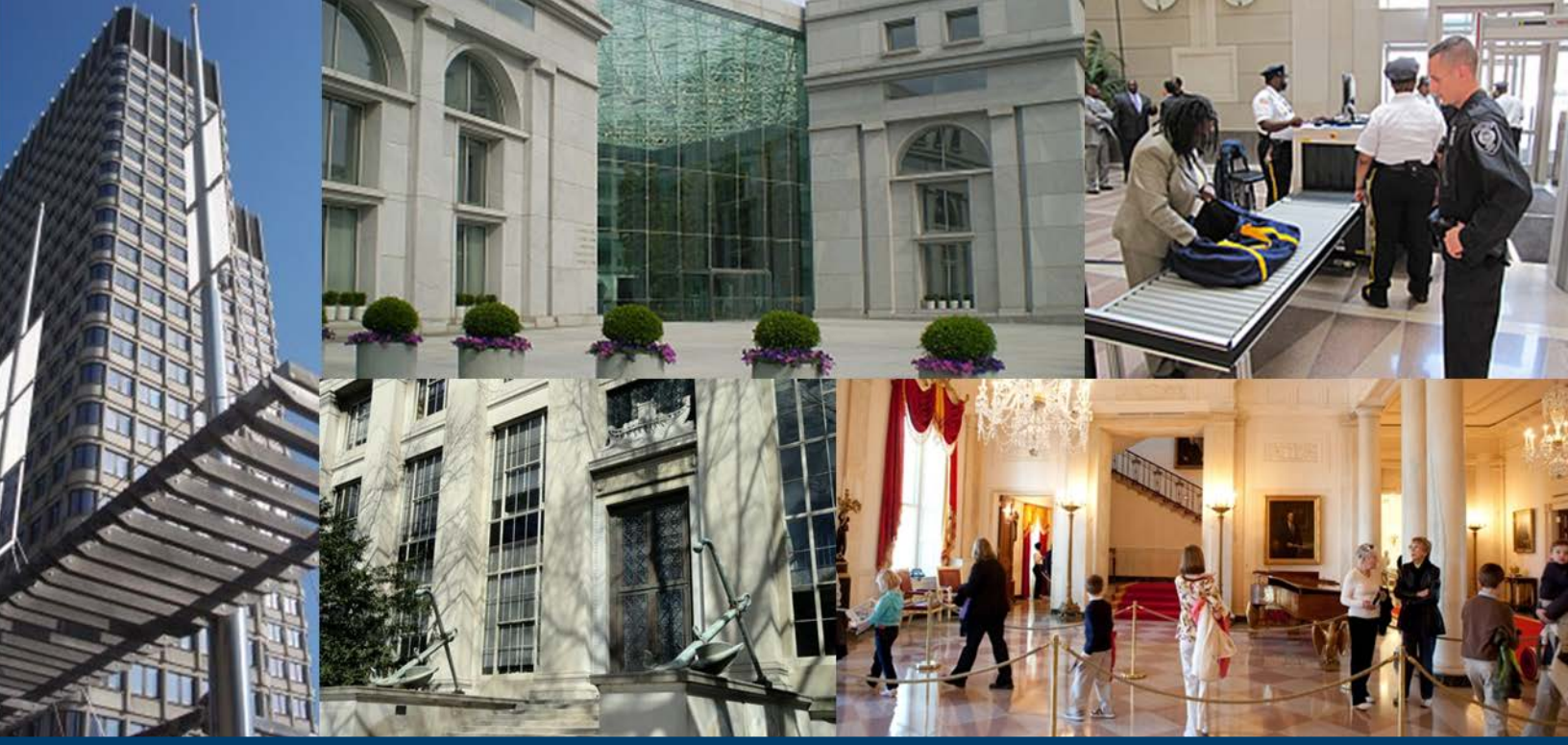


Facility Security Plan:
An Interagency Security Committee Guide

February 2015
1st Edition

Interagency
Security
Committee

This page left intentionally blank.

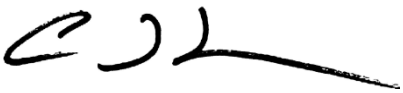
Message from the Interagency Security Committee Executive Director

One of the Department of Homeland Security's (DHS) priorities is the protection of Federal employees and private citizens who work within and visit U.S. Government-owned or leased facilities. The Interagency Security Committee (ISC), chaired by DHS, consists of 54 Federal departments and agencies and has as its mission the development of security standards and best practices for nonmilitary Federal facilities in the United States.

As Executive Director of the ISC, I am pleased to introduce the new ISC document titled Facility Security Plan: An Interagency Security Committee Guide (Guide). This ISC Guide aims to provide guidance for organizations in formulating and ultimately implementing an operable and effective Facility Security Plan (FSP). A Facility Security Plan is a critical component of an effective security program. The guidelines contained in this document are based on recognized industry best practices and provide broad recommendations for the protection of Federal facilities and Federal employees, contractors, and visitors within them.

