Best Practices for Working with Lessors:

An Interagency Security Committee Guide

November 2014
1st Edition

Interagency Security Committee

Best Practices for Working with Lessors

Released by: Interagency Security Committee

Name of Signing Authority: Caitlin Durkovich

Title and Branch/Division/Department: Chair of the Interagency Security Committee

Document Control

This document is UNCLASSIFIED. It may be distributed without restriction.

Message from the ISC Chair

As Chair of the Interagency Security Committee (ISC), I am pleased to introduce the *Best Practices for Working with Lessors: An Interagency Security Committee Guide.* This guide will improve the working relationship between Federal tenants and lessors in implementing appropriate countermeasures.

This guide focuses on security countermeasures associated with the necessary Level of Protection (LOP) for common and public access areas. The best practices identified in this guide will assist Federal agencies and lessors early in the leasing process in developing adequate risk management strategies when applying necessary or achievable LOPs, using the ISC *Risk Management Process: An Interagency Security Committee 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 53 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 ISC's objective was to develop recommendations all Federal agencies could utilize to increase cooperation between Federal tenants and lessors.

This guideline is a significant milestone and represents exemplary collaboration within the ISC working group and across the entire ISC. The ISC will review and update this guideline as needed.

Caitlin Durkovich
Assistant Secretary
Infrastructure Protection

This page intentionally left blank.

Executive Summary

Best Practices for Working with Lessors: An Interagency Security Committee Guide is intended to further improve the working relationship between Federal tenants and lessors in implementing appropriate countermeasures, principally those security countermeasures associated with the necessary Level of Protection (LOP) for common and public access areas. The best practices identified in this guide will assist Federal agencies and lessors early in the leasing process in developing adequate risk management strategies when applying necessary or achievable LOPs, using the Risk Management Process as outlined in the Interagency Security Committee (ISC) Standards.

This document addresses Government Accountability Office (GAO) findings that the ISC's *Physical Security Criteria for Federal Facilities Standard*, 2010, does not sufficiently address tenant agencies' degree of control over common areas and public access, particularly in mixed multi-tenant facilities. The *Best Practices for Working with Lessors* guide provides a framework for working with lessors to identify required security countermeasures early in the leasing process and to implement those measures in a risk-based approach before finalizing the lease agreement. The best practices identified in this document apply to all agencies with delegated security responsibilities in non-military Federal government leased space.

In most facilities, it is neither common to find anything close to perfect security nor is perfect security an economically feasible objective. Several constraints to providing security for leased space exist, not the least of which are security limits imposed by lessors in common areas, therefore requiring risk-based analysis and ultimately risk acceptance by the Federal government and tenants. Aside from the obvious financial limitations, other limitations such as manpower and set-back factor into security measures required or risks accepted. In the leasing process, the earlier the constraints are recognized and addressed, the greater the chances for success in overcoming or compensating for complications. Once the lease is signed, any subsequent security-related changes come only with the approval of the lessor and likely at greater expense to the government. An 'earlier is better' approach summarizes an overriding best practice theme throughout this guide.

After considering potential constraints, the pre- and post-award best practices identified in this document look for early and ongoing involvement by government physical security specialists in guiding a balanced process for leasing space that ensures appropriate risk-based protection for Federal tenants. Pre-award actions set the process on the right course, starting with assigning key government players to the project team, the de facto predecessor to the eventual Facility Security Committee (FSC). Most important for the government is involvement by physical security specialists from conception to design, construction, acceptance, and occupancy. Their involvement provides the best guarantee for instituting and implementing risk-based Federal security standards.

Physical security specialists of appropriate seniority and experience, and in sufficient numbers, can promote and preserve government security interests. Their early involvement in the leasing process can help reduce costs to the lessor and the government by advocating appropriate rather than excessive or unnecessary measures and by suggesting cost-effective options and mitigations.

Involvement by physical security specialists must extend throughout the leasing process. Post-award, assuring full and proper implementation of agreed upon security measures may fall on the government physical security specialists overseeing project completion.

If a physical security specialist is on the project team from the onset, they can advocate for and implement the use of the ISC Risk Management Standard Process (RMP). An early commitment to the risk management process, starting with the project team during pre-award, encourages a universal understanding of why government security specialists advocate a particular facility security level (FSL) and the inherent security countermeasures. The security specialists can guide the development of the Design-Basis Threat (DBT) that in turn helps determine the LOP and associated protection countermeasures required at the facility and, therefore, inclusion in the lease.

Tenants must identify their security needs as early as possible in the process. This is especially true for any unique or unusually expensive requirements and any requirements affecting the entire building. Individual tenant requirements may either conflict with or complement each other and are subject to peripheral but related requirements such as Homeland Security Presidential Directive (HSPD) -12 implementation and information technology considerations. This highlights the need for open lines of communication with the lessors and among tenants on a formal and frequent basis. Channels of communication may include, but are not limited to, inviting lessors to FSC meetings and specific "status update" meetings to maintain continual security dialogue among all interested parties.

Co-locating Federal and private organizations and/or different Federal components with varying levels of protection requirements can create security challenges. Early assessment will assist in identifying how security measures may impact different tenants or whether individual floors or suites merit consideration as their own facility for security. Co-location of tenants with similar security requirements and limited mixing of Federal and non-Federal tenants is a cost-efficient best practice. In the cases where agencies are not compatible, the financial burden and operational impacts should be considered in the decision to co-locate tenants.

Where risk acceptance becomes unavoidable, project documentation must reflect why the necessary levels of protection cannot be achieved. Documentation should explain the mitigation strategy and how the tenant agency, security organizations, and the real estate property provider will coordinate oversight of the risk acceptance and implementation of the risk management strategy.

In summary, the best practices include early and frequent involvement of government physical security specialists and open lines of communication and routine coordination among the lessor, the lessees, and government agencies overseeing the leasing process. Adopting this approach minimizes the probability of the difficult and unlikely prospect of making changes post-award and reduces the likelihood of requiring potentially disruptive and cost-prohibitive changes. If changes are required due to the addition of a new tenant, adjustment in mission criticality, or lease renewals, the continuity of the relationship already built with the lessor, embodied in open lines of communication and coordination, may necessitate more flexibility and accommodation.

Table of Contents

Table of Figures

1 Background

On September 22, 2010, the Government Accountability Office issued a report titled GAO-10-873, *Building Security: New Federal Standards Hold Promise, But Could Be Strengthened to Better Protect Leased Space*. The report was in response to House Report No. 110-207 that directed the GAO to assess the ISC's 2004 standard, *Security Standards for Leased Space*. However, the 2004 standard was superseded in April 2010 by the ISC's *Physical Security Criteria for Federal Facilities Standard* that made security a priority in the operations, planning, design, construction, renovation, and/or acquisition of non-military Federal facilities, whether they are owned or leased. In light of the new standard, the GAO focused its attention on identifying challenges that continue to exist in protecting leased space and how well the 2010 ISC standard addresses those challenges.

The GAO concluded that the ISC's 2010 *Physical Security Criteria for Federal Facilities Standard* did not sufficiently address tenant agencies' lack of control over common areas (e.g., elevator lobbies, building corridors, restrooms, stairwells, loading docks) and public access, particularly in mixed multi-tenant facilities. In addition, despite some tenant agencies' in-house expertise, the GAO report stated, "leasing officials sometimes do not have the information they need to allocate resources using a risk management approach before a lease is signed because early risk assessments are not conducted for all leased space."

