



Facility Security Committees

An Interagency Security Committee Standard

January 1, 2012

2nd Edition



Authority and Responsibility: This Interim Standard is developed under the authority of Executive Order 12977 (as amended). It provides procedures for Facility Security Committees (FSCs) to use when presented with security issues that affect an entire nonmilitary Federal facility.

The document was developed after extensive interagency coordination, and Interagency Security Committee members have agreed to comply with this standard to the extent permitted by law and subject to the availability of appropriations. This Interim Standard is intended to improve the internal management of facility security and is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its agencies, its officers, or its employees.



Homeland
Security

Preface



Todd M. Keil
Assistant Secretary for
Infrastructure Protection

As Chair of the Interagency Security Committee (ISC), I am pleased to re-issue the interim ISC Standard titled, *Facility Security Committees: An Interagency Security Committee Standard* (the Standard). Starting on January 1, 2012, the pilot will expand and apply to all facilities with a Facility Security Level (FSL) of I, II, III, or IV. Building on the first six months of the 12-month validation period, and based on recommendations from both the Steering and Standards Subcommittees, the expanded testing at all levels will provide a more complete picture of the Standard's effectiveness and utilization, allowing user input to inform the final standard.

One of our top national priorities is the protection of all Federal employees and private citizens who work within and visit U.S. Government-owned or leased facilities. Composed of 50 Federal departments and agencies, the ISC's primary mission is to craft security standards and best practices for non-military Federal facilities in the United States.

The Interim Standard establishes procedures for a Facility Security Committee (FSC) to use when addressing security issues that affect its respective facility. The Interim Standard specifically defines the organizational structure, operations, accountability, and the decisionmaking authority of FSCs. Each executive agency and department shall comply with this Interim Standard.

This Interim Standard supersedes all previous ISC guidance on establishing FSCs, as well as the 1995 Department of Justice report, *Vulnerability Assessment of Federal Facilities*. Consistent with Executive Order 12977 (October 19, 1995), this Interim Standard applies to all buildings and facilities in the United States occupied by Federal employees for non-military activities. These include: presently owned, to be purchased, or leased facilities; stand-alone facilities; Federal campuses; and where appropriate, individual facilities on Federal campuses and special-use facilities.

The Interim Standard is a significant milestone and represents extraordinary collaboration across the ISC and among the ISC Working Group. With full concurrence, ISC primary members approved the Interim Standard on March 24, 2011, and will review and update it by July 2012.

A handwritten signature in blue ink that reads "Todd M. Keil".

Todd M. Keil
Assistant Secretary for Infrastructure Protection

Table of Contents

1. Purpose.....	1
2. Background.....	1
3. Applicability and Scope.....	1
4. How to Apply This Standard	2
4.1. Risk Mitigation or Acceptance	3
4.2. Risk Acceptance	3
4.3. Financial Commitment	4
4.4. Financial Authority	4
4.5. Selecting a Security Organization	4
4.6. Interagency Security Committee Training.....	4
5. Facility Security Committee Procedures and Duties	4
5.1. Voting Procedures.....	5
5.1.1. Decision Item Approval	6
5.1.2. Decision Item Disapproval.....	7
5.2. Facility Security Committee Chairperson.....	7
5.3. Facility Security Committee Members	8
5.4. Owning or Leasing Authority	8
5.5. Security Organization	8
5.6. Federal Department and Agency Headquarters	9
6. Facility Security Committee Operations.....	9
6.1. Facility Security Committee Business Process.....	9
6.1.1. Meeting Agenda and Discussions.....	12
6.1.2. Security Organization Guidance	12
6.1.3. Decision Point: Is a vote required by the Facility Security Committee?.....	12
6.1.4. Decision Point: Does the vote have a funding impact?	12
6.1.5. Decision Point: Do Facility Security Committee members desire guidance from organizational authority?.....	12
6.2. Facility Security Committee Funding Process.....	12
6.2.1. Security Organization Presents Countermeasures Implementation and Funding Plan to the Facility Security Committee.....	16
6.2.2. Facility Security Committee Members Request Guidance from their Respective Funding Authority	16
6.2.3. Decision Point: Did the Facility Security Committee vote to approve the proposed security proposal?.....	16
6.2.4. Decision Point: Has the security organization considered alternatives?	16
6.2.5. Decision Point: Does the Facility Security Committee desire an enhanced decision process?.....	17
6.3. Decision Process	17
6.3.1. Facility Security Committee Chairperson Invokes Decision Process.....	19
6.3.2. Decision Point: Was the review period successful?	19
6.3.3. Organizational Security Element Assistance	19
6.3.4. Decision Point: Did the organizational security element assistance resolve the issue?	19
6.3.5. Organizational Chief of Security Officer Review	19

6.3.6. Decision Point: Were the Chief Security Officers able to resolve the issue?	20
6.3.7. Organizational Chief Security Officer Briefs Executive Level Management	20
6.3.8. Executive Level Management for Each Organization Represented at the Facility Agrees on a Decision for the Facility	20
7. Funding	20
7.1. Funding for a Non-Unanimous Vote	20
7.2. Facility Security Committee Member Funding Authority	21
7.2.1. Approval of Funds	21
7.2.2. Disapproval of Funds	21
7.3. Funding Documents	21
7.4. Funding Impact to Occupant	21
7.5. Occupancy Agreement	22
8. Special-Use Facilities	22
8.1. Facility Security Committee Functions at a Special-Use Facility	22
9. Record Keeping	22
9.1. Purpose	22
9.2. Format of Records	22
9.3. Access to Records	22
Appendix A: Acronym List	24
Appendix B: Glossary of Terms	25
Appendix C: ISC Pro Rata Voting Share Calculation Tool	30
Interagency Security Committee Participants	31