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

This standard represents exemplary collaboration within the ISC working groups and across the entire ISC. ISC primary members approved the Guide with full concurrence on February 20, 2015 and will review and update this document as necessary.



Austin Smith

Executive Director, Interagency Security Committee

This page left intentionally blank.

Table of Contents

1 Background

On April 20, 1995, the day after the bombing of the Alfred P. Murrah Building in Oklahoma City, Oklahoma, the President directed the U.S. Department of Justice (DOJ) to assess the vulnerability of Federal facilities to terrorism and other acts of violence. On June 28, 1995, DOJ issued the *Vulnerability Assessment of Federal Facilities Report* (1995 Report) establishing government-wide facility security standards. The 1995 Report laid the foundation for all subsequent Interagency Security Committee (ISC) security standards documents.

In 2013, the ISC released *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (RMP) which includes a list of physical security criteria. The intent of the document is to provide cohesive guidance for the application of physical security countermeasures at Federal facilities. In May 2013, the ISC established the Facility Security Plan Working Group in response to concerns raised by its membership. The Working Group was tasked with preparing reference guidance for agencies to use in developing and implementing an operable and effective Facility Security Plan (FSP) as required by the physical security criteria set forth in the RMP.

2 Applicability and Scope

This document is issued pursuant to the authority granted to the Interagency Security Committee (ISC) in Executive Order (EO) 12977 as amended by Executive Order 13286. The EO directs the ISC to "…take such actions as may be necessary to enhance the quality and effectiveness of security and protection of Federal facilities." The purpose of this document is to provide guidance for organizations in formulating and ultimately implementing an operable and effective Facility Security Plan (FSP).

A Facility Security Plan is a critical component of an effective security program. The guidelines contained in this document are based on recognized industry best practices and provide broad recommendations for the protection of Federal facilities and Federal employees, contractors, and visitors within them. *Facility Security Plan: An Interagency Security Committee Guide* identifies and defines the basic guidelines and procedures used in establishing and implementing an FSP. This document is generally applicable to all buildings and facilities in the United States occupied by Federal employees, including:

- Buildings and facilities owned or leased by the Federal government;
- Federally leased rooms or suites within privately owned buildings;
- Stand-alone Federal facilities;
- Federal campuses; and
- Individual facilities on Federal campuses and special-use facilities where appropriate.

This document is intended to provide the initial guidance to be used by all agencies and facilities. When developing an FSP, departments and agencies may make the necessary adjustments to the basic guidelines and procedures presented to meet specific requirements or needs. Regardless of the FSP developed by an agency, it should have mechanisms in place to validate the plan's effectiveness and manage its maintenance.

This guidance may be used to assist Federal agencies in selecting, implementing, and evaluating appropriate protective measures and practices against identifiable security risks and threats; and to implement appropriate responses and countermeasures. When utilizing this guidance, an agency may choose to consider all or part of its overall facility security strategy. This document is not meant to supersede agency policies and funding guidelines, or impose any undue burdens on an agency.

3 Document Control

3.1 Identification

The document can be titled as the “Facility Security Plan” (FSP) or similar title as required by individual agency policy.

3.2 Storage and Distribution

At a minimum, the FSP should be stored in an electronic format in a central location for ease of access. The Designated Official (DO) and other emergency management personnel (i.e. security organizations, facility managers, etc.) must have access to the document 24 hours a day.

3.3 Retention

Current copies of the Facility Security Plan should be retained for three years or until superseded. Where there are conflicts, retention periods outlined in agency-specific requirements for storage, retention, disposition, and protection of FSPs will supersede all other guidelines.

3.4 Disposition

The plan should be discarded in accordance with agency-specific policies for destruction, based on the overall classification of the document.

3.5 Protection and Classification

At a minimum, protect the FSP as “For Official Use Only” (FOUO) or in accordance with agency-specific classification guidelines. Consideration should be given to the sensitivity of a customized FSP developed by individual agencies and departments (i.e., floor plans, specific facility information, etc.) and how this information should be protected. Plans including National Security Information (classified information) shall be classified in accordance with applicable classification standards and access to the document shall be restricted to appropriately cleared personnel with a valid need-to-know.

4 Roles and Responsibilities for Plan Development

4.1 Facility Security Committee

The Facility Security Committee (FSC) is the committee responsible for addressing facility-specific security issues and approving the implementation of protective measures and practices. At facilities where an FSC is required in accordance with Interagency Security Committee (ISC) standards, the Facility Security Plan should be submitted for review and approval prior to implementation. Additional guidance for FSC operations can be found in Appendix D of the *Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (RMP).