2 Purpose

The *Best Practices for Working with Lessors* was created in response to the GAO recommendation contained in its final report, GAO-10-873, *Building Security: New Federal Standards Hold Promise, But Could Be Strengthened to Better Protect Leased Space*.

According to the GAO, although the ISC's *Physical Security Criteria for Federal Facilities Standard* outlined specific countermeasures for addressing public access, it lacked in-depth discussion and guidance, such as best practices, that could provide a framework for working with lessors to implement such countermeasures. Given the critical role lessors play, such guidance is warranted.

One standard unavailable to the GAO for consideration during the review period was the *Facility Security Committees: An Interagency Security Committee Standard* issued January 2, 2012. FSCs are required in facilities with two or more Federal tenants that have funding authority, and they are established to make security decisions for the facility. The FSC standard provides guidelines, policies, and procedures for how an FSC should function, make decisions, and resolve disputes, thereby creating a partnership to work with lessors in securing leased space.

The purpose of this document is to:

- Articulate guidance to organizations when working with lessors;
- Define a decision-making process to determine, address, and mitigate risks using a risk management approach; and
- Ensure decisions are tracked and documented (per ISC standards).

The ISC may integrate this guidance into editions of the ISC's *Risk Management Process*.

3 Applicability and Scope

Pursuant to the authority provided to the ISC in Section 5 of Executive Order (EO) 12977, as amended by EO 13286, this ISC document provides guidance to non-military Federal departments and agencies, leasing officials, and security officials on how to work with lessors. The document provides direction on how to secure common areas and protect leased space. In addition, it provides recommendations for developing and sustaining effective partnerships with lessors.

This document is to be used in conjunction with the ISC's standards when implementing a risk management process to determine the necessary or highest achievable LOP or appropriate risk management strategy.

To determine guidance for potential best practices, the working group met with private industry representatives ensuring their perspectives were presented for consideration. The working group specifically discussed how Federal agencies can enhance the working relationships with the lessors to effect greater protection of non-military government-leased space.

In an effort to develop a more robust and complete set of guidelines, the working group met with private industry representatives to ensure the relationship between non-military Federal agencies and the lessor can be made as mutually beneficial as possible. The agenda of the meeting with the private industry was framed by four questions:

- What primary challenges does a lessor face while working with government lessees?
- If security conditions change and upgrades or additional countermeasures need to be added to a facility, what approach best suits the lessor?
- What is the lessor's expectation regarding a lease with the Federal government?
- What advice would a lessor give the Federal government to enhance and strengthen the relationship?

In addition, the working group met with the U.S. General Services Administration (GSA) leasing specialists to obtain their recommendations for best practices when working with the lessors to develop security measures for publicly accessible and common areas.

4 Constraints and Limitations

No single security strategy, system or process exists that will eliminate all risk, even in government-owned facilities. Perfect security is often unaffordable or unobtainable. In leased space, the lessors, not tenant agencies, may place limits on security measures and typically control physical security in common areas. Limitations outside of direct government control can constrain security measures and will impose risk acceptance requirements. Reconciliation of multiple competing requirements, standards, and priorities cannot always be achieved without acceptance of risk. As a result, recommendations or guidance provided by this document may still fall short of achieving the desired or necessary LOP in leased facilities. Despite constraints, including budget realities, the Federal government must put forth its best effort to provide a secure environment supporting policy, mission, and operational requirements.

Given that the Federal government does not own the building and/or other tenants in the building may have limiting lease requirements, the lessor may not be able to comply with the government's security needs. When a building or lease situation presents neither the capability nor inclination to provide a countermeasure or process to provide full security to mitigate that risk, the government may need to implement a risk management strategy.

The best time to request a countermeasure or a specific risk reduction process is prior to award of the lease. Potential lessors are more responsive than a lessor with a signed lease. The flexibility prior to award may include location of the space, layout of the space offered, and other variables often locked in at award. Once the lease is awarded, the flexibility is reduced due to contract law issues, financial issues, and because there is less value to the lessor to change items that are not "easy" to change.

The risk management process as outlined by the ISC is still a relatively new concept; therefore, education of non-military Federal agency personnel is on-going. Some gaps in application of knowledge may exist in the short term until outreach and education is completed throughout the ISC membership. These gaps may include, but are not limited to:

- A leasing specialist may not have the ability to obtain the countermeasures required, from a lessor or owner, for "full security" coverage, before or after award of the lease;
- Ultimately the buildings are privately owned with many limitations (i.e. zoning, permitting, etc.);
- The entire lease procurement cannot be driven by the security requirements; and
- Requiring more of the leasing agency's security organization's designated physical security specialist's time to communicate and work with the client agency, the client agency's security organization, the lessor and any security professionals involved.

Most existing leased buildings, especially in downtown metropolitan areas, were built with little or no "setback" from streets or public access. Therefore, there is little expectation of protection for the facility from potential threats such as improvised explosive devices (IED), whether borne by vehicle or placed by an individual. In addition, with regard to new construction, there may be some issues with setback requirements, especially in light of the Competition in Contracting Act and GSA location policy (e.g. central business district policy, environmental location policy, and transportation access policy).

All items that the non-military Federal tenant(s) require to secure the facility should be included in the solicitation and the lease when it is being written. Only those items included in the lease can be required of the lessor. Therefore, if a countermeasure is not specified in a lease, the lessor cannot be required to provide it.

When leasing space, the government must abide by the following regulations, policies, and factors that affect agencies' location decisions and subsequent selection of a delineated area:

- Federal Management Regulation (FMR) Part 102-83—Location of Space;
- Rural Development Act (7 U.S.C. 2204b-1);
- Executive Order 11990, "Protection Of Wetlands";
- Executive Order 11988, "Floodplain Management";
- Executive Order 12072, "Federal Space Management";
- Executive Order 13006, "Locating Federal Facilities on Historic Properties in Our Nation's Central Cities";
- Executive Order 13514, "Federal Leadership in Environmental, Energy and Economic Performance"; and
- Implementing Instructions – Sustainable Locations for Federal Facilities.

All of these are factors in the selection of a delineated area and the acceptability of any of the buildings in that area.

4.1 Manpower

The number of non-military government-leased buildings dwarfs the number of trained physical security specialists that are available to conduct timely and effective training, inspections, and surveys. A single physical security specialist can be assigned multiple government-leased facilities located in multiple cities, counties, and states. In many cases, these government-leased facilities can be hundreds of miles apart, causing a logistical challenge for the security organization. Geographical dispersion can often cause inspectors or the security organization to interact with lessors in person only during the recurring assessment period. Facility security posture and communication with tenants and security organizations can be improved when lessors understand ISC Standards.

4.2 Financial

While security compliance and training is driven by standards, current and future funding is a major variable. Government agencies are restricted by the allocated or appropriated funds available and the requirements to implement many recommended countermeasures outlined in the ISC standards. This restriction will limit funding available to pay for security criteria to be implemented by the lessor. Additionally, funding may limit the number of agency security staff, the ability of those physical security specialists to travel, and the acquisition of countermeasures. In leased facilities where the government is not the sole tenant, funding and implementing some countermeasures presents particular challenges.

