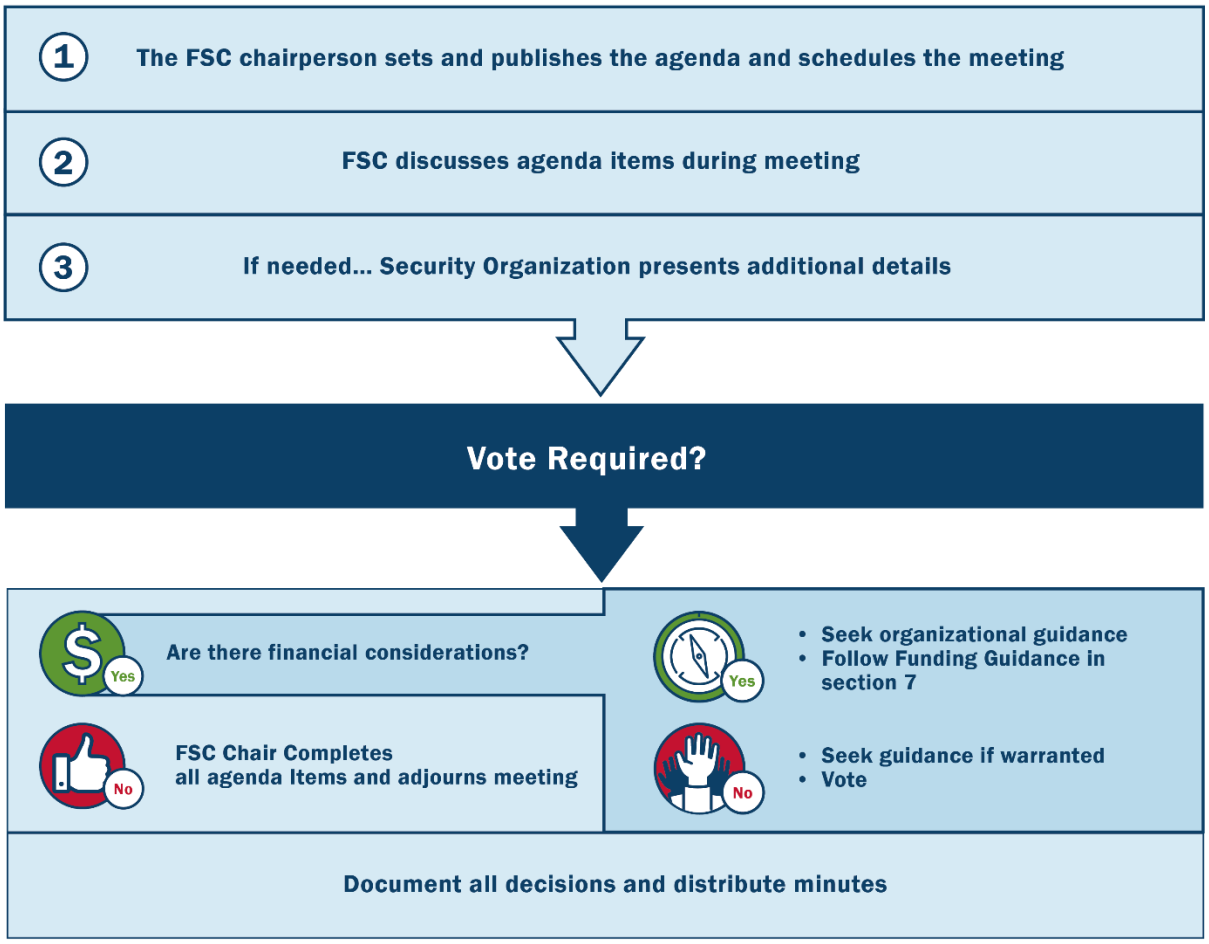


Figure 14: FSC Business Process

D.4.2 FSC 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. When the FSC receives the final risk assessment report, they begin the decision process. When the FSC is at an impasse, the FSC chair must determine whether to submit the issue for a second level review or accept risk. While the FSC moves through the decision process on a countermeasure(s) that leaves the facility vulnerable, they are accepting risk for this vulnerability until the final decision.