Figures

Figure 1: Calculation of Pro Rata Voting Share	6
Figure 2: FSC Business Process	11
Figure 3: FSC Funding Process	15
Figure 4: Decision Process	18

1. Purpose

The *Facility Security Committees: An Interagency Security Committee Standard* (the Interim Standard) establishes procedures for a Facility Security Committee (FSC) to use when presented with security issues that affect the entire facility. This Interim Standard is issued pursuant to the authority of the Interagency Security Committee (ISC) contained in Executive Order 12977, October 19, 1995, "Interagency Security Committee," as amended by Executive Order 13286, March 5, 2003. Each executive agency and department shall comply with this Interim Standard. The Standard is applicable to all buildings and facilities in the United States occupied by Federal employees for nonmilitary activities.

2. Background

The U.S. Department of Justice (DOJ) Vulnerability Assessment of Federal Facilities dated June 28, 1995 (1995 DOJ document) called for the creation of the Interagency Security Committee (ISC). The ISC was established under Executive Order 12977 dated October 19, 1995. The ISC was created to enhance the quality and effectiveness of security and protection of buildings and facilities in the United States occupied by Federal employees.

The 1995 DOJ document directed the General Services Administration (GSA) to establish a Building Security Committee (BSC) in each facility under its control. That document provided that BSCs should evaluate and apply the appropriate minimum standards developed for each type of facility under GSA control.

Since 1995, BSCs existed without guidelines, policy, or procedures that outlined how they should function, make decisions, or resolve disputes. As a result, the BSC concept was inconsistently applied.

During the development of this document, the ISC changed the name of the BSC to FSC.

3. Applicability and Scope

The authority for Federal departments and agencies to provide security for their facilities and employees is cited in various sections of the United States Code and the Code of Federal Regulations (CFR).¹ Per their respective authority, each department or agency obtains the funds to provide security. In single tenant facilities, the Federal department or agency with funding authority is the decisionmaker for the facility's security and has the option to use these standards or other internal procedures to make security decisions. For facilities with two or more Federal tenants with funding authority, an FSC will be established to make security decisions for the facility.

¹ It is beyond the scope of this document to cite individual department and agency authorities. For more information regarding authorities the reader should contact their agency Office of General Counsel. In accordance with their respective authority, each department or agency obtains the funds to provide security.

At a minimum, the FSCs shall meet annually or as needed, as determined by the committee chairperson.

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

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

4. How to Apply This Standard

This document is intended to be used in conjunction with the following ISC documents:

- *Facility Security Level Determinations for Federal Facilities (FSL)*
- *Physical Security Criteria for Federal Facilities (PSC)*
- *The Design-Basis Threat Report (DBT)*

The FSC will work with the facility security organization and the owning or leasing authority to establish the FSL and determine the minimum standards (security countermeasures) for the facility. The PSC identifies the baseline level of protection (LOP) for a Federal facility. The DBT establishes a profile of the type, composition, and capabilities of adversaries. It is designed to correlate with the countermeasures contained in the PSC.

The facility's security organization will conduct a risk assessment of the facility to identify risk(s) and determine whether the existing LOP meets the baseline standard. The findings of the risk assessment are used to determine whether the baseline LOP is adequate or if a customized LOP is established. Any recommended countermeasures are reviewed by the FSC chairperson and the owning or leasing authority of the facility in advance of a scheduled FSC meeting. At the FSC meeting, the security organization will present the risk assessment findings, recommendations, and cost proposal for the countermeasures presented for consideration. Each FSC member votes to determine whether:

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

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

4.1. Risk Mitigation or Acceptance

In general, risk is mitigated by lowering the vulnerability to exploitation of a potential weakness in the facility security posture. A common way to improve security is by adding or increasing the countermeasures to achieve a higher LOP. Some threats or vulnerabilities can be mitigated by a combination of applying a higher level countermeasure and changing existing or adding new physical security policies or procedures. Accepting risk is generally considered or presented as something that should never be done; however, accepting risk may be the logical outcome to a rational decision process.

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

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

4.2. Risk Acceptance

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

4.3. Financial Commitment

An FSC vote to approve a countermeasure is a financial commitment by each Federal tenant that pays rent for space in the facility. Each Federal tenant is responsible for funding their prorated share of the cost of the approved countermeasure, regardless of how they voted. The prorated share of the cost is equal to the percentage of rentable square feet of space in the facility occupied by the Federal tenant. (For GSA-controlled facilities please refer to paragraph 5.1.1.)

4.4. Financial Authority

FSC members may or may not have the authority to obligate their respective organizations to a financial commitment. When funding issues are considered, each FSC representative that does not have funding authority is allowed time to obtain guidance from their respective organization. Each FSC chairperson will establish a date for a vote on a decision item, while providing a reasonable period (not to exceed 45 calendar days) for FSC representatives to obtain guidance from their headquarters element. If financial guidance is not provided to the FSC representative within this allotted time, the FSC chairperson may use the Decision Process (see page 18) or other means as determined by the FSC to reach a resolution.