4.2 Designated Official

The Designated Official (DO) is the highest ranking official of the primary tenant agency of a Federal facility, or a designee as determined by individual agency policy. Alternatively, a designee may be selected by mutual agreement of tenant agency officials. The DO should be the final decision authority on any issues regarding the FSP.

4.3 Security Organization

The Security Organization (SO) is the government agency or internal agency component responsible for physical security at a specific facility. The SO also has the following responsibilities:

- Advise the FSC;
- Perform the Facility Security Level (FSL) assessment and present it to the FSC for review and approval;
- Prepare, present, and distribute a Facility Security Assessment (FSA) in accordance with the time intervals established by the ISC based on the FSL;
- Evaluate the facility to determine whether the baseline level of protection (LOP) is adequate or if a customized LOP is necessary;
- Present written plans for proposed countermeasures identifying how it will mitigate the risks associated with specific, credible threats;
- Present written operating procedures for countermeasures;
- Present written cost impact for proposed countermeasures; and
- Provide technical assistance and guidance to the FSC as appropriate.

4.4 Organizational Director of Security/Chief Security Officer

Security managers at the headquarters level are responsible for the effective implementation of security policies, programs, directives, and training within their organization. These managers should ensure there are policies and procedures in place to draft and implement organization-wide and/or site-specific Facility Security Plans.

4.5 Tenant Security Representative

The Tenant Security Representative is an individual appointed by their respective agency and is responsible for implementation and administration of day-to-day security operations (including the FSP) at a specific site or facility. Depending on the facility or campus size, more than one representative may be necessary.

4.6 Tenant Managers/Supervisors

Tenant managers and supervisors are persons with supervisory responsibility of facility occupants. Tenant managers/supervisors should:

- Assist, as needed, in the implementation of security policies and programs, and
- Ensure facility occupants are aware of site-specific security and access control procedures, operational security protocols, and provide training as needed to meet this requirement.

4.7 Facility Occupant

A facility occupant is any person permanently or regularly assigned to the facility and displays the required identification badge/pass for access. The Facility Security Committee establishes thresholds for determining who qualifies for "occupant" status. All facility occupants should become familiar with their responsibilities within the FSP.

4.8 Financial Authority

The financial authority is an organizational element, usually at the headquarters level, responsible for finance and budget decisions. Organizations should obtain guidance from their respective financial authority on issues such as:

- Identifying available funding sources, and
- Coordinating funding documents to ensure mitigation of site-specific vulnerabilities or implementation of threat-based protective measures.

4.9 Chief Information Officer

The Chief Information Officer (CIO) is the person responsible for the management, implementation, and usability of information and computer technologies. Tenant CIO representatives can provide technical reviews when considering implementation or modification of security measures that require use of an information technology system (e.g., physical access control system [PACS] and closed circuit television [CCTV]).

5 Plan Development

5.1 Risk Management Process

Implementing an effective Facility Security Plan (FSP) requires an understanding of events that could present a threat to personnel, operations, and information. Assessing and categorizing the consequences of these events is the basic function of a risk management process. Once risks to a facility are accurately assessed, the Facility Security Committee (FSC) can determine whether countermeasures in place are adequate to address or mitigate those risks or if additional procedural, programmatic, or physical security countermeasures must be implemented.

5.1.1 Process

Agencies may utilize any agency-approved risk management methodology to perform the risk assessment. The methodology used should adhere to the fundamental principles of a sound risk management methodology and be:

- Credible and assess the threat, vulnerability, and consequences of specific acts;
- Reproducible and produce similar or identical results when applied by various security professionals; and
- Defensible and provide sufficient justification for deviation from the baseline.

The methodology should also develop actions to reduce risk to an acceptable level and incorporate the Interagency Security Committee standard for identifying the necessary level of protection (LOP) to mitigate security risks. The ISC Risk Management Process (RMP) presents a process that corresponds directly to the ISC Physical Security Criteria and provides a step-by-step method to provide the FSC with an assessment of key security risks, necessary measures (in accordance with applicable threat events), and options that meet ISC standards. The following sub-sections (5.1.1.1 through 5.1.1.4) outline key elements of this process.

5.1.1.1 Threat Assessment

A threat assessment is the process of identifying or evaluating entities, actions, or occurrences (natural or man-made) that possess or indicate the potential to harm or destroy government assets.[1] A threat assessment considers the full spectrum of threats (i.e., natural, criminal, terrorist, accidental, etc.) for a given facility/location. Threat data can be derived from various resources including security organizations, intelligence community reports and assessments, as well as state and local authorities. The ISC publishes the *Design-Basis Threat Report* (DBT) used to identify a broad range of threats to Federal facilities and is updated regularly based on threat trends and data provided. This report can be utilized in conjunction with other threat assessment and agency/site-specific data, or used to determine a baseline threat if timely data and intelligence resources are not readily available.