FSCs either use the decision process in this standard or adopt a documented alternate process, which includes the same timelines, to facilitate a decision provided it includes levels to elevate decisions within tenant organizations ending with the senior officials. The organizational structure used by each 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 FSC's Decision Process allows three opportunities to reach a decision. Most often, the process concludes at the first review by "FSC Deliberation." If an FSC cannot reach a decision, present the information to the organizational security element for each agency at the facility. The FSC is responsible to implement and manage the process at each level. The FSC will coordinate with the security organization to develop and implement risk mitigation strategies aimed at reducing the accepted risk during this process. Establish mechanisms to monitor and evaluate mitigation strategies and develop/coordinate response efforts in case of an undesirable event.

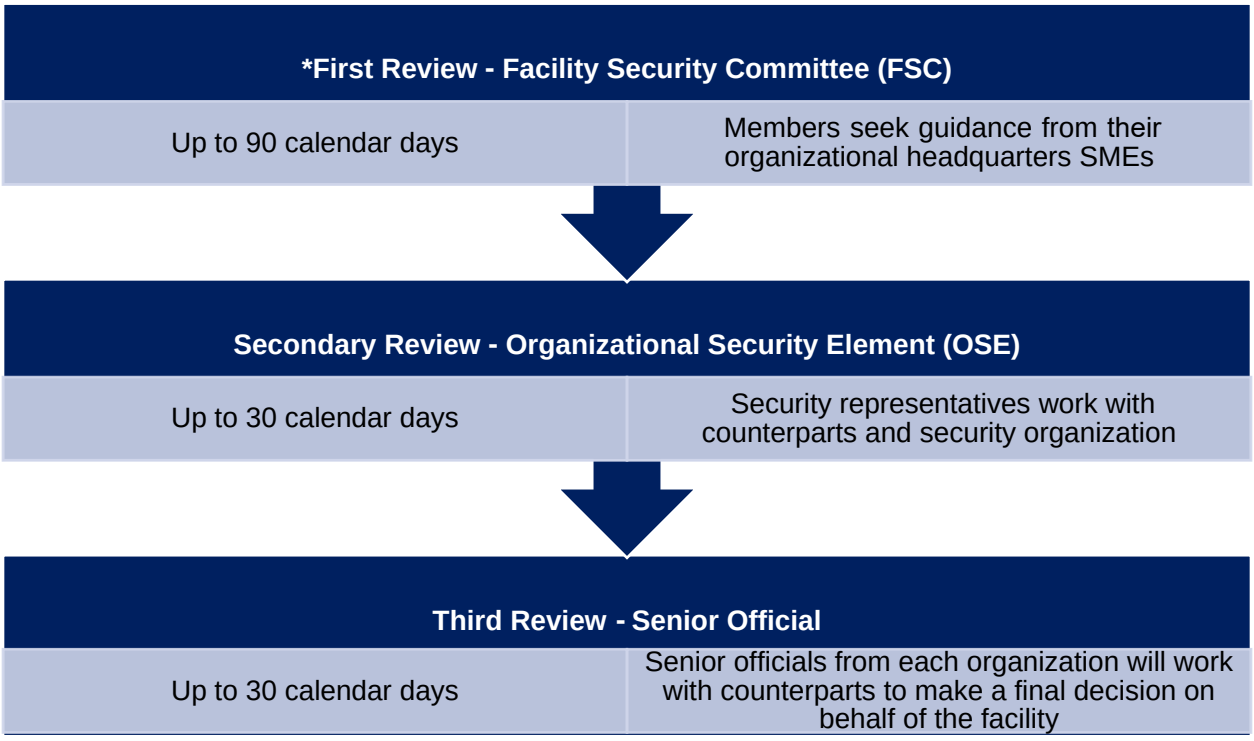


Figure 15: FSC Decision Process

* When using the FSC decision process, if the current level of review is successful, record results in the meeting minutes and appropriate actions taken. It does not need to move to the next level. If the review period was unsuccessful, then the FSC proceeds to the next level in the decision process.

D.4.2.1 First Review – Facility Security Committee

Most FSCs make decisions at during the first review through agenda item discussions and voting. The FSC chairperson has the option to continue to use additional levels of the decision process should the discussions become unproductive. Allow FSC representatives a review period to consult with their respective organizational security element for guidance when they need additional information. The FSC may also coordinate with the ISC regional advisor for additional guidance or recommendations. FSCs must complete the first review no longer than 90-days if responding to a risk assessment (see Section 8.2.5). If the FSC chair decides to submit the subject to a secondary review, the FSC must document the decision and provide the documentation to the security organization.