4.5. Selecting a Security Organization

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

4.6. Interagency Security Committee Training

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

- IS-890a Introduction to the Interagency Security Committee
- IS-891 Facility Security Level Determinations for Federal Facilities
- IS-892 Physical Security Criteria for Federal Facilities
- IS-893 Facility Security Committees for Federal Facilities (available late 2011)

5. Facility Security Committee Procedures and Duties

Each FSC will have a chairperson. Each Federal tenant that pays rent on space they occupy in a Federal facility will have one representative with one vote on decision items before the FSC. The owning or leasing authority and security organization are members of the FSC with voting

privileges, if they pay rent on and occupy space in the Federal facility. FSCs are encouraged to include the child-care center director (as applicable) as a nonvoting member. Each Federal department or agency headquarters shall provide guidance to its FSC representative. Meeting agendas must be published, and each agenda item must be identified either as a discussion or as a decision item. If a single Federal tenant occupies a facility, they have the option to use this standard or other internal procedure to determine what security countermeasures are implemented, how funding is provided, and what risk is accepted. The PSC details other functions where the FSC is expected to make decisions and provide guidance relating to:

- 6.1.7 Determine the Highest Achievable LOP
- 6.1.10 Accept Risk
- 6.2.1 Application to New Construction
- 6.2.2 Application to Existing Federal Facilities
- 6.2.3 Modernization and Renovation
- 6.2.4 Application to Lease Solicitations
- 6.2.5 Tenant and Mission Changes in Occupied Buildings
- 6.2.6 Campus Environments
- Appendix A – Details of Security Measures

5.1. Voting Procedures

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

Each vote is weighted to the number of occupants and rentable square footage of assigned space (by percentage of total number of occupants and square footage for the building) for each Federal tenant. The weighted vote in relation to the number of occupants account for 60 percent of an individual vote, and the remaining 40 percent is in relation to the rentable square footage of assigned space for each Federal tenant (see Figure 1).

Figure 1 illustrates how weighted voting is established based on the number of occupants and 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. To disallow the joint use and vacant space, the FSC can subtract the square footage of the joint use and vacant space from the total square footage of the facility and then recalculate the pro rata voting share for each tenant. Voting to eliminate joint use/vacant space should only be done once.

[Using the United States Marshals Service (USMS) data in Figure 1 as an example, the pro rata voting share is determined by using the following formula: Divide the number of USMS occupants in the facility (88) by the total number of occupants in the facility (193); then multiply

that quotient (0.456) by .6 to calculate the “occupants” portion of the pro rata USMS voting share (0.274). Next, take the amount of square feet USMS occupies in that facility (28,491) and divide it by the amount of square feet for the entire facility (161, 542); then multiply that quotient (0.176) by .4 to calculate the “square feet” portion of the pro rata USMS voting share (0.0705). Finally, take the sum of the two products (“occupant” and “square feet”; 0.274 + 0.0705) to calculate the pro rata voting share for USMS (.34, or 34%).] The FSC Chair can make these calculations for an entire facility by using the *ISC Pro Rata Voting Share Calculation Tool* located on the ISC HSIN web site.

Calculation of Pro Rata Voting Share

Agency Tenant	Number of Occupants	Square Feet	Weighted Combined Values Occupants = 60% / Sq. Ft. = 40%	Pro Rata Voting Share
USMS	88	28,491	27.4 + 7.05 =	34%
Dept of Labor	11	13,333	3.41 + 3.30 =	7%
IRS	10	32,682	3.10 + 8.09 =	11%
DHS/FPS	6	3,600	1.86 + .89 =	3%
GSA	3	12,264	.93 + 3.03 =	4%
Judiciary	14	46,144	4.35 + 11.42 =	16%
Social Security Administration	61	25,028	18.96 + 6.19 =	25%
Total	193	161,542		100%

Figure 1: This figure illustrates each tenant’s calculated pro rata voting share. See Appendix C for instructions on how to use the ISC Pro Rata Voting Share Calculation Tool.

A quorum of 50 percent of the FSC members is required for a vote on a decision item. A decision item passes or fails with a majority of the facility’s weighted vote. If 50 percent of the FSC membership is not present for two consecutive meetings, the FSC chair may invoke the decision process to seek remedy.

5.1.1. Decision Item Approval

When an agenda decision item is approved by the FSC, this vote must be recorded in the FSC meeting minutes. If the vote approves the implementation of a security countermeasure, this vote is a financial commitment by each Federal tenant in the facility regardless of how each FSC representative voted. If a decision item is approved, all Federal tenants in the facility shall

provide their prorated share of the cost to fund the countermeasure. The FSC must also approve security countermeasures that are procedural in nature and have no funding implications.

- In a GSA-controlled facility, per the *GSA Pricing Desk Guide, 4th Edition*, a signature is not required to modify a tenant Occupancy Agreement (OA) when the FSC approves a security feature.
- The security organization and/or the owning or leasing authority must be prepared to accept funding from multiple sources and from mixed fiscal years. Funding for a project approved by the FSC is detailed in Section 7 of this document.
- If a facility owner 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. If agreement on alternative proposals cannot be reached, this acceptance of risk will be documented in the FSC meeting minutes.

5.1.2. Decision Item Disapproval

The meeting minutes must document each Federal department or agency vote to approve or disapprove a recommended countermeasure. If an agenda decision item is disapproved and the decision item would have mitigated a risk, the meeting minutes must document the chosen risk management strategy. If a countermeasure is not approved, the FSC will document the basis for the risk acceptance. The meeting minutes shall be maintained by the FSC chairperson and the security organization as an historical document for the facility. Each member of the FSC and their respective security element at the organization headquarters level shall be provided a copy of the meeting minutes that document the chosen risk management strategy.