Countermeasures planning can be extremely time-consuming, expensive, complex and involved. Non-government tenants may consider relocating, thereby creating further hardship for the lessor. To avoid such events, the project team and the lessor should work closely with the security organization. In some cases, the government tenant organization may choose to accept the risk as identified by the security organization. Although the risk may be accepted, the project team should attempt to implement new procedures or augment current security protocols in an attempt to reduce the building's vulnerability and document any risk accepted by virtue of limited or lack of mitigating measures. Ultimately, the goal is to provide appropriate protection to the government tenant and reduce the impact of cost and inconvenience to non-government tenants.

4.3 Suitability

Suitability of employees can be a limitation for a lessor when they are trying to hire quickly. Please refer to section 5.8.4, suitability and background checks of building employees, for more information regarding suitability.

4.4 Limitations on Possible Mitigations/Solutions

4.4.1 Control of Building Space

In any commercial/government office lease, the only space fully controlled by the lessee is the space occupied under the contract. The common areas of the building are for the use of all tenants in the building. Common areas are under the control of the lessor and not for any one tenant's exclusive use.

4.4.2 Cost of Security Protection

Most of the government's leased space is in existing buildings not specifically designed with the expectation of a level of security required under the ISC guidelines. The cost to bring leased buildings up to FSL III and IV level of protection may be prohibitively expensive or may cause rents to increase to prohibitive levels.

Upgrade costs for structural components in most buildings could result in: 1) lease cost escalation above high-end market values; or 2) increase in lease payments that over the life of the term exceeds the value of the building at lease inception. In the latter case, the lease would be determined to be a capital expenditure and the government would be required to obligate the entire rent over the term at award of the lease (Office of Management and Budget [OMB] Circular A-11 Appendix A and B). But in either case the cost could stop the award of the lease.

4.4.3 Control of Tenant Choice

The Federal Management Regulations require vacant leased space be filled with any agencies looking for space. An agency with a lower FSL being moved into a building with a higher FSL can cause major problems. The lower FSL agency, for example, could be responsible for paying the security fees associated with the higher level of security.

5 Best Practices for Working with Lessors

5.1 Roles and Responsibilities

5.1.1 Project Team

A project team typically includes the architects, engineers, contracting officers, subject matter experts, project managers, and a member of the security organization responsible for the building from the contracting agency, the client organization, contractors, end user representatives, and anyone else with a stake in the successful completion of the project. Upon award, lessors and subject matter experts would be added to the project team.

The project manager and his/her team manage all aspects of the project from beginning to end. The team is responsible for ensuring activities and tasks are completed on schedule, addressing changes or issues, and adjusting the project schedule accordingly.

Federal agencies' security organizations should assign a physical security specialist to the project team at the onset of all new lease projects, construction projects, or addition/alteration to an existing building. **Involving a physical security specialist in the project, starting with the initial requirements development and continuing through design, award, construction, and acceptance is paramount to a successful lease.**

Involving a Physical security specialist during the concept phase of proposed projects especially FSLs 3, 4, and 5, is critical for those who will:

- Deliver the project;
- Use the space at the end of the project; and
- Have a stake in the project to reach agreement on its concept and definition.

At the end of the concept phase, general guidelines should be generated to assist in defining the overall parameters of the project and an agreement on the project's end product(s).

Analyzing project constraints, alternatives, and related assumptions may also be part of the initial concept phase. These activities should be kept at a high level, such as a needs requirement document that does not result in a project design document, unless otherwise appropriate.

Many of the future requirements could have major effects on project and security costs. This includes the possibility some security requirements cannot be achieved.

5.1.2 Facility Security Committees

The Facility Security Committee is responsible for addressing facility-specific security issues and approving the implementation of security measures and practices. During the design phase of a project, the project team will act as the FSC. The FSC consists of representatives from all Federal tenants in the facility, the security organization, and the owning or leasing department or agency. The project manager will act as the designated official in a lease project. In the case of new construction or pending lease actions, the project team and the planned tenant(s) will also be included in the FSC. Refer to the *ISC Risk Management Process: an ISC Standard, Appendix D, How to Conduct a Facility Security Committee* for further information.

5.1.3 Designated Security Organization

The project team should involve the designated security organization in the concept phase of new projects in order to ensure that physical security requirements are identified and captured in the solicitation document. Involving the security organization early in the process may prevent delays, additional cost to the government, losses to the lessor and the general contractor, unnecessary acceptance of risk, and degraded countermeasures.

The leasing authority's security organization will designate a physical security specialist to represent them during the lease project. The tenant may provide security representation as needed. The security organizations shall provide their physical security specialists with the additional expertise needed to perform this function.

During the pre-award, physical security specialists' responsibilities include the following (Note: *responsibilities may vary depending on the size and scope of a project and other factors specific to each Federal agency*):

- Recommending the FSL determination;
- Performing risk assessments to assist with establishing necessary and customized LOPs;
- Developing a customized statement of requirements for physical and procedural countermeasures and agency required security features in the conceptual and/or planning phases of new projects to be included in the solicitation document;
- Providing an Independent Government Cost Estimate (IGCE) or input to an IGCE to stakeholders for project budget planning;
- Developing, reviewing, modifying, and approving designs for physical security countermeasures;
- Performing market research in conjunction with the project team and providing feedback and recommendations to stakeholders;
- Evaluating solicitations to ensure the lessor/lessee-provided security requirements are adequately addressed and meet security needs; and
- Developing scopes of work for the installation of security systems and providing scheduling input to the project team on security activities to identify inter-dependencies and critical paths.

During the post-award phase, physical security specialists' responsibilities (as contracting officer's technical representatives [COTR] or subject matter experts [SME]) include the following (Note: *responsibilities may vary depending on the size and scope of a project and other factors specific to each Federal agency*):

- Providing oversight for quality assurance during construction to ensure construction methods and materials are installed as designed;
- Performing acceptance testing and commissioning of electronic and mechanical security systems;
- Providing guidance to FSCs and on-site security specialists as needed on alterations to existing countermeasures or implementation of additional countermeasures; and

- Providing guidance or oversight lifecycle management and maintenance for security systems.

5.2 Organizational and Project Specific Security Requirements

Tenant agencies should pre-determine their most stringent security needs. Fine tuning the security plan can be completed at the design phase.

The ISC standards are risk-based, minimum physical security standards for non-military Federal facilities. It should be understood there may be additional requirements affecting physical security specific to each organization and/or project. These factors include but are not limited to the following:

- Physical security requirements governed by other Federal or agency-specific policies for special use or storage areas (e.g. storage or processing of classified information; weapons and ammunition; nuclear, biological, or chemical agents; laboratories; containment or interview rooms; etc.);
- Specific Federal agency templates, guides, or standards for physical security construction;
- HSPD-12 Physical Access Control Systems requirements for identity verification;
- Information technology requirements affecting security systems; and
- The ability to increase security posture due to imminent and elevated threats including but not limited to those related in the National Terrorism Advisory System (NTAS).

5.3 Entrance and Perimeter of the Building vs. Leased Space

In many instances Federal agencies lease office space in facilities shared with other Federal tenants, private organizations, or a mix of both. When a private tenant requires unrestricted access for employees and visitors but the minimum LOP requires entry controls, this becomes a challenge. The lessor is put in a situation where meeting the Federal security requirements could violate the lease terms of a private organization. In other instances there may be ISC requirements for alarms and entry control measures at the building perimeter, but there may be different Federal agencies occupying suites in the building with varying agency specific requirements for physical access control, intrusion detection, and/or video monitoring systems.