D.4.2.2 Secondary Review – Organizational Security Element[16]

The physical security component from each of the facility's organizations participates in a review of the issue. They evaluate the facility and the security organization's proposal, then work with representatives from the facility, their counterparts from the other represented organizations, and the security organization to develop a plan that each organization finds acceptable. If the security representatives and the security organization cannot develop a modified proposal, they will work together to develop alternative proposals, and the FSC will schedule a vote.

When the FSC representative contacts their respective organization and requests assistance, they must complete this step in the decision process within 30 calendar days of the initial contact. If a resolution is not reachable in the agreed upon timeframe, refer the issue(s) in question to each respective organizational senior official for action.

D.4.2.3 Third Review – Senior Official

The organizational security element for each tenant represented at the facility briefs their senior official on the issue in question. The senior official for each organization represented at the facility will work with representatives from the facility, their counterparts from the other represented organizations, to decide on behalf of the facility. Organizations have multiple opportunities to resolve an issue with facility-level input before the issue reaches the senior officials for resolution. If an issue rises to the senior officials for resolution, they will make a final decision, and the facility will implement this decision. Document the decision in the FSC meeting minutes.

Complete this step in the decision process within 30 calendar days of referring it to each respective organizational senior official. The FSC can request assistance from the ISC Standard Subcommittee or accept risk if unable to reach a resolution in the agreed-upon timeframe.

[16] This level includes the organizational Chief Security Officer or equivalent.

Figure 16: RMP Decision Process Timeline

D.5 Record Keeping

FSCs will retain meeting minutes, and other documents or information the FSC deems important. This includes:

- All FSC decisions.
- Vote tabulations.
- Project funding approval or disapproval.
- Risk acceptance details.

The FSC and the security organization should maintain 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.[17]

All FSC members, and organizational headquarters will have access to meeting records. Additional access to FSC records held by other agencies will require the FSC's approval. Only appropriately cleared personnel with the need-to-know shall receive records containing National Security Information (NSI) or sensitive information.

[17] NARA, General Records Schedule 5.6: Security Management Records, March 2022

Appendix E: Security Performance Measures

This guidance assists agencies with establishing or refining a comprehensive performance measurement program for assessing the effectiveness of security programs that enhance the security and protection of federal facilities. Within large agencies, security performance measures 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, the senior official should ensure the consistent application and testing of performance measures throughout the agency.

Many resources are available to assist organizations with the establishment of a security performance measurement program to include:

- Interagency Security Committee Compliance Benchmarks,
- ISC Making a Business Case for Security,
- Government Accountability Office (GAO), GAO-06-612, "Homeland Security: Guidance and Standards Are Needed for Measuring the Effectiveness of Agencies' Facility Protection Efforts", (May 2006),
- Government Performance and Results Act (GPRA) of 1993,
- Government Performance and Results Act Modernization Act (GPRAMA) of 2010,
- U.S. Army Cost Benefit Analysis Guide,
- U.S. Environmental Protection Agency (EPA) / National Center for Environmental Innovation's Guidelines for Measuring the Performance of EPA,
- NIST SP 800-55 R1, Performance Measurement Guide for Information Security[18],
- Resources | Performance.gov,
- Foundations for Evidence-Based Policymaking Act of 2018.

The Performance Improvement Council (PIC) offers a wide variety of resources to include Performance Measurement Basics, Performance Management, and the PIC Performance Principles and Practices Playbook. The Performance Improvement Council (PIC) is a government-wide body that supports cross-agency collaboration and best practice sharing. The Government Performance and Results Act Modernization Act (GPRAMA) established the PIC in 2010. The PIC's mission is to advance and expand the practice of performance management and improvement.

E.1 Performance Measurement Classification

When measuring performance, most organizations will focus on qualitative or quantitative measurements, see Table 10. Organizations will need to review their organizations goals and/or objectives to determine the measurement type that will be suited to assess the activity or initiative. Once done, the organization can select the set of benchmarks or standards for the measurement.

[18] NIST SP 800-55 R1, Performance Measurement Guide for Information Security is currently under review.

Table 10: Classification of Performance Metrics

Classification of Performance Metrics	
Qualitative	**Quantitative**

• Qualitative measurements are contextual data that measure changes in human behavior or a desired condition.
• Behavioral change may be the result of constructing a fence, installing bollards, or even installation of VSS, each achieving behavioral modification or redirection.
• Qualitative measurements utilize various methods such as interviews, surveys, or case studies.
	• Quantitative measurements are anything measured and presented as a number.
	• Typically used to measure physical occurrences or evaluated with raw datapoints; examples include:
	  ○ to measure direct throughput at security checkpoints prior to, and following, a security enhancement, degradation, or occupancy change
	  ○ evaluate cost reduction measures (using VSS…), cost avoidance….