5.2. Facility Security Committee Chairperson

The FSC chairperson is the senior representative of the primary tenant. The senior person with the primary tenant may designate a senior staff member with decisionmaking authority to serve as the FSC chairperson; however, the senior representative retains the responsibility for the FSC. Should the senior person with the primary tenant decline to serve as the FSC chairperson, the FSC members shall select a chairperson by majority vote. The FSC chairperson must be an occupant of the facility or campus and is responsible for the following:

- Setting FSC meeting agendas
- Scheduling FSC meetings
- Distributing FSC meeting minutes
- Maintaining FSC meeting records
- Maintaining training records for all FSC members
- Coordinating with outside organizations
- Assigning tasks to other FSC members for drafting plans
- Maintaining a current list of Federal tenant agency occupant status

- Maintaining a current list of Federal tenants' square footage
- Serving as the point of contact for the FSC between meetings
- Calling for votes on issues before the FSC
- Establishing deadlines (not to exceed 45 days) by which each FSC member organization must provide guidance to their FSC representative
- Casting votes for their organization

5.3. Facility Security Committee Members

FSC members shall be senior officials with decisionmaking authority for their organization. If the FSC member does not have authority to make funding decisions, the FSC member is responsible for making the appropriate request(s) to their organizational headquarters for funding authorization as well as for the following tasks:

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

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

5.4. Owning or Leasing Authority

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

- Representing organizational interests
- Attending meetings
- Providing technical information
- Assisting with vendor access to the facility when requested by the security organization
- Casting votes for their organization

5.5. Security Organization

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

- Advising the FSC
- Performing the FSL assessment
- Presenting the FSL assessment to the FSC
- Evaluating the facility to determine whether the baseline LOP is adequate, or whether a customized LOP is necessary

- Presenting a written plan for proposed countermeasures that identifies how it will mitigate the risks identified with specific credible threats
- Presenting written operating procedures for countermeasures
- Presenting written cost impact for proposed countermeasures
- Provide technical assistance and guidance to the FSC as appropriate
- Casting votes for their organization

5.6. Federal Department and Agency Headquarters

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

6. Facility Security Committee Operations

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

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

6.1. Facility Security Committee Business Process

Figure 2: FSC Business Process outlines the basic steps taken to address decision and discussion items on the meeting agenda. Discussion agenda items allow the FSC to explore and document facility-related issues. If a decision item carries a funding impact, the funding decision process is used (see Figure 3). If the decision does not carry a funding impact, each FSC representative has the option to request guidance on decision items.