There are a variety of threats and resources to consider when conducting a threat assessment. For natural hazards, historical data and future trend analysis concerning frequency of occurrence for given natural disasters such as tornadoes, hurricanes, floods, fires, or earthquakes can be used to determine the likelihood of the given threat. For criminal threats, the crime rates in the surrounding area provide a good indicator of the type of criminal activity that may put the

[1] As defined in the DHS Risk Lexicon

facility at risk. In addition, the type of assets and/or activities housed in the facility may also increase the target attractiveness in the eyes of an aggressor. The type of assets and/or activities at the facility will also relate directly to the likelihood of various types of accidents. For example, a facility using heavy industrial machinery will be at higher risk for serious or life-threatening job-related accidents than a typical office building. For terrorist threats, the symbolic value of the facility as a target is a primary consideration. In addition, the type of terrorist act may vary based on the potential adversary and the method of attack most likely to be successful for a given scenario.

5.1.1.2 Consequence (Criticality) Assessment

A consequence assessment is the process of identifying or evaluating the potential or actual effects of an event, incident, or occurrence.[2] Determining the relative importance to the tenant's mission provides the security manager with an understanding of how to develop an effective protection strategy. The ISC process incorporates a consequence assessment within the Facility Security Level (FSL) determination process by evaluating tenant data such as population, square footage, mission-related information, etc. This is then adjusted according to the impartial, documented, and defensible assessment to address the occurrence of a specific undesirable event and the tenant agency's ability to continue its mission should an event occur. The results of a consequence assessment can also be used to inform the prioritization of resources.

5.1.1.3 Vulnerability Assessment

Once credible threats are identified, a vulnerability assessment must be performed. A vulnerability assessment is the process of identifying physical features or operational attributes that may render an entity, asset, system, network, or geographic area susceptible or exposed to hazards.[3] Existing countermeasures must be compared to those stipulated by the baseline LOP, given the Facility Security Level, to determine if deficiencies exist. The lack of appropriate and/or effective countermeasures would equate to vulnerability. Site-specific vulnerability assessment data must be protected in accordance with appropriate agency guidance.

5.1.1.4 Risk Assessment

After the above data is considered, a risk assessment can be conducted. Assessing risk is the process of collecting information and assigning values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.[4] To assess risk effectively, information that is timely, reliable, and actionable regarding threats, vulnerabilities, and consequences is needed. Factors such as the likelihood of an undesirable event and the consequence(s) of the event's occurrence can then be quantified. The method of determining and quantifying risk is dictated by the organization performing the assessment, usually a security organization.

The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard quantifies risk from Level I (Low Risk) to Level V (Very High Risk). The risk

[2] As defined in the DHS Risk Lexicon

[3] As defined in the DHS Risk Lexicon

[4] As defined in the DHS Risk Lexicon

assessment should, as much as possible, conform to ISC standards. For example, the assessment should identify whether the facility meets the ISC countermeasures criteria or documents the risk management strategy used to mitigate any deficiencies to achieve the necessary level of protection. The assessment should incorporate some type of documentation acknowledging the risks associated with the implementation of countermeasures that do not achieve the necessary LOP. Organizations must periodically re-assess at predetermined intervals according to the established FSL, or as changes occur to threat, vulnerability, or consequence factors.

5.2 Elements of a Facility Security Plan

The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard is the key starting point for the development of a Facility Security Plan. Once the RMP is applied, other critical elements can be added to make the plan a more robust document. The elements listed in this section are recommendations that should be considered when developing an FSP. Additional items that are not included in this document may be included in the plan based on the needs of the facility or tenant organizations. The level of detail to which the plan is written may vary based on the nature of the facility (e.g., Level I facilities may have an abbreviated document). The Facility Security Committee will make final determinations of the content of the facility's final, comprehensive plan. A sample plan template is provided in Appendix A.

5.2.1 Facility Profile

The facility profile should provide a description of the facility including the following:

- Type of facility (e.g., single or multi-story, campus, mixed-use, etc.);
- Population (e.g., single or multi-tenant, Federal and/or non-Federal, child care center, visitors, etc.);
- Mission and critical functions conducted at the facility (e.g., administration, operations center, classified information, continuity of operations [COOP] site, etc.);
- Utilities (e.g., power, water, gas, communications, etc.); and
- The most current facility diagrams, construction documents and specifications.