To assist organization with developing performance measures, organizations can start with the questions below to design a set of criteria for either type of performance measure (Qualitative or Quantitative).

- What needs measurements?
- What is the measure's scope?
- What are the intangible and tangible benefits of the performance measure?
- Is available data reliable?
- When to measure and how frequent?
- How to measure and what is the basis of measurement?
- How to analyze and to determine conclusions?
- Who is the audience for the results? When and what to report?

E.2 Performance Measures

There are three basic categorizations of performance measures: input/process measures, output measures, and outcome measures.

In the *Government Accountability Office (GAO), GAO-06-612, "Homeland Security: Guidance and Standards Are Needed for Measuring the Effectiveness of Agencies' Facility Protection Efforts", (May 2006),* the GAO recommended organizations have a "particular focus on developing outcome countermeasures."

E.2.1 Input/Process Measures

Input/process measures address the type or level of program activity an organization conducts, and the resources used by the program. 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 geared toward accomplishing an objective.

Table 11: Examples of Input/Process Measures for Facility Protection

Example	Purpose
Resources required to accomplish the security program mission: • Full-Time Equivalent (FTE) employees, contract support, and training • Risk Assessments • Countermeasure installation, maintenance, testing, evaluation and replacement; and • Overall Security Program Management costs (salaries, administrative cost).	Provides program managers with an understanding of the necessary resources, including expenditures and personnel required for effective security program operations. Program managers can use this information to determine program growth, increases in cost, efficiency gains, and output costs
Track time and costs from initial completion to final approval of the risk assessment identified countermeasures.	To maximize efficient use of resources (human capitol)
Number of facilities, number assessed, number at acceptable level of risk	Program scope identification

E.2.2 Output Measures

Outputs measures focus on the direct product/services delivered by a program. Output measure means the tabulation, calculation, or recording of activity or effort expressed in a quantitative or qualitative manner. This could include changes in risk ratings over time from risk assessments.

Table 12: Examples of Output Measures for Facility Protection

Example	Purpose
Risk assessments completed versus planned	A core component of a security program is the scheduling of initial and recurring risk assessments
Timely completion of risk assessments	To assess whether the actual completion dates align with the planned completion dates and determine if they fall within the established timelines.
Cost per active background investigation file	To monitor the cost efficiency of the personnel security program, including processing of background investigations, issuance and verification of clearances, and case file maintenance
Status of identified countermeasures designed to mitigate risk	To indicate the percentage of identified security enhancements funded and implemented, and operational
Countermeasure functionality (e.g., surveillance cameras, x-ray machines)	Gauges whether a countermeasure works as intended once deployed. This measure focuses on accomplishing an established schedule for testing. Testing may include elements such as verifying proper equipment calibration, ensuring security guards are knowledgeable in post order procedures, and confirming that intrusion detection systems activate properly.

Example	Purpose
Time required for responders (guard, law enforcement, emergency response technician) to arrive/initiate response protocol	Program management, response readiness, stakeholder's trust/confidence
OEP, COOP exercises (actual vs. expected behaviors); after action report assessment	Emergency response enhancement, program management, stakeholder communication
Staff development (scheduled training vs. actual)	Program development

E.2.3 Outcome Measures

Outcome measures assess the results of a program activity compared to its intended purpose. They are particularly useful because they indicate what program activities are accomplishing. Outcome measures 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:

Table 13: Example of Outcome Measures for Facility Protection

Example	Purpose
Incident Reduction: Security violations, thefts, vandalism, etc., reduced	Strategic goal accomplishment, inventory experienced fewer security violations, etc.
Security programs operating more efficiently	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. Track, record, and summarize the results of individual efficiencies.
Strategic goal accomplishment, security measures are effective	To assess the risk-reduction benefits associated with implementing countermeasures at an individual asset.
Facility Asset Inventory Secured	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.
Emergency Preparedness	Focuses on the training degree of employees and senior management and how they perform up to expectations in emergency training exercises.

Appendix F: Forms and Templates

Select a commonly used fillable form or template to open or modify the content.