THIS SPACE INTENTIONALLY LEFT BLANK

THIS PAGE INTENTIONALLY LEFT BLANK

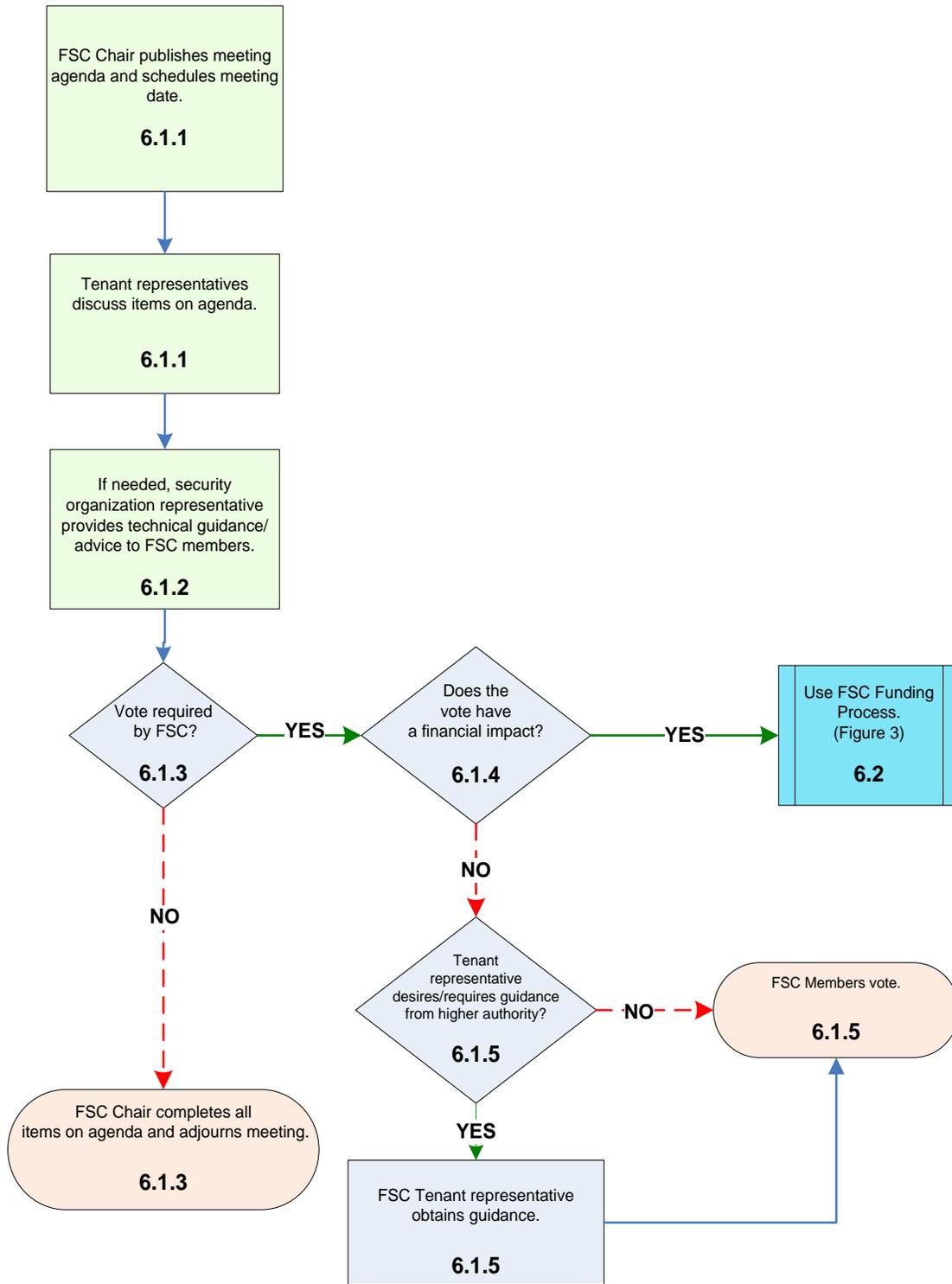


Figure 2: FSC Business Process

6.1.1. Meeting Agenda and Discussions

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

6.1.2. Security Organization Guidance

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

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

A vote can be held on meeting agenda items marked as decision items. Discussion agenda items relay information to the FSC members and document issues in the meeting minutes. A vote is permitted only on agenda items identified as decision items. Once all items on the agenda are addressed, the meeting is adjourned. The FSC voting process is detailed in Section 5.1 of this document. Section 6.1.4 of this document addresses processes for decision items that also have a funding impact.

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

A funding impact may be associated with a decision item. Section 6.2 of this document provides guidance on how to address decision items with a funding impact. Section 6.1.5 of this document provides details concerning decision items that do not carry a funding impact.

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

FSC members may desire guidance from their respective organizational authority. The FSC chairperson will establish a date for a vote on a decision item, while providing a reasonable period for FSC representatives to obtain guidance from their organization (not to exceed 45 calendar days). If an organization does not provide guidance to the FSC representative within this allotted time, the FSC chairperson may use the decision process or other means as determined by the FSC to obtain a resolution (see Figure 4). All FSC votes are recorded in the meeting minutes and distributed to each FSC member and security organization.

6.2. Facility Security Committee Funding Process

The FSC will be asked to consider changes to the security posture of their facility by adding new policies, changing existing policies, or by implementing new or enhancing existing physical security countermeasures. Generally, policy and procedures do not require funding to implement or change. Countermeasures usually require funding to purchase, install, and maintain the

countermeasure (e.g., purchasing of equipment or hiring of guards). When the FSC considers items that require funding, each FSC member is responsible for seeking guidance from their respective funding authority. Figure 3 outlines the funding decision process.

The FSC chairperson shall establish a date for a vote on a decision item requiring funding, while providing a reasonable period for FSC representatives to obtain guidance from their respective authority (not to exceed 45 calendar days). If guidance is not provided to the FSC representative within this allotted time, the FSC chairperson may use the decision process or other means as determined by the FSC to obtain a resolution. The meeting minutes must document each Federal department's or agency's vote to approve/disapprove a recommended countermeasure. If a countermeasure is not approved, the FSC accepts all associated risks relating to that decision.