As defined by the Physical Security Criteria (PSC), a facility is inclusive of a building or suite. Sometimes it is not feasible to treat the entire building as the facility, but instead to treat the individual suite as its own facility. In such an instance, the perimeter of the leased space would be treated as the perimeter of the facility.

The necessary level of protection for blast mitigation and structural requirements can be addressed for the building as a whole; however, other countermeasures and controls may be implemented at the perimeter of the suite leased by each Federal agency. In an instance where there is more than one Federal tenant following this model, the requirement to form an FSC still applies, and the building should meet structural requirements that may not be limited to the leased perimeter.

5.4 Co-location for Low Risk and High Risk Tenants in Mixed Space

The determination of the necessary level of protection in accordance with the ISC Risk Management Process is essential. Identification of countermeasures appropriate for the level of protection agreeable to the tenants in a multi-tenant facility is especially challenging when tenants do not have similar security requirements or needs, such as when a high-risk law enforcement entity is located in the same facility as a low-risk administrative entity or public-facing entity.

A tenant requiring a significantly higher level of security should not be moved into a facility with a low security level or vice versa. Such a move would result in the lower-risk tenants having to accept and share the cost of a higher level of security than they require. Even if an alternative is to allow the higher-risk tenant to pay for any increased security measures required, based on its move into the facility, the operational impacts upon the other agencies must be considered (e.g., the implementation of extensive visitor screening procedures may adversely affect a tenant with a high volume of public contact).

The onus is not just on the agency with real property authority that facilitates the relocation; it is shared by agencies seeking to relocate. By agreeing to occupy a space, the agency is agreeing to the level of security established for that facility and any operational or cost impacts associated with maintaining it. Modifications to security requirements over time must be addressed through FSC procedures.

The addition of other occupants after the first lease is acquired can have major security and financial effects on the existing tenants.

5.5 Security Manpower Considerations for Lease Project Development

Background:

Because projects occur in varied environments (from an area of dense high-rise office buildings with many public or private tenants to single story stand-alone buildings) and diverse locales (from urban center cities to rural open land), an attempt was made to identify some of the factors affecting the security needs of a project. Others factors are harder to define and have less effect on the security needs in a project.

How to use the matrix:

The following matrix was created to be used as a best practice to help determine the difficulty of providing the appropriate security for the tenant agencies early in the lease process. Please refer to Figure 1: Project Difficulty Index as a guide with the understanding that not all information may be available at the time of application. Several of the factors may not be determined prior to award, but this tool may be used as a guide to identify major areas of security uncertainty. Since there may be several unknown factors, divide the total by the number of factors known and get the average points per factor and use the ratings below to determine the project difficulty.

Case Study:

The matrix is populated using the following example: There is a level III procurement, around 100,000 square feet, with two Federal agencies; one of the agencies has some public access (e.g., Social Security Administration or Internal Revenue Service). It is a smaller/rural city with an urban Central Business District (CBD) with mid/ high rises (3+ stories) around 100,000 to 250,000 square feet. There are several vacant spaces in buildings that may have one or a few private, small businesses in those buildings. Like many city center buildings, there may be commercial space on the ground floor with some minor access to the office building lobby.

Figure 1: Project Difficulty Index

Factor	Points				Score
Facility Security Level	***I*** *1 Point*	***II*** *2 Points*	***III*** *3 Points*	***IV*** *4 Points*	3
# of Private Tenants in the Building*	***SINGLE TENANT*** *1 Point*		***MULTIPLE TENANTS*** *3 Points*		1
Location	***RURAL*** *1 Point*	***SUBURBAN*** *2 Points*	***RURAL CITY CENTER*** *3 Points*	***URBAN*** *4 Points*	3
Building Type	***NEW CONSTRUCTION*** *1 Point*		***EXISTING BUILDING*** *3 Points*		3
# of Government Tenants*	***ONE GOVT TENANT*** *1 Point*	***TWO GOVT TENANTS*** *3 Points*	***3+ GOVT TENANTS*** *4 Points*		3
Agency's Accessibility to the Public	***NONE*** *1 Point*	***MINIMAL*** *2 Points*	***SOME*** *3 Points*	***FULL TIME*** *4 Points*	3
Location in Building (Floor #) Only Multi-Story Bldgs.	***MID LEVEL*** *1 Point*	***UPPER LEVEL*** *2 Points*	***TOP FLOOR*** *3 Points*	***1st FLOOR*** *4 Points*	1
Types of Private Tenants*	***NO PRIVATE TENANTS*** *1 Point*	***PRIVATE BUSINESS*** *2 Points*	***PUBLIC FACING*** *3 Points*	***FOOD SERVICE/ RETAIL*** *4 Points*	2
% of Full Occupancy*	***100% OCCUPANCY*** *1 Point*	***75% OCCUPANCY*** *2 Points*	***50% OCCUPANCY*** *3 Points*	***25% OCCUPANCY*** *4 Points*	3
Project Difficulty Level ***Average points (Project Difficulty Points ÷ Total # of Factors = Average Points)*** *1.75 or Less = Minimum Difficulty* *1.75 – 2.50 = Standard Difficulty* *2.51 – 3.25 = Difficult* *3.26 or More = Very Difficult*					**Project Difficulty Points:** 22

Denotes an approximation or estimate that may have to be made at the beginning of a project.

Figure 2: Sample Project Difficulty Calculation and Scoring Index

Project Difficulty Points	÷	# of Factors	=	Average Points
22		9		2.444
Average per factor known				
1.75 or less		Minimum Difficulty		
1.75 to 2.5		Standard Difficulty		
2.5 to 3.25		Difficult		
3.25 or greater		Very Difficult		

5.6 Scoring Interpretation

Minimum Difficulty (1.75 Average Points or Less) – Projects will need input early in the leasing process. Most of the countermeasures are in the interior of the space and will be included in the base requirements of a lease. Most of the need for input will occur in the requirements development phase and in the Request for Lease Proposal (RLP)/lease (solicitation) creation phase. Little other input in the process will be needed.

Standard Difficulty (1.75 – 2.5 Average Points) – Projects considered "normal" or "typical" will need a security organization's input throughout the process in:

1. The requirements development phase;
2. The market survey phase;
3. The RLP/lease(solicitation) creation phase;
4. The design phase; and
5. The final inspection phase.

Difficult (2.5 – 3.25 Average Points) – Projects will require heavy input by a security organization or consultant throughout all phases of the leasing process. There are many times the leasing specialist will need input from the security specialist, including layout, design, countermeasures, and alternatives to countermeasures. Input for alternative methods will be needed in many of these projects to achieve "full" protection.

Very Difficult (3.25 or More Average Points) – These projects will require the security organization or consultant, the tenant agency security staff, or a security consultant to completely commit to the project team. Many of the complex's or building's surrounding areas will need to be specially reviewed and designed. There may be numerous countermeasures that will affect the project, both in scope and design. Each project detail could have a major effect on the security of the space.