Example FSC Charter

Facility Security Committee (FSC) Charter		
[Facility Name] [Facility Address]		
Responsible Authority:	Signature:	Date:
Mission:		
Purpose:		
Bylaws: **Membership** This section establishes the roles and responsibilities of The FSC membership. Individually define the positions of chairperson, representative, tenant, leasing authority, and any other members (voting and non-voting). Be sure to include a list of respective responsibilities. Use the roster below to record the names and agencies for each member fulfilling the respective role.		
Member Roster ***denotes voting member*		
Agency	**Function**	
	FSC Chair	
	Security Organization	
	Owning/Leasing Authority	
	Tenant Representative	
	Support Specialist	
Procedures FSC shall hold meetings in accordance with processes and procedures outlined in Appendix D of the RMP. This includes procedures for voting, funding requirements, and risk acceptance. **Training** Federal employees selected for FSC membership must successfully complete the minimum training standards established by the ISC. For training details, refer to Section 6.0 Training Requirements in the RMP.		

Example Memorandum for Record-Facility Security Level Determination

MEMORANDUM FOR THE RECORD FACILITY SECURITY LEVEL DETERMINATION

FROM: [Security Organization]
TO: [First and Last Name] Responsible Authority

PURPOSE:
The purpose of this Memorandum for Record is to document the security organization's input to assist in determining the Facility Security Level (FSL) for [**insert building identification here**].
BACKGROUND:
Based on a review of the below five security factors, including considerations for an intangible adjustment, the security organization has evaluated the facility in accordance with the criteria associated to each factor to determine a preliminary FSL established by the Interagency Security Committee (ISC).
The table below details the scores for each factor according to the security organization analysis:

Table 14: FSL Determination Matrix

Factor	Points				Score
	1	2	3	4	
Mission Criticality	MINIMUM	LOW	MEDIUM	HIGH	
Symbolism	MINIMUM	LOW	MEDIUM	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 Agency	MINIMUM	LOW	MEDIUM	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					**+/- 1 FSL**
					Final FSL
* Facilities with a child-care center (CCC) receives a facility population value of "high."					

Based on this score, and consideration of any applicable intangible factors, the security organization recommends that the FSL for this facility should be: **[Insert Facility Security Level, i.e.., FSL III]**.

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

Assessor	Signature:	
Print:		Date:
Property Manager	Signature:	
Print:		Date:
Responsible Authority	Signature:	
Print:		Date:

Example Risk Acceptance Justification Form

Risk Acceptance Justification Form

Facility Name/Identification Number:	
Region/Address:	Responsible Authority:
	Risk Assessment Date:
Lead Agency:	FSL:

Introduction: After considering and documenting alternative risk mitigation strategies, the risk management process allows for the outcome of risk acceptance. In all cases, the project documentation must clearly indicate the reason why it is not possible to achieve the necessary LOP. 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.

Identified Risk: Summarize the identified risk(s) and potential impact.
Risk Mitigation: Detail the implemented or proposed risk mitigation measures designed to decrease the likelihood or impact of identified risks.
Risk Acceptance Rationale: Outline the rationale for accepting risk, including the roles and responsibilities of FSC members, the decision-making criteria, and the documentation requirements.
Documentation: Specify the documentation requirements for accepting risk, such as the completion of a risk acceptance form, sign-off by FSC members, and notification to relevant stakeholders. Add a check mark to indicate each associated documentation. Risk Assessment Cost Estimate Project Documentation Disapproval/Denial of Funds Other Documentation **Attach File**

Security Organization POC	Signature	Date

Responsible Authority	Signature	Date

Disclaimer: Federal employees acting within the scope of their duties are protected from personal tort liability. See Federal Employees Liability Reform and Tort Compensation Act of 1988 (Westfall Act). For additional information seek advice from agency legal counsel. Refer to section 8.4.3 Protection from Liability.