THIS SPACE INTENTIONALLY LEFT BLANK

THIS PAGE INTENTIONALLY LEFT BLANK

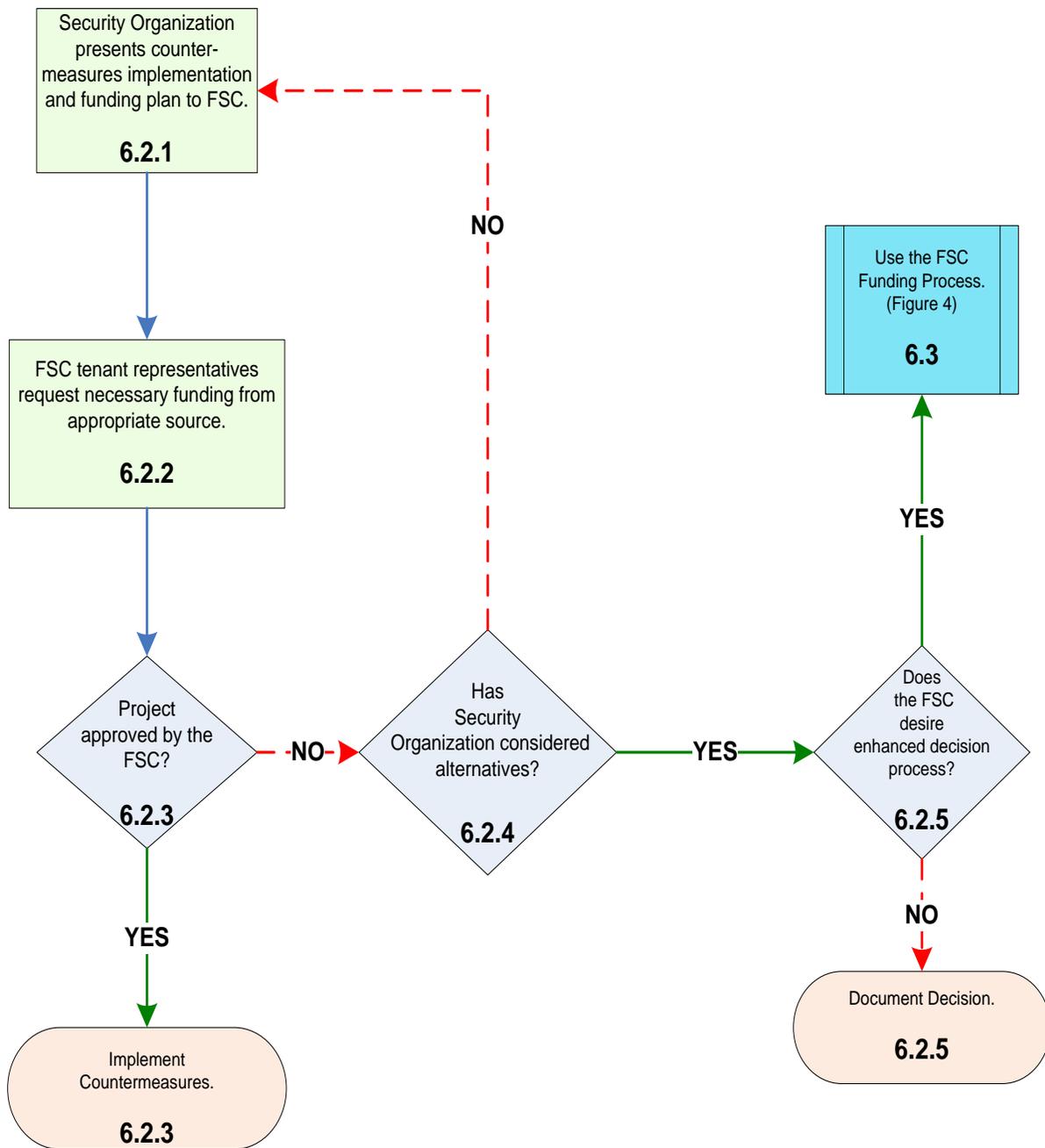


Figure 3: FSC Funding Process

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

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

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

6.2.2. Facility Security Committee Members Request Guidance from Their Respective Funding Authority

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

The FSC chairperson will establish a date for a vote on a decision item, while providing a reasonable period for FSC representatives to obtain guidance from their organization (not to exceed 45 calendar days). If an organization does not provide guidance to the FSC representative within this allotted time, the FSC chairperson may use the decision process or other means as determined by the FSC to reach a resolution (see Figure 4).

An FSC representative shall submit a written funding request to their respective authority and also request that their respective authority respond with a written approval or denial.

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

FSC members vote to approve or disapprove each proposed countermeasure based on the guidance provided by their respective authority. If approved, each countermeasure is implemented. Procedures for handling proposed countermeasures that are not approved are presented in Section 7.2.2 of this document. When the FSC votes to deny the implementation of a security countermeasure(s), each Federal department or agency will have accepted risk as an integral part of the committee's risk management strategy.

6.2.4. Decision Point: Has the security organization considered alternatives?

This decision point is an iterative loop for the purpose of facilitating technical discussions between the security organization and the security elements of the FSC members. The purpose of discussions is to promote creative thinking and evaluate multiple countermeasures to mitigate threat. If certain risks are accepted, the FSC must document the basis for the chosen risk management strategy. See Section 4.2 of this document for more information on Risk Acceptance.

6.2.5. Decision Point: Does the Facility Security Committee desire an enhanced 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 the Decision Process. For more information on the Decision Process, see Section 6.3 of this document.

6.3. Decision Process

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

The decision process illustrated in Figure 4 is a general guide. The organizational structure used by each Federal department and agency may be different. FSC representatives are responsible for determining the appropriate security level to contact within their respective organization for guidance and assistance.