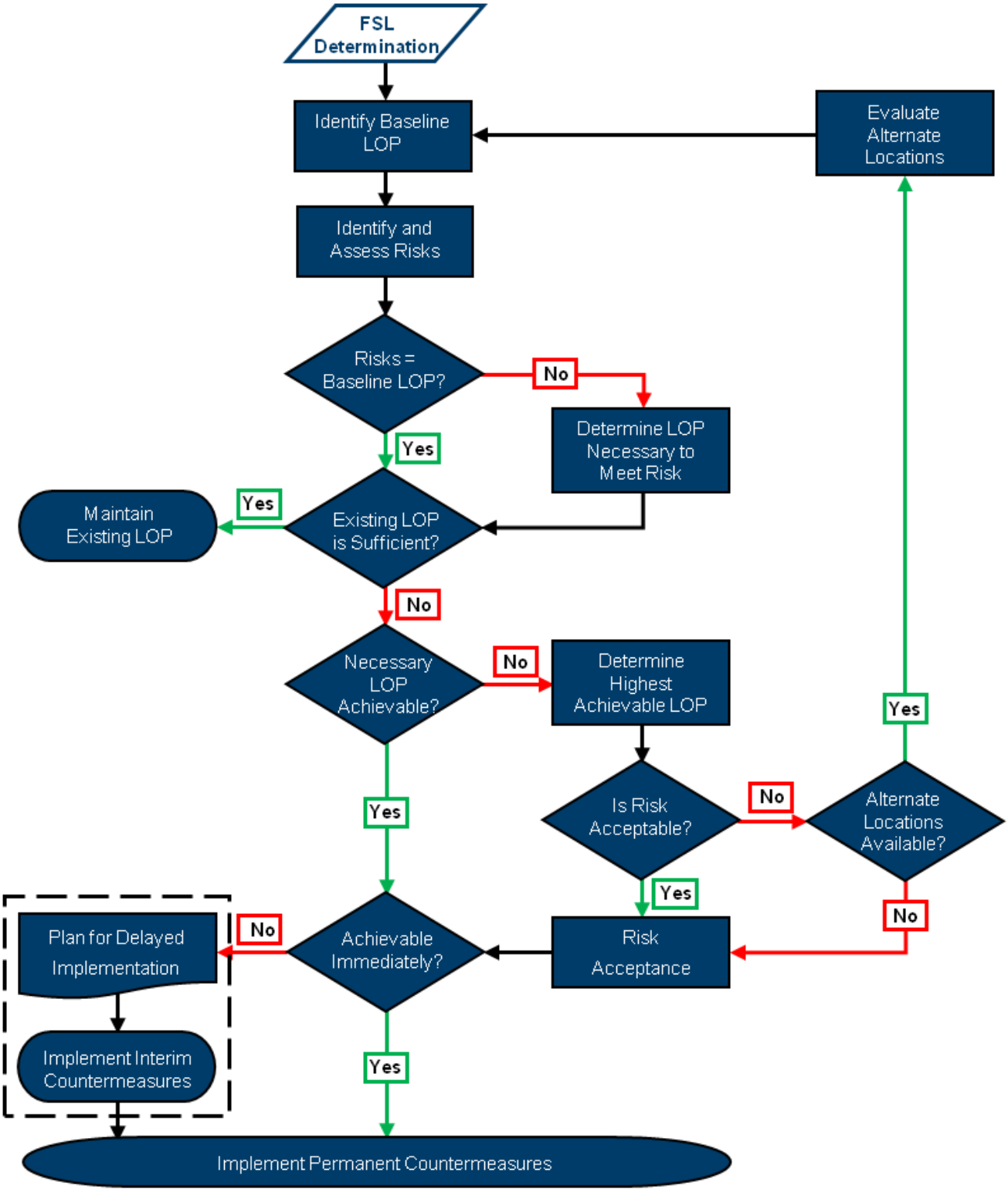
Determining the Project Difficulty Level is achieved by assessing up to nine of the project factors and assigning point scores to each factor. The chart (part of Figure 1) displayed on the following page is used to collect project data (example data is shown in the Score column). The calculation table below can then be used to determine the difficulty level. [Note that both the calculation table and the scoring table are part of the same figure.]

5.7 The ISC Risk Management Process

As a best practice, the project team acting as the FSC must refer to *the Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, Appendix D, How to Conduct a Facility Security Committee.* It provides business, funding, and decision-making processes designed to assist the project team and establish guidelines for discussing and determining security related issues.

Both the project team and the FSCs must adopt the ISC's *Risk Management Process* to identify and achieve either the appropriate LOP or the highest achievable LOP. The determination of the FSL is crucial in opening communication and beginning the project properly. The ISC *Risk Management Process* is identified in Figure 3.

Figure 3: The Risk Management Process



5.8 Pre-Award

5.8.1 Project Kick-Off Meeting

The Leasing Authority should schedule a project kick-off meeting between all relevant parties (e.g., leasing agency, security organization representative and tenant agencies, etc.). As part of the discussions, the Realty Specialist/Contracting Officer (RS/CO) should confirm the initial FSL determination and review the report to verify that all of the representatives understand the security requirements and countermeasures to be included in the solicitation.

5.8.2 Requirements and Development Phase

During the requirements and development phase, the project team acting as the FSC should adopt the ISC Risk Management Process. The security organization should conduct a project-specific risk assessment during the requirements definition phase. Recommend adjustments (additions or reductions) to the FSL countermeasures and design features to be included in the design specifications. The project team should determine whether the identified countermeasures will be enacted or a risk management/acceptance strategy will be implemented.

5.8.3 Risk Assessment Process

Risk assessment is the process of evaluating credible threats, identifying vulnerabilities, and assessing consequences. It takes into account the likelihood that an event will occur. A risk assessment for proposed leased facilities is the foundation for assessing and prioritizing risk in order to provide stakeholders with cost effective countermeasures. Agencies determine their best course of action in keeping with their risk management philosophy. The security organization's and/or the physical security specialist's first step is to determine which assets are to be protected. Generally this includes people/employees, information, critical assets, and equipment.

As part of the assessment, the physical security specialist will determine the threats, some of which are dynamic. Agencies and departments should utilize the ISC's *Design Basis Threat* report as a tool to identify possible threats. The DBT establishes a profile of the types, composition, and capabilities of adversaries; however, it is not all encompassing. While the DBT should not be the sole document in determining the outcome of an assessment, it should certainly be one of the sources of information.

In addition to the agency's broad threat vectors focusing on the overall mission, the physical security specialist should also coordinate with local law enforcement to review historical and recent crime trends for the area. For example, if possible, a proposed facility should be located away from an area experiencing an increase in crime. However, that concern should not be the only deciding factor in determining a location. Agencies should look at each facility individually and conduct a cost-benefit analysis to weigh the benefits of a location against the cost of mitigating threats.

Upon gathering all of the facts during the security assessment, the physical security specialist should:

- Provide a briefing to the market survey team;
- Provide a list of countermeasures required for each facility; and

- Offer input into the security situation based on the ISC's *Risk Management Process*.

The physical security specialist should be aware that security is not the sole determinant in facility selection.

5.8.4 Considerations

An agency or a tenant agency should conduct an ISC-compliant facility security assessment, inclusive of the ISC *Risk Management Process*, prior to awarding a lease. This can be completed by the security organization using the ISC Standards or a compliant tool when one becomes available.

A security organization should be involved prior to the issuance of a RLP/Solicitation for Offers (SFO) to ensure that ISC, specific agency, or building security requirements are included and satisfied. By requiring an official pre-lease assessment, the contracting officer can incorporate the appropriate security paragraphs within the RLP-Lease/SFO so that the potential lessors are made fully aware of the PSC requirements and necessary LOP.