5.2.2 Roles and Responsibilities

Identify facility-specific positions and explain roles and responsibilities for security-related tasks. Include who is responsible for preparing and approving the plan. Also, include contacts for all first-responder and/or support organizations responsible for securing the facility (i.e., local law enforcement, security organization(s), and building management), and requirements based on the Occupant Emergency Program or Plan(s) (OEP), and applicable memoranda of understanding (MOU)/memoranda of agreement (MOA).

5.2.3 Risk Management Strategy

Utilizing information from the RMP, outline and prioritize threats to the facility, tenant agencies, and/or operations; and prepare an overview of the strategies used to mitigate them. Explain any risks accepted as part of the risk management process and any possible consequences.

5.2.4 Security Countermeasures

Identify and describe in detail all current and planned security countermeasures (including floor plans when available) to address all identified threats. The list can be derived from the ISC RMP or other similar agency-specific criteria. As much as possible, ensure countermeasures are scalable to allow for an increased or decreased security posture as the threat evolves (i.e., upgrades in the National Terrorism Advisory System/Force Protection Conditions, etc.).

5.2.5 Maintenance, Repair, and Testing Procedures

Describe requirements in detail for operator and manufacturer maintenance/repair of security countermeasures. Outline a testing schedule performed by the security manager at Level IV and V facilities.

5.2.6 Incident Response Management and Procedures

Describe in detail the procedures for responding to security incidents and emergencies. Details should include:

- *Reporting*: How do employees report incidents? Do they call an internal operations center or 911?
- *Notification*: How are first responders and facility occupants notified an incident is taking place or has occurred? How are changes in the facility's security posture communicated?
- *Response*: Who should respond and how should they respond? What is the chain of command?
    - Law Enforcement/Security Organizations
    - Fire Department
    - Medical
    - Alarm Response
- *Recovery*: Once incident response is terminated, what is the process to resume normal operations?
- *Documentation*: How is an incident documented? Where is the information maintained? Who has authorized access to that information?

5.2.7 Facility Specific Policies

Include any unique requirements to address issues such as landlord/tenant agreements or special missions (i.e., classified areas, operations centers, network control centers, child care centers, etc.).

5.2.8 Special Events

Protocols should be included to manage requirements for special events, such as temporary increases in population, traffic/parking control, and the media.

5.2.9 Information Security

Address issues related to the protection of sensitive but unclassified information as well as classified information, if applicable.

5.2.10 Cyber Security

Collaborate with all tenant Chief Information Officers to develop a plan for the physical and logical protection of information technology systems and equipment associated with security countermeasures.

5.2.11 Government Property

Include procedures to control pilferage, destruction, and disposal of government-owned property.

5.2.12 Training and Exercising the Plan

Develop a strategy or program to train personnel and exercise all aspects of the FSP. Exercises simulate realistic, fluid situations where critical decision-making tools are applied and occupants are familiarized with the Facility Security Plan. Exercises help to broaden understanding of the plan and identify areas for improvement. These exercises can be table-top, drills, or full-scale exercises and should be coordinated with Occupant Emergency Program or Plan (OEP) requirements.

5.2.13 Program Review

Provide program review guidelines within the plan. It cannot be overstated that the FSP and security program are ultimately the responsibility of senior leadership and/or the Facility Security Committee. These officials have the authority and responsibility to alter or add to the program as deemed necessary to accommodate tenant needs and operational constraints. Program reviews should be conducted at least annually.

5.2.14 Resource Support

Outline fiscal instructions on how funding support is gained to sustain security operations from pre-incident to post-incident.

6 Training and Exercises

6.1 Training

All occupants should be familiar with and trained on the Facility Security Plan (FSP). Any personnel holding key positions, as identified in the FSP, should be trained in his/her assigned duties. Organizational security directors, with assistance from Tenant Security Representatives, are responsible for this training as indicated in section 4.4. The security organization associated with the facility and any assigned security specialists may also provide assistance, such as preparing a training plan and recommending training materials.

6.2 Exercises

Exercises are an effective and cost-efficient method of validating FSPs, identifying areas for improvement, and soliciting feedback from those who will be executing security plans.

- Exercises may be:[5]
    - Discussion-Based (e.g., seminars, workshops, table-top, etc.); or
    - Operations-Based (e.g., drills, functional, full scale, etc.); or
    - Any combination of the two.
- Exercises may be facility-specific or part of a cooperative exercise program.
- All aspects of the FSP should be exercised including testing communication and notification procedures, elements of coordination, resource availability, and response.
- At a minimum, the FSP should be exercised annually with participation at all levels from the security organization to facility occupants.

6.3 Occupant Emergency Plan Exercise Coordination

All aspects of the Facility Security Plan should be matched against the current Occupant Emergency Program or Plan(s) (OEP) for the facility. This will ensure that all pertinent security and emergency items are included. A review of the FSP and OEP should also ensure that the Facility Security Committee, Tenant Security Representatives, and other key personnel with assigned duties under the FSP and/or OEP are not overly tasked or have responsibilities that require them to be at two places at the same time. Close coordination between the developers of the OEP and FSP is essential to ensure the both plans complement each other.