Information and Considerations	
For Each Identified Risk Not Fully Mitigated: 1. Summarize the identified risk, including the undesirable event addressed. 2. Identify the necessary LOP the risk mitigation would provide. 3. Summarize any alternative countermeasures instituted in lieu of the necessary LOP. 4. Identify the achievable LOP the alternative measure will provide. 5. Justify why risk acceptance is necessary. If applicable, note rationale from choices, and include details, as necessary. **If necessary, use additional paper 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 scheduled for closure 9. Lease ending

Appendix G: Resources

G.1 List of Abbreviations/Acronyms/Initialisms

Abbreviation	Full Name of Term
CCC	Child-Care Center
CESER	Office of Cybersecurity, Energy Security, and Emergency Response
CFR	Code of Federal Regulations
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
EPA	U.S. Environmental Protection Agency
EO	Executive Order
FSC	Facility Security Committee
FSL	Facility Security Level
FEMA	Federal Emergency Management Agency
GAO	Government Accountability Office
GPRAMA	Government Performance and Results Act Modernization Act
GSA	General Services Administration
GSAM	General Services Acquisition Manual
HSPD	Homeland Security Presidential Directive
IG	Implementation Guidelines
ISC	Interagency Security Committee
LOP	Level of Protection
NARA	National Archives and Records Administration
NEF	National Essential Functions
NCEI	National Centers for Environmental Information
NIST	National Institute of Standards and Technology
OSE	Organizational Security Element
RA	Responsible Authority
SO	Security Organization
PIC	Performance Improvement Council
PPD	Presidential Policy Directive
RMP	Risk Management Process
RSF	Rentable Square Footage
UE	Undesirable Event
U.S.C.	United States Code
VSS	Video Surveillance System

G.2 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 willingly accept or expose themselves to the risk that the event might occur. Extended definition: Action not deemed necessary due level of risk at which, given costs and benefits associated with risk reduction measures. Example: Extremely low levels of water-borne contaminants can be 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.
Agency	An executive agency, as defined in section 105 of title 5, United States Code.
Alteration	A limited construction project for an existing building that comprises the modification or replacement of one or several 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 preliminary countermeasures for each FSL and is only applicable until the security organization completes the risk assessment (i.e., new lease solicitation or new construction).
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.
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 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. Annotation: Commonly measure consequence in four ways: human, economic, mission, and psychological, but may also include other factors such as impact on the environment.

Term	Definition
Continuity of Government (COG)	A coordinated effort within each branch of government (e.g., the federal Government's Executive Branch) to ensure NEFs continued performance 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. These areas may also be "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.
Countermeasure	Action, measure, or device intended to reduce an identified risk, threat, or danger.
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 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.
Facility Security Committee	A committee that is established in accordance with an Interagency Security Committee standard, and that is responsible for addressing facility-specific security issues and approving the implementation of security measures and practices in multi-tenant facilities.
Facility Security Level	A categorization based on the analysis of several security-related facility factors, which serves as the basis for the identification of preliminary countermeasures and recurring risk assessments.

Term	Definition
Federal Contractor Worker	Any individual who performs work for or on behalf of any agency under a contract, subcontract, or contract-like instrument and who, in order to perform the work specified under the contract, subcontract, or contract-like instrument, requires access to space, information, information technology systems, staff, or other assets of the Federal Government in buildings and facilities of the United States.
Federal Employee	An employee, as defined in section 2105 of title 5, United States Code, of an agency.
Federal Facility	A federally owned or leased building, structure, or the land it resides on, in whole or in part, that is regularly occupied by Federal employees or Federal contractor workers for nonmilitary activities. The term "Federal facility" also means any building or structure acquired by a contractor through ownership or leasehold interest, in whole or in part, solely for the purpose of executing a nonmilitary Federal mission or function under the direction of an agency. The term "Federal facility" does not include public domain land, including improvements thereon; withdrawn lands; or buildings or facilities outside of the United States.
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	An 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 an agency.
Interior	Space inside a building controlled or occupied by the government.
ISC Regional Advisor	The ISC Regional Advisor provides field level advisory and Federal facility security expertise to Federal facility stakeholders and organizational officials to enhance the security in and protection of Federal facilities.
Lease Construction (Build- to-Suit)	A new construction project 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.
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.

Term	Definition
Mixed-Tenant Facility	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 Facility	A facility that includes tenants from multiple agencies AND at least one non-federal tenant.
Multi-Tenant Facility	A facility that includes tenants from multiple agencies but no non-federal tenants.
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 building project for an entirely new facility.
New Lease	A lease established in a new location adding 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 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, 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.
Owning or Leasing Authority	Entity authorized to enter into a lease agreement with a person, co-partnership, corporation, or other public or private entity for the accommodation of a federal agency in a facility.
Primary Tenant	The federal tenant identified by Bureau Code in Office of Management and Budget Circular No. A-11, Appendix C, which occupies the largest amount of rentable space in a federal facility.
Responsible Authority	Facility Security Committee (FSC), tenant representative for single-tenant facilities, or legal authority (i.e., c courtroom where a judge exercises authority).