Funding, manpower, and time minimize the security organization's ability to complete many pre-lease assessments before the lease is signed. Hence, occasionally the lessor is surprised once a post-lease assessment is completed by the security organization and ISC-compliant implementations are recommended. To avoid such occurrences, some Federal organizations may utilize their own security organization or a third party security organization to provide an ISC-compliant assessment of their facilities.

5.8.5 Pre-Award Meetings

The pre-award meeting should include all relevant parties (i.e., leasing agency, lessors, owners, Security Organization, and tenant agencies, etc.). The Leasing Authority and the RS/CO should confirm that the potential lessors understand all the security requirements and countermeasures as defined in the solicitation document and agree that they can be met.

5.9 Post-Award

Until the contract is signed by both parties, a lessor has greater incentive to fulfill the government's requested security alterations to get a signed lease. Once the lease has been executed, the flexibility is greatly lessened because the incentive for a lessor to make any changes decreases. Once signed, any change to the lease will require additional communication and coordination between the tenant and the lessor and may also require additional funding and/or resources. There is very little incentive for the lessor to change the contract without compensation.

Potential security changes to a contract may occur for many reasons. The reasons most frequently include, but are not limited to: the changing of tenants during the term of the lease, changing occupying tenants within the facility, agency mission changes, and the need for temporary upgrades to countermeasures due to significant threats and/or undesirable events. More communication between the primary government agency (e.g., contracting officer, COTR), the facility, security subject matter experts and the lessor is rarely harmful and is often helpful.

5.9.1 Maintaining Communication

Project teams are encouraged to invite lessors to security meetings, as appropriate, in order to keep the lessor abreast of evolving conditions. Attendance by the lessor also helps maintain open communication and builds a strong partnership for the safety and security of personnel, visitors, information, equipment, and physical assets.

5.9.2 Tenant or Mission Change

If a new tenant or change in mission of an existing tenant brings new or increased risks, recommended countermeasure upgrades should be considered and discussed with the lessor prior to the change taking place. Additionally, an FSL determination should be conducted.

5.9.3 Temporary Upgrades

When a significant threat is discovered, the security organization should notify the tenant agency(s) and the leasing agency of the issue. As a best practice, the security organization should have a meeting with the lessor, the tenant agency(s), and the leasing agency. The objective of this meeting would be to discuss the issues and options available to counter the threat, including expected timeframes for this heightened security status.

In many leases, the government has a clause giving it the ability to undertake temporary security upgrades in leased space. The biggest issues with this clause, from a lessor's perspective, are the scope of the upgrades and the length of time. In some situations the exercise of this clause can create legal problems for lessors and tenants because some tenants (non-Federal and Federal) may have clauses in their leases that would allow them to terminate their lease if certain alterations are made to the facility.

5.9.4 Suitability and Background Checks of Lessor's Employees and Contractors

The following codes and regulations are applicable for clearance of building employees; the Office of Personnel Management (OPM) has delegated authority to several agencies to make final suitability determinations:

- Code of Federal Regulations (CFR) 731, "Suitability" provides the authority for the OPM as the lead agency for contract personnel suitability requirements and background investigations;
- GSA Lease Desk Guide, Chapter 19: Security; and
- DHS Management Directive 11055, "Suitability Screening Requirements for Contractors," provide additional reference information to satisfy contractor suitability requirements.

OPM defines suitability as, "Identifiable character traits and conduct sufficient to decide whether an individual is likely or not likely to be able to carry out the duties of a Federal job with appropriate integrity, efficiency, and effectiveness" (OPM Suitability Primer, 2007: http://www.archives.gov/isoo/oversight-groups/nisp/opm-suitability-primer.pdf).

Suitability is sometimes required for all contractor personnel requiring routine, ongoing, and unescorted access to government-owned and/or leased facilities. This may include contract Protective Security Officers, childcare workers, and janitorial staff, among others.

An initial suitability determination includes a preliminary check of credit, name, address, education, and fingerprints to establish whether the applicant can perform the duties without compromising security or public trust. If an individual successfully clears preliminary checks, the applicant is eligible to begin work on an interim adjudication pending the completion of a full background investigation and adjudication for the final suitability.

The government reserves the right to verify the identities of and conduct background checks on personnel with routine access to government space. Government agencies reserve the right to implement agency-specific requirements for background checks associated with granting of access and security clearances, but the level of clearance should reasonably be determined during the requirement development phase. The procuring agency and potential lessors must be advised prior to award, at the latest.

Routine access is defined as regularly scheduled access for a period greater than six (6) months. At a minimum and upon request, the lessor shall submit completed Form FD-258, Fingerprint Charts, and Standard Form 85P or Standard Form 85P-S, Questionnaire for Public Trust Positions, for each employee of the lessor as well as employees of the lessor's contractors or subcontractors, who will provide building operating services requiring routine access to the government's leased space (GSA Memorandum for Assistant Regional Administrators PBS dated 2007-07, *Background Investigations in Leased Space*).

Non-routine access is defined as unscheduled access or limited access required for a period of less than six (6) months. An intermittent contractor – one who is requested for a service call as needed – is not required to have a background investigation, but must be escorted by someone who has already been cleared and meets escort requirements.

The risk and sensitivity designation determines the type of background investigations required. Some background investigations may be more in-depth and require more time to complete. Therefore, lessors should initiate required fingerprint charts and questionnaires early in the initial hiring.

5.10 Risk Acceptance

Risk acceptance is an allowable outcome of applying the risk management process. In some cases, risk acceptance is unavoidable. Competing requirements, standards, and priorities cannot always be reconciled. Additionally, budgeting limitations are always present but policy and mission requirements cannot be ignored.

Risk acceptance occurs when a countermeasure suggested by the security organization is not implemented or a lower level countermeasure is selected. In all cases, the project documentation must clearly reflect both the reason why the necessary LOP cannot be achieved and the rationale for the selection of the risk management strategy to be implemented.

As a best practice, agency security organizations, in coordination with real property offices, should establish methods to oversee risk acceptance and risk management strategies. At a minimum, risk acceptance documentation must be reviewed when the designated official for risk

acceptance changes or when a new risk assessment is completed. The ISC's RMP provides sample templates to assist in making these determinations.

5.11 Tracking and Documentation

Meeting minutes and other documents or information the Project Team/FSC deems important shall be retained as building-specific records. All Project Team/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 as well as the facility security assessment.

The Project Team's documentation must clearly identify the necessary level of protection. In those circumstances where the necessary level of protection cannot be attained, the documentation must clearly demonstrate why and identify the achievable level of protection and risk management strategy to be implemented. Project documentation must be maintained by the security organization and leasing agency during the life of the lease.

To promote transparency and ensure greater understanding of the processes involved and determinations agreed upon, all Project Team/FSC members will have access to meeting records.

5.12 Lease Renewal

The ISC standards require that risk assessments be conducted at least once every five years for Level I and II facilities and at least once every three years for Level III, IV, and V facilities. The FSL will be reviewed and adjusted, if necessary, as part of each initial and recurring risk assessment. As a best practice, security organizations should seek opportunities to conduct risk assessments in conjunction with lease renewals. For example, if a lease is under consideration for renewal and the risk assessment is not required by the standards for another twelve months, the security organization should perform the risk assessment early so any changes in the necessary LOP and associated countermeasures can be addressed during the lease process.