[5] Homeland Security Exercise and Evaluation Program (HSEEP), April 2013

7 Plan Maintenance

The Facility Security Plan should be reviewed at a minimum annually, or as required when significant changes to the tenant mission, facility population, site composition, or threat occur. Review exercise documentation to ensure lessons learned are addressed and incorporated.

8 References and Resources

1. *The Risk Management Process: An Interagency Security Committee Standard*
2. *The Risk Management Process: An Interagency Security Committee Standard, Appendix A: Design Basis Threat Report* (FOUO)
3. *The Risk Management Process: An Interagency Security Committee Standard, Appendix B: Countermeasures* (FOUO)
4. *The Risk Management Process: An Interagency Security Committee Standard, Appendix D: How to Conduct a Facility Security Committee*
5. *Best Practices for Mail Handling Processes: A Guide for the Public and Private Sectors*
6. *Federal Protective Service Facility Security Assessment Manual 15.8.1.1,* March 2014
7. *Homeland Security Exercise and Evaluation Program* (HSEEP), April 2013
8. *DHS Risk Lexicon,* September 2008

9 Interagency Security Committee Participants

Interagency Security Committee
Bernard Holt
Deputy Executive Director

Interagency Security Committee Representative
Anthony Evernham

Working Group Chair
Marcus James
Executive Office of the President, Office of Administration

Working Group Participants
Dwayne Deaver
Department of Justice

Glen Legus
United States Marshals Service

Brett Knutson
United States Marshals Service

Dave Lively
Department of State

Joseph Cassone
Pentagon Force Protection Agency

Shawn Frensley
Pentagon Force Protection Agency

Raymond Gauvin
Federal Protective Service

List of Abbreviations/Acronyms/Initializations

TERM	DEFINITION
CCTV	Closed Circuit Television
CIO	Chief Information Officer
COOP	Continuity of Operations
DBT	Design Basis Threat
DHS	Department of Homeland Security
DO	Designated Official
DOJ	Department of Justice
EO	Executive Order
FOUO	For Official Use Only
FSA	Facility Security Assessment
FSC	Facility Security Committee
FSL	Facility Security Level
FSP	Facility Security Plan
HSEEP	Homeland Security Exercise and Evaluation Program
ISC	Interagency Security Committee
LOP	Level of Protection
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
OEP	Occupant Emergency Program or Plan
PACS	Physical Access Control System
RMP	*The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*
SO	Security Organization

Glossary of Terms

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 located on site and typically sharing some aspects of the environment, such as parking, courtyards, private vehicle access roads, or gates and entrances to connected buildings. A campus also may be referred to as a "Federal center" or "complex".

Consequence: The level, duration, and nature of the loss resulting from an undesirable event.

Countermeasure: A specific action taken to mitigate an undesirable event.

Criticality: Any facility, equipment, service, or resource considered essential to operations and warranting measures and precautions to ensure their continued efficient operation; protection from disruption, degradation, or disruption; and timely restoration.

Exercise: An instrument to train for, assess, practice, and improve performance in prevention, protection, mitigation, response, and recovery capabilities in a risk-free environment.

Exterior: Area between the building envelope and the site perimeter.

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 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.

Facility Security Committee: A committee that is responsible for addressing facility-specific security issues and approving the implementation of security measures and practices. The Facility Security Committee (FSC) consists of representatives of all Federal tenants in the facility, the security organization, and the owning or leasing department or agency. In the case of new construction or pending lease actions, the FSC will also include the project team and the planned tenant(s). The FSC was formerly known as the Building Security Committee "BSC."

Facility Security Level: A categorization based on the analysis of several security-related facility factors, which serves as the basis for the implementation of physical security measures specified in ISC standards.

Facility Security Plan: A plan that provides direction to key personnel on the security management and policies of a building or facility.

Federal Departments or Agencies: Those executive departments enumerated in 5 U.S.C. 101 and DHS, independent establishments as defined by 5 U.S.C. 104(1), Government corporations as defined by 5 U.S.C. 103(1), and the U.S Postal Service.

Federal Facilities: Leased and owned facilities in the United States (inclusive of its territories) occupied by executive branch Federal employees for nonmilitary activities.

Government-Owned: A facility owned by the United States and under the custody and control of a Federal department of agency.

Interior: Space inside a building controlled or occupied by the Government.

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, Moderate, 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.