Term	Definition
Risk	A measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence. 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 the potential for an unwanted outcome and 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 identification 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 risk is difficult to eliminate; however, it is usually possible to take actions to reduce it.
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.

Term	Definition
Risk Management Strategy	A proactive approach to mitigate 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 the risk to another entity based on a set of stated priorities. 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. Example: Risk mitigation greatly reduced the potential impact of the tsunami on the local population. Annotation: Implement measures before, during, or after an incident, event, or occurrence.
Risk Reduction	A decrease in risk through risk avoidance, risk control or risk transfer.
Risk Register	A repository of risk information including the data understood about risks over time. Extended definition: A central record of current risks, and related information, for a given scope or organization. Current risks comprise both accepted risks and risks that have a planned mitigation path
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 and performs preliminary FSL determinations and initial or recurring risk assessments.

Term	Definition
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) 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.
Senior Official	An organization's principle executive authority responsible for implementation and compliance ISC Standards.
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 agency.
Site	The government controls the physical land area by right of ownership, leasehold interest, permit, or other legal conveyance, on which a facility is situated.
Site Entry	A vehicle or pedestrian access point into, or exit from, the site.
Site Perimeter	The outermost boundary of a site. The property line often delineates the site perimeter.
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 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."

Term	Definition
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. Annotation: When calculating the risk of an intentional hazard, the common measure of vulnerability is the likelihood of a successful attack if attempted.

G.3 References Cited

Congress.gov

- Federal Employees Liability Reform and Tort Compensation Act of 1988 (Westfall Act), Public Law 100-694
- Foundations for Evidence-Based Policymaking Act of 2018, Public Law 115-435
- Government Performance and Results Act (GPRA Modernization Act), Public Law 111-352

Department of Energy

- Office of Cybersecurity, Energy Security, and Emergency Response

Department of Homeland Security

- DHS Lexicon

Department of Labor

- Government Performance and Results Act (GPRA) of 1993

Environmental Protection Agency

- National Center for Environmental Innovation's Guidelines for Measuring the Performance of EPA

General Services Administration

- General Services Acquisition Manual 570.301 (GSAM)
- Title 41 CFR, part 102-81, Physical Security

Interagency Security Committee

- Federal Register: EO 14111-Interagency Security Committee
- ISC Making a Business Case for Security
- Interagency Security Committee Compliance Program | CISA
- Interagency Security Committee Training | CISA

National Archives and Records Administration

- NARA General Records Schedule 5.6

National Institute of Standards and Technology

- NIST SP 800-55 R1, Performance Measurement Guide for Information Security

Office of Management and Budget

- Appendix C of OMB Circular No. A-11
- OMB Memorandum M-21-27, Evidence-Based Policymaking: Learning Agendas and Annual Evaluation Plans

Performance.gov

- Performance Improvement Council
- Resources | Performance.gov
- Government Performance and Results Act Modernization Act (GPRAMA) of 2010

U.S. Army

- U.S. Army Cost Benefit Analysis Guide

U.S. Government Accountability Office

- Government Accountability Office (GAO), GAO-06-612, "Homeland Security: Guidance and Standards Are Needed for Measuring the Effectiveness of Agencies' Facility Protection Efforts", (May 2006).

Acknowledgments

Standards Subcommittee

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

Jason Young
Chair
Department of Commerce

Jonathon Luhman
Co-Chair
Securities and Exchange Commission

Subcommittee Members

Gean Alston
Department of Homeland Security

Matthew Barbieri
Department of Commerce

William Earl
General Services Administration

Phillip Fishbeck
Internal Revenue Service

Derek Gaines
Department of Homeland Security

Michael Griffin
General Services Administration

Michelle Hoffman
United States Citizenship and Immigration Services

Aaron Lewis
Federal Protective Service

Kevin McCombs
Environmental Protection Agency

Rachel Russell
Federal Deposit Insurance Corporation

Renee Speare
Internal Revenue Service

Cybersecurity and Infrastructure Security Agency
Interagency Security Committee Support Staff

Daryle Hernandez
Branch Chief

Tarvis Bonner
Management and Program Analyst

Robert Chaiet
Technical Editor

Scott Dunford
Senior Security Specialist

Anthony Evernham
Regional Advisor

Harrison Heller
Operations Research Analyst