The leasing authority (e.g., Lease Contracting Officer [LCO], Lease Contracting Officer's Representative) and security organization should schedule a meeting annually to review all pending lease renewals so the security organization can adjust and plan risk assessments accordingly.

6 Educational Requirements

The ISC has developed a series of free online training courses to provide non-military Federal facility security professionals, engineers, building owners, construction contractors, architects, design teams, and project teams with basic information pertaining to the ISC and its facility security standards, processes, and practices. This training is mandatory for personnel assigned to FSCs, which would include project teams who are acting as the FSC.

Note: *This training is mandatory for Federal officials assigned duties as members of an FSC. It is recommended that lessor officials who work closely with Federal Security Committees complete the following ISC training courses*:

- IS-890a - Introduction to the Interagency Security Committee;
- IS-891 - Interagency Security Committee: Facility Security Level Determinations for Federal Facilities (FOUO);
- IS-892 - Physical Security Criteria for Federal Facilities (FOUO); and
- IS-893 - Facility Security Committees.

Please refer to Appendix B for additional information on the ISC training courses.

7 References

- DHS, Facility Security Committees: An Interagency Security Committee Standard, 2nd Edition. (January 2012).
- DHS, Facility Security Level Determinations for Federal Facilities: An Interagency Security Committee Standard. (March 2008).
- DHS, Interagency Security Committee: Security Standards for Leased Space, 2004 (Superseded).
- DHS, Physical Security Criteria for Federal Facilities: An Interagency Security Committee Standard. (April 2010).
- DHS Management Directive 11055, "Suitability Screening Requirements for Contractors" (Title 5 Code of Federal Regulations 731.106(b)).
- Executive Order 11988, "Floodplain Management."
- Executive Order 11990, "Protection of Wetlands."
- Executive Order 12072, "Federal Space Management."
- Executive Order 12977, Interagency Security Committee, October 19, 1995.
- Executive Order 13006, "Locating Federal Facilities on Historic Properties in Our Nation's Central Cities."
- Executive Order 13286, Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security, February 28, 2003.
- Executive Order 13514, "Federal Leadership in Environmental, Energy and Economic Performance."
- FMR Part 102-83—Location of Space, http://www.gsa.gov/Portal/gsa/ep/channelView.do?pageTypeId=17113&channelId=-24559&specialContentType=FMR&file=FMR/FMRTOC102-_83.html#wp436256 .
- GAO-10-873, "Building Security: New Federal Standards Hold Promise, But Could Be Strengthened to Better Protect Leased Space."
- GSA Realty Services Letter 2007 "Background Investigations in Leased Spaces."
- House Report No. 110-207, at 62-63 (2007).
- Implementing Instructions – Sustainable Locations for Federal Facilities
- OPM, Credentialing, Suitability, and Security Clearance and Decision-making Guide, January 14, 2008.
- OPM Suitability Primer, 2007.
- Rural Development Act (7 U.S.C. 2204b-1).

8 Interagency Security Committee Participants

ISC Chair

Caitlin Durkovich

Assistant Secretary for Infrastructure Protection

U.S. Department of Homeland Security

ISC Executive Director

Austin Smith

Interagency Security Committee

Office of Infrastructure Protection

U.S. Department of Homeland Security

Interagency Security Committee Representative

Bernard Holt

ISC Working Group Members

Chair, Bernard Minakowski – GSA

Scott Dunford – ISC

Ashley Gotlinger – FPS

Richard Cestero – USMS

Colin Doniger – DHS

Shaun Irvine – PFPA

Rodney Ludvigson – DOL

James Pelkofski – PFPA

Jerry Stanphill – FAA

Byron Tonic – PFPA

James Ward – GSA

Sandra Wilson – PFPA

List of Abbreviations/Acronyms/Initializations

TERM	DEFINITION
CBD	Central Business District
CFR	Code of Federal Regulations
COTR	Contracting Officer's Technical Representative
DBT	Design-Basis Threat, or Design Basis Threat Report
EO	Executive Order
FMR	Federal Management Regulation
FOUO	For Official Use Only
FSC	Facility Security Committee
FSL	Facility Security Level
GAO	Government Accountability Office
GSA	U.S. General Services Administration
HSPD	Homeland Security Presidential Directive
IED	Improvised Explosive Devise
IGCE	Independent Government Cost Estimate
ISC	Interagency Security Committee
LCO	Lease Contracting Officer
LOP	Level of Protection
NTAS	National Terrorism Advisory System
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PSC	Physical Security Criteria
RLP	Request for Lease Proposal
RMP	Risk Management Process
RS/CO	Realty Specialist/Contracting Officer
SFO	Solicitation for Offers
SME	Subject Matter Expert

Glossary of Terms (Definitions)

TERM	DEFINITION
Acceptable Risk	Acceptable risk describes the likelihood of an event whose probability of occurrence is small, whose consequences are so slight, or whose benefits (perceived or real) are so great, that individuals or groups in society are willing to take or be subjected to the risk that the event might occur. **Extended definition:** level of risk at which, given costs and benefits associated with risk reduction measures, no action is deemed to be warranted at a given point in time. **Example**: Extremely low levels of waterborne contaminants can be deemed an acceptable risk.
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.
Consequence	The level, duration, and nature of the loss resulting from an undesirable event.
Countermeasures	An action, measure, or device that reduces an identified risk. Countermeasure cost may be monetary, but also no-cost such as administrative findings.
Customized LOP	The final set of countermeasures developed as the result of the risk-based analytical process.
Delegated Authority	To grant the leasing agency's authority to a requesting Federal agency to perform for itself all functions necessary to acquire office space in privately-owned buildings. Each authorization to use the delegation is for specific lease space and that particular Federal agency for the lease procurement, subject to the limitations contained in the FMR and FMR Bulletin 2008-B1.

TERM	DEFINITION
Design Phase	Transitional phase of a project where a "designer" (architect, architect/engineer, interior designer, or similar professional) takes the schematics (the written requirements and the description of the entities and relationships) and the needs that were documented during the requirements development phase are further refined and the design specifications are organized for implementation within the constraints of a physical environment. The designer prepares drawings and other presentation documents to crystallize the design concept and describes it in terms of architectural, electrical, mechanical, and structural systems. The designer may also prepare a statement of the probable project cost.
Design-Basis Threat (DBT)	A profile of the type, composition, and capabilities of an adversary.
Entrance	The designated point or points to which pedestrians or vehicles are channeled through the use of barriers or landscaping to gain entry into a government controlled space, campus, compound, facility, or suite.
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.
Existing LOP	The degree of security provided by the set of countermeasures determined to be in existence at a facility.
Exterior	Area between the building envelope and the site perimeter.
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, which 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 and the Department of Homeland Security, independent establishments as defined by 5 U.S.C. 104(1), government corporations as defined by 5

TERM	DEFINITION
	U.S.C. 103(1), and the U. S. Postal Service.
Federal Facilities	Government leased and owned facilities in the United States (inclusive of its territories) occupied by Federal employees for non-military 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 Renewal (Exercised Option)	The exercising of an option to continue occupancy based upon specified terms and conditions in the current lease agreement.
Leasing Agency/Authority	Government entity that acquires leased real property for occupancy for Federal tenants. The leasing authority maintains responsibility for administration of the lease throughout the term and enforces the Lessors compliance with the terms and conditions of the lease.
Lessor	Any individual, firm, partnership, limited liability company, trust, association, state or local government, or legal entity that is the rightful owner of the property leased to the Federal government.
Level of Protection (LOP)	The degree of security provided by a particular countermeasure or set of countermeasures. Levels of protection are Minimum, Low, Medium, High, and Very High.
Level of Risk	The combined measure of the threat, vulnerability, and consequence posed to a facility from a specified undesirable event.
Lobby	An area of space which appears to occupants as open, regardless of size, which is usually found directly after the main entrance to a facility. A lobby could also be referred to as a waiting/reception point within a tenant's controlled space.
Major Modernization	The comprehensive replacement or restoration of virtually all major systems, tenant-related interior work (e.g., ceilings, partitions, doors, floor finishes), or building elements and features.
Mixed-Multi-Tenant Facility	A facility that includes tenants from multiple Federal departments and agencies as well as one or more non-Federal tenants.