National Terrorism Advisory System (NTAS): This system effectively communicates information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector. These alerts will include a clear statement that there is an imminent threat (warning of a credible, specific, and impending terrorist threat against the United States) or elevated threat (warns of a credible terrorist threat against the United States). Using available information, the alerts will provide a concise summary of the potential threat, information about actions being taken to ensure public safety, and recommend steps that individuals, communities, businesses and government can take to help prevent, mitigate or respond to the threat.

Occupant: Any person who is permanently or regularly assigned to the government facility and displays the required identification badge/pass for access. The facility security committee establishes the thresholds for the determining who qualifies for "occupant" status.

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 Report: The documentation of the risk assessment process to include the identification of undesirable events, consequences, and vulnerabilities and the recommendation of specific security measures commensurate with the level of risk.

Risk Management: A comprehensive approach to allocating resources for the protection of a facility, assets, and occupants to achieve an acceptable level of risk. Risk management decisions are based on the application of risk assessment, risk mitigation, and – when necessary – risk acceptance.

Security Organization: The Government agency or an internal agency component responsible for physical security for the specific facility.

Site: The physical land area controlled by the Government by right of ownership, leasehold interest, permit, or other legal conveyance, upon which a facility is placed.

Site Entry: A vehicle or pedestrian access point into, or exit from, the site.

Site Perimeter: The outermost boundary of a site. The site perimeter is often delineated by the property line.

Special-Use Facilities: An entire facility or space within a facility itself that contains environments, equipment, or data normally not housed in a typical office, storage, or public access facilities. Examples of special-use facilities include, but are not limited to, high-security laboratories, hospitals, aircraft and spacecraft hangars, or unique storage facilities designed specifically for such things as chemicals and explosives.

Suite: One or more contiguous rooms occupied as a unit.

Threat: The intention and capability of an adversary to initiate an undesirable event.

Undesirable Event: An incident that has an adverse impact on the operation of the facility or mission of the agency.

Visitor: Any person entering a government facility that does not possess the required identification badge or pass for access or who otherwise does not qualify as an "occupant".

Vulnerability: A weakness in the design or operation of a facility that an adversary can exploit.

Appendix A: Facility Security Plan Template

The following pages contain a basic Facility Security Plan template that meets the requirements outlined in Appendix B of *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*.

[*Insert Agency/Facility Name*]

Facility Security Plan

Date: [*For tracking updates*]

1. Introduction

This Facility Security Plan (FSP) outlines the procedures and measures employed by [*agency/facility name*] to address security needs at various risk levels and respond effectively during instances when undesirable events occur. In addition, this document contains a wealth of information unique to this facility and its occupants that should be used in conjunction with the Occupant Emergency Plan (OEP) [and/*or other applicable plan(s)*].

2. Facility Profile

[*Provide a description of the facility including the physical address for first responders.*]

Facility Type:

- Mixed-Tenant: A facility that includes one Federal tenant as well as non-Federal tenants, including commercial and State/local government tenants.
- Mixed-Multi-Tenant: A facility that includes tenants from multiple Federal departments and agencies as well as one or more non-Federal tenants.
- Multi-Tenant: A facility that includes tenants from multiple Federal departments and agencies but no non-Federal tenants.
- Single-Tenant: A facility that only includes one Federal tenant or multiple components of the same Federal department or agency that fall under one "umbrella" for security purposes.
- Special-Use: An entire facility or space within a facility that contains environments, equipment, or data normally not housed in typical office, storage, or public access facilities. Examples of special-use facilities include, but are not limited to, high-security laboratories, hospitals, aircraft and spacecraft hangers, or unique storage facilities designed specifically for such things as chemicals and explosives.

Construction: Describe the physical construction of the facility. Attach floor plans or describe location where floor plans are located.

Facility Security Level: A categorization based on the analysis of several security-related facility factors, which then serves as the basis for the implementation of certain protective security measures specified in other ISC standards.

Population: How many employees/contractors/daily visitors to the facility? List all tenant agencies and points of contact for each.

General functions performed at the facility: What functions are performed at this facility (e.g., administration, operations center, child care, etc.)?

Essential functions: List essential government functions (e.g., provide vital services, exercise civil authority, maintain the safety and well-being of the general populace, sustain the industrial/economic base in an emergency, etc.)

Utilities: List all utilities used at the facility (include provider's name and contact information) and details of how they enter and are distributed throughout the facility. Identify procedures to mitigate the effects due to service interruption or contamination.