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

THIS SPACE INTENTIONALLY LEFT BLANK

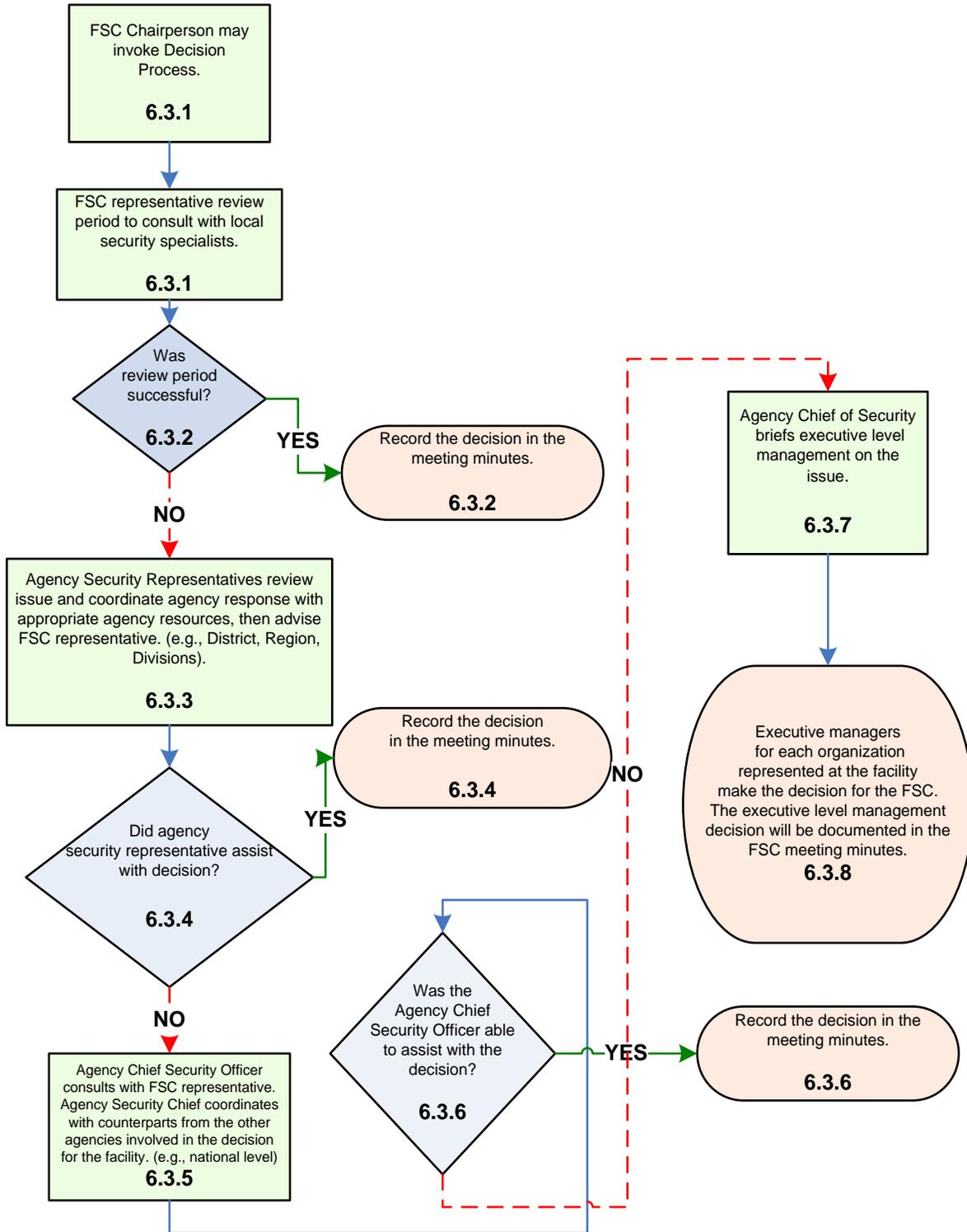


Figure 4: Decision Process

6.3.1. Facility Security Committee Chairperson Invokes Decision Process

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

6.3.2. Decision Point: Was the review period successful?

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

6.3.3. Organizational Security Element Assistance

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

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

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

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

6.3.5. Organizational Chief Security Officer Review

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

This step in the decision process must be completed within 30 calendar days of being referred to each respective organizational Chief Security Officer. The FSC may vote to extend the 30-calendar-day timeframe. Should a resolution not be reached in the agreed upon timeframe, the issue(s) in question shall be referred to each respective Organizational Executive Level Management for action.

6.3.6. Decision Point: Were the Chief Security Officers able to resolve the issue?

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

6.3.7. Organizational Chief Security Officer Briefs Executive Level Management

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

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

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

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

7. Funding

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

7.1. Funding for a Non-Unanimous Vote

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

7.2. Facility Security Committee Member Funding Authority

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

7.2.1. Approval of Funds

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

7.2.2. Disapproval of Funds

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

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

7.3. Funding Documents

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

7.4. Funding Impact to Occupant

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

The decision to implement security countermeasures or risk acceptance at a facility contains a financial component. To address this area, the security organization must provide a cost analysis that indicates the cost effectiveness of the proposed countermeasure. This analysis will follow the performance-measurement methodology outlined in the ISC's *Use of Physical Security Performance Measures* Standard.

7.5. Occupancy Agreement

Federal tenants may have the option to work with their owning or leasing authority to fund security countermeasure projects by means of rent increases. Usually this requires a change to the OA to adjust the amount of rent paid to the owning or leasing authority.

8. Special-Use Facilities

Special-use facilities are facilities that are regulated or mandated to have special security requirements under the supervision and control of another authority due to their special nature, work, or the special program that they support. Special-use facilities have the option of using ISC standards or their agency-specific standards.

8.1. Facility Security Committee Functions at a Special-Use Facility

The functions of an FSC at a special-use facility will be accomplished by the Federal department or agency responsible for the security of the facility.

9. Record Keeping

Meeting minutes and other documents or information the FSC deems important shall be retained as building-specific records. All FSC decisions shall be documented in the meeting minutes. Vote tabulation shall be recorded in the meeting minutes. Project funding approval, disapproval, and risk acceptance information shall be documented in the meeting minutes and the Facility Security Assessment. It is recommended that the FSC and the security organization maintain copies of records for a minimum of 10 years.

9.1. Purpose

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

9.2. Format of Records

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

9.3. Access to Records

All FSC members will have access to meeting records. Additional access to FSC records held by other agencies will require the approval of the FSC.

APPENDICES

Appendix A: Acronym List

BSC	Building Security Committee
CFR	Code of Federal Regulations
DBT	Design-Basis Threat Report
DOJ	Department of Justice
FEMA	Federal Emergency Management Agency
FSC	Facility Security Committee
FSL	Facility Security Level
GSA	General Services Administration
HSIN	Homeland Security Information Network
ISC	Interagency Security Committee
LOP	Level of Protection
OA	Occupancy Agreement
OMB	Office of Management and Budget
PSC	Physical Security Criteria for Federal Facilities
USMS	United States Marshals Service

Appendix B: Glossary of Terms

Adjacency: A building or other improvement that abuts or is proximate to a multiple building site, a specific building within a multiple building site, or a single building site.

Alteration: A limited construction project for an existing building that comprises the modification or replacement of one or a number of existing building systems or components. An alteration goes beyond normal maintenance activities but is less extensive than a major modernization.

Baseline Level of Protection (LOP): The degree of security provided by the set of countermeasures in the *Physical Security Criteria for Federal Facilities Standard* for each FSL that must be implemented unless a deviation (up or down) is justified by a risk assessment.

Building: An enclosed structure (above or below grade).

Building Entry: An access point into, or exit from, the building.

Building Envelope: The outside surface and dimensions of a building, inclusive of the façade and roof.

Campus: Two or more Federal facilities located on one 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 may also be referred to as a “Federal center” or “complex.”