TERM	DEFINITION
Mixed-Tenant Facility	A facility that includes one Federal tenant as well as non-Federal tenants, including commercial and State/local government tenants.
Multi-Tenant Facility	A facility that includes tenants from multiple Federal departments and agencies but no non-Federal tenants.
Necessary LOP	The degree of security determined to be needed to mitigate the assessed risks at the facility.
New Construction	A project in which an entirely new facility is to be built.
New Lease	A lease established in a new location when space must be added to the current leased space inventory.
Non-Federal Tenant	For the purposes of entry control, employees of non-Federal tenants who occupy other space in a mixed multi-tenant facility. The FSC (and lease agreement) would establish entry control requirements applicable to non-Federal tenants passing through a Federal entry control point (in accordance with established policies).
Non-Military Activities	Any facility not owned or leased by the Department of Defense.
Occupant	Any person who is permanently or regularly assigned to the government facility and displays the required identification badge or pass for access, with the exception of those individuals providing a service at the facility (guards, custodians, etc…). The FSC establishes the thresholds for determining who qualifies for "occupant" status.
Owner	The person, collective group or agency who can legally claim the facility as an asset has the right to speak on the asset's behalf and also claims possession of the asset.
Perimeter of Leased Space	The outermost limits of the area controlled under a Federal agency, adjacent to public areas or other tenants by walls, doors, windows, floors, ceilings, or other barriers.
Physical Security Specialist	Individuals responsible for assessing risks, advising organizational leadership on physical protection of assets, and managing the implementation of selected countermeasures.
Post-Award	The time after a contract is negotiated and signed by the government and lessor.
Pre-Award	The time prior to the signing of a contract allowing for the continued negotiations on projects, requirements, cost, etc.
Primary Tenant	The Federal tenant identified by Bureau Code in OMB Circular No. A-11, Appendix C who occupies the largest amount of rentable space in a

TERM	DEFINITION
	Federal facility.
Project Team	A group of individuals usually made up of different skill sets, working towards a common goal. A project team typically includes architects, engineers, subject matter experts, project managers and/or a lease contracting officer from the contracting agency, the client organization, contractors, end user representatives, and anyone else with a stake in the successful completion of the project.
Public Facing	The amount (number of people), type (business partners, professionals, general public or at risk clientele) and mass (volume and timing) of public access required by the occupant organizations to function properly and fulfill their mission. A major factor is the intent and need of the individuals that would access the space.
Request for Lease Proposal (RLP) and Lease Contract	A form of solicitation tailored to each lease model. RLP has no force or effect after lease award, when the lease contract becomes the legally binding document.
Risk	A measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence.
Risk Acceptance	The explicit or implicit decision not to take an action that would affect all or part of a particular risk.
Risk Assessment	The process of evaluating credible threats, identifying vulnerabilities, and assessing consequences.
Risk Assessment Report	The documentation of the risk assessment process to include the identification of undesirable events, consequences, and vulnerabilities; and the recommendation of specific security measures commensurate with the level of risk.
Risk Management	A comprehensive approach to allocating resources for the protection of a facility, assets, and occupants to achieve an acceptable level of risk. Risk management decisions are based on the application of risk assessment, risk mitigation, and-when necessary-risk acceptance. **Extended Definition**: process of identifying, analyzing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level at an acceptable cost. **Annotation**: The primary goal of risk management is to reduce or eliminate risk through mitigation measures (avoiding the risk or reducing the negative effect of the risk), but also includes the concepts of acceptance and/or transfer of responsibility for the risk as appropriate. Risk management principles acknowledge that, while risk often cannot be eliminated, actions can usually be taken to reduce risk.

TERM	DEFINITION
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, and/or consequences from an undesirable event. **Extended Definition**: Application of measure or measures to reduce the likelihood of an unwanted occurrence and/or its consequences. Measures may be implemented prior to, during, or after an incident, event, or occurrence. **Example**: Through risk mitigation, the potential impact of the tsunami on the local population was greatly reduced. **Annotation**: Measures may be implemented prior to, during, or after an incident, event, or occurrence.
Security Maintenance	The regularly scheduled or routine upkeep of equipment.
Security Organization	The government agency or an internal agency component either identified by statute, interagency Memorandum of Understanding/Memorandum of Agreement or policy responsible for physical security for the specific organization or facility.
Security Systems	Any type of program, mechanism, device, obstacle, or visual assessment tool which provides any portion in assessment, access, detection, or response to a government controlled space. **Extended Definition**: Electronic system(s) that are designed to prevent theft or intrusion and protect property and life. Burglar alarm systems, access control systems, fire alarm systems, and video surveillance systems are all types of security systems.
Setback	The distance from the façade to any point where an unscreened or otherwise unauthorized vehicle can travel or park.
Single-Tenant Facility	A facility that only includes one Federal tenant or multiple components of the same Federal department or agency that fall under one "umbrella" for security purposes.
Site	The physical land area controlled by the government by right of ownership, leasehold interest, permit, or other legal conveyance, upon which a facility is placed.

TERM	DEFINITION
Site Entry	A vehicle or pedestrian access point into, or exit from, the site.
Site Perimeter	The outermost boundary of a site. The site perimeter is often delineated by the property line.
Solicitation Document	A document used to solicit offers for a lease acquisition. The document describes government requirements and performance criteria against which a lessor is expected to perform and the evaluation criteria that the government will use to evaluate offers.
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.
Tenant Agency	An agency who is occupying a space in a facility.
Threat	The intention and capability of an adversary to initiate an undesirable event.
Undesirable Event	An incident that has an adverse impact on the facility occupants or visitors, operation of the facility, or mission of the agency.
Visitor	Any person entering the government facility that does not possess the required identification badge or pass for access or who otherwise does not qualify as an "occupant."
Vulnerability	A weakness in the design or operation of a facility that an adversary can exploit. **Extended Definition**: physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard; characteristic of design, location, security posture, operation, or any combination thereof, that renders an asset, system, network, or entity susceptible to disruption, destruction, or exploitation. **Extended Definition**: characteristic of design, location, security posture, operation, or any combination thereof, that renders an asset, system, network, or entity susceptible to disruption, destruction, or exploitation. **Example**: Installation of vehicle barriers may remove a vulnerability related to attacks using vehicle-borne improvised explosive devices. **Annotation**: In calculating risk of an intentional hazard, the common measurement of vulnerability is the likelihood that an attack is successful, given that it is attempted.