Sample Description Spreadsheet:

General Facility Description:								
Lessor's Name:				Contact Number:				
Lessor's Address:								
Lessor's City:				State:		Zip:		
Building Management Name:								
Building Management POC:			Title:					
Contact Number:			e-mail address:					
Date Building was constructed:		Total Square Footage:			Lease Footage:			
Total Number of Floors above Ground:			Total Number of floors below Ground:					
Total Number of Occupants in Bldg.:			Total Number of Daily Visitors for Bldg.:					
Total Number of Occupants in Component's Space:			Total Number of Daily Visitors for Space:					
General Hours of Operation for the Building:			Notes:					
General Hours of Operation for the Component Space:			Notes:					
Distance in feet from the building to the nearest public street:								
Distance in feet from the building to the nearest public on-street parking:								
Distance in yards from the building to the nearest public Parking Lot:								
Facility Structure Information: i.e., composition of walls, slabs, roof (brick, block, concrete [pre-cast or poured]), medal panels, glass exterior, metal framing or reinforced concrete.								
Building Facade: i.e., composition of walls (brick, block, concrete [pre-cast or poured]), metal panels, glass exterior, metal framing or reinforced concrete.								

3. Roles and Responsibilities

List key positions with responsibility to execute this plan to include facility occupants and public affairs personnel. Also, include contact information for each key individual.

Security Organization: The government agency or an internal agency component responsible for physical security at the facility (e.g., Federal Protective Service, United States Marshals Service, U.S. Environmental Protection Agency's Security Management Division).

4. Risk Management Strategy

Utilizing information derived from the Risk Management Process (RMP), outline and prioritize threats to the facility, tenant agencies, and/or operations; and develop an overview of the

strategies used to mitigate them. Explain any risks that have been accepted as part of the risk management process and any potential consequences.

5. Security Countermeasures

Describe in detail all current and planned countermeasures (both physical and procedural) to address all identified threats. Consider scalable actions to allow for increases and decreases in security posture as the threat level changes.

Security of Facility Exterior Areas (public areas outside the building):

A. Security at all pedestrian entrances:

   1. Consideration should be given to reducing the number of public entrances if there are too many to ensure security. This may require approval from the building manager.

   2. Consider the use of metal detectors and X-ray machines at pedestrian/public entrances.

   3. Security screening may be done at employee entrances; however, because not all facilities have restricted entrances for employees, the merits of this precaution need to be evaluated for each facility.

B. Security at vehicle entrances:

   1. Describe the security available for employee vehicles parked inside and outside the building.

   2. Numbers, not names or agency identification, should be used to indicate reserved parking spaces.

   3. Security officers and/or security devices that may be used at vehicle entrances.

C. The overall physical security of the building should be considered, especially windows, doors, utility grates, and air intakes at or near ground level.

D. Appropriate security responses to disturbances in this area should be developed.

Security of Facility Interior Areas - Public areas inside the building (excluding Critical Areas):

A. Location, level, and adequacy of security provided in this area;

B. Access control procedures; and

C. Mail handling procedures.

Security of Critical/Restricted Areas (Limited Access or Exclusionary Zones):

A. Location, level, and adequacy of security provided in this area; and

B. Access control procedures.

6. Countermeasure Maintenance, Repair, and Testing

Describe in detail requirements for operator and manufacturer maintenance and repair of security countermeasures.

Outline testing schedule performed by the security manager at level IV and V facilities.

7. Incident Response Management

Describe procedures for responding to security incidents and emergencies.

A. Reporting: How do employees report incidents? Do they call an internal operations center or 911?

B. Notification: How are first responders and the facility occupants notified an incident has occurred or is in progress?

C. Response: Who should respond and how should they respond? What is the Chain of Command?

- Law Enforcement/Security Organizations
- Fire Department
- Medical
- Alarm Response

D. Recovery: Once an incident response is terminated, what is the process to resume normal operations? Consider employee, facility, and process recovery procedures.

E. Documentation: How is an incident documented, where is the information maintained, and who has authorized access to it?

8. Facility-Specific Policies

Specify any unique requirements to address issues such as landlord/tenant agreements or special missions (i.e., classified areas, operations centers, and network control centers).

9. Special Events

Additional protocols should be included to address requirements for special events such as temporary increases in population, traffic/parking control, and the media.

10. Information Security

Address issues related to the protection of sensitive but unclassified information (also known as controlled unclassified information) as well as classified information, if applicable.

11. Cyber Security

Collaborate with all tenant Chief Information Officers (CIO) or office representatives to develop a plan to address the physical and logical protection of information technology systems and equipment associated with security countermeasures.

12. Government Property

Procedures to control pilferage, destruction, and disposal of government owned property.

13. Training

Describe plans and procedures for training employees and managers and coordination with first responders for execution of this plan.

14. Exercises

Describe the participants, type, frequency, and how exercises will be executed and documented. Exercises can be coordinated and conducted in conjunction with OEP requirements.

15. Plan Review

Outline program review and approval guidelines.

16. Resource Support

Fiscal instructions on how funding support is gained to sustain security operations from pre-incident to post-incident.

Approved by:

[*Signature of Approving Authority*]

NAME
TITLE