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

Critical Areas: Areas that, if damaged or compromised, could have significant adverse consequences for the agency’s mission or the health and safety of individuals within the building or the surrounding community. May also be referred to as “limited access areas,” “restricted areas,” or “exclusionary zones.” Critical areas do not necessarily have to be within Government-controlled space (e.g., generators located outside Government-controlled space).

Customized LOP: The final set of countermeasures developed as the result of the risk-based analytical process.

Design-Basis Threat (DBT): A profile of the type, composition, and capabilities of an adversary.

Existing Federal Facility: A facility that has already been constructed or for which the design and construction effort have reached a stage where design changes may be cost prohibitive.

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

Facade: 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 (FSC): A committee responsible for addressing facility-specific security issues and approving the implementation of security measures and practices. The 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 (FSL): A categorization based on the analysis of several security-related facility factors, that serves as the basis for the implementation of physical security measures specified in ISC standards.

Federal Departments and Agencies: Those executive departments enumerated in 5 U.S.C. 101, 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.

Federal Tenant: A Federal department or agency that occupies space and pays rent on this space in a Federal facility.

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

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

Lease Construction (Build-to-Suit): A new construction project 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 (LOP): The degree of security provided by a particular countermeasure. 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 consequences 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.

New Construction: A project in which an entirely new facility is to be built.

New Lease: A lease established in a new location when space must be added to the current leased space inventory.

Non-Federal Tenant: For the purposes of entry control, employees of non-Federal tenants who occupy other space in a mixed multi-tenant facility. The FSC (and lease agreement) would establish entry control requirements applicable to non-Federal tenants passing through a Federal entry control point (in accordance with established policies).

Occupant: Any person who is permanently or regularly assigned to the Government facility and displays the required identification badge or pass for access. The FSC establishes the thresholds for determining who qualifies for “occupant” status.

Outlease: The practice of an owning Government agency leasing Government space to non-Governmental tenants.

Primary Tenant: The Federal tenant identified by Bureau Code in OMB Circular No. A-11, Appendix C, that occupies the largest amount of rentable space in a Federal facility.

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

Risk Acceptance: An explicit or implicit decision not to take an action that would affect all or part of a particular risk. Risk acceptance is one of four risk management strategies, along with risk avoidance, risk control, and risk transfer.

Risk Assessment: The process of evaluating credible threats, identifying vulnerabilities, and assessing consequences.

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

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

Risk Management Methodology: A set of methods, principles, or rules used to identify, analyze, assess, and communicate risk, and mitigate, accept, or control it to an acceptable level at an acceptable cost.

Risk Management Strategy: A proactive approach to reduce the usually negative impacts of various risks by choosing within a range of options that include complete avoidance of any risk that would cause harm or injury, accepting the risk, controlling the risk by employing risk mitigation options to reduce impacts, or transferring some or all of the risk to another entity based on a set of stated priorities.

Risk Mitigation: The application of strategies and countermeasures to reduce the threat of, vulnerability to, or consequences from, an undesirable event.

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

Setback: The distance from the façade to any point where an unscreened or otherwise unauthorized vehicle can travel or park.

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 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.

Standoff: Distance between an explosive device and its target.

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 operation of the facility or mission of the agency.

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

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

Appendix C: The ISC Pro Rata Voting Share Calculation Tool

The FSC chairperson may determine each Federal agency tenant’s pro rata voting share by using the *ISC Pro Rata Voting Share Calculation Tool*, located on the ISC HSIN web site. The following instructions outline how to complete the necessary calculations in the tool.

1. List separately each agency tenant who is an occupant of the facility.
2. Enter the number of employees for each separate agency tenant occupying space in the facility.
3. Enter the rentable square footage of each separate agency tenant’s assigned space.
4. Finally, to calculate the agency’s share of the vote, click in the Pro Rata Voting Share column for each separate agency tenant. (The tool will automatically make the calculations and populate both the Weighted Combined Values column and the Pro Rata Voting Share column. As each separate agency tenant is either added to or deleted from the tool, the tool will automatically recalculate all pro rata voting shares.)

Example of the Pro Rata Voting Share Calculation Tool

Agency Tenant	Number of Occupants	Square Feet	Weighted Combined Values (Employees = 60% / Sq. Ft. = 40%)	Pro Rata Voting Share
EXAMPLE - USMS	88	28,491	60.00 + 40.00 =	100%

Interagency Security Committee Participants

ISC Chair

Todd M. Keil

Assistant Secretary for Infrastructure Protection
U.S. Department of Homeland Security

ISC Executive Director

Austin L. Smith

Interagency Security Committee
Office of Infrastructure Protection
U.S. Department of Homeland Security

2010-2011 Working Group Co-Chairs and Members	
<u>Co-Chair</u> David Olson - DHS	<u>Co-Chair</u> Mark Strickland - GSA
Diane Dixon - EPA	Bernard Holt - ISC
Ed Templeman - AO USCO	David Dimmitt - DOJ
Bill Dwyer - DOE	Mark Oberholtzer - FAA
Christopher Strambler - ED	Tommy L. Hinson - IRS
Justin Sotherden - USDA	Ashley Gotlinger - ISC
2008-2010 Working Group Chair and Members	
<u>Chair</u> Mark Strickland - GSA	
Paul Raudenbush - NASA	Tommy Barnes - FDIC
Reginald Allen - OPM	Bernard Holt - ISC
Mark Applewhaite - USPIS	Ray Patterson - NASA
Sonya Rowe – State	Bob Harding - GSA
Thomas Holman - DOL	Don Williams - HHS
Tom Thomas - UCIA	Charles Luddeke - DHS
Mark Harvey - DHS	Leslie Wiggins - State