Best Practices for Planning and Managing Physical Security Resources:

An Interagency Security Committee Guide

December 2015

Interagency Security Committee

Best Practices for Planning and Managing Physical Security Resources:

An Interagency Security Committee Guide

Released by: The Interagency Security Committee

Preface

One of the Department of Homeland Security's (DHS) national priorities is the protection of Federal employees and private citizens who work within and visit U.S. government-owned or leased facilities. The Interagency Security Committee (ISC), chaired by DHS and consisting of 56 Federal departments and agencies, has as its mission the development of security standards best practices, and guidelines for nonmilitary Federal facilities in the United States.

As Acting Executive Director of the ISC, I am pleased to introduce *Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide*. The purpose of this document is to identify practices most beneficial for physical security programs, determine the extent to which Federal agencies currently use these practices, and compile and circulate best practices agencies can use as a supplement to the ISC's existing security standards.

Consistent with Executive Order (EO) 12977 (October 19, 1995), *Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide* should be applied to all buildings and facilities in the United States occupied by Federal employees for non-military activities. These include existing owned; to be purchased or leased facilities; stand-alone facilities; Federal campuses; individual facilities on Federal campuses; and special-use facilities.

This guide, approved with full concurrence of the ISC primary members, is a significant milestone and represents exemplary collaboration across the ISC and among the ISC Resource Management Working Group. This guide was approved December 1, 2015 and will be reviewed and updated as needed.

Bernard Holt
Acting Executive Director
Interagency Security Committee

This page left intentionally blank.

Table of Contents

1 Background

The Interagency Security Committee (ISC) was formed by Executive Order (EO) 12977, signed by President Bill Clinton in 1995 following the Oklahoma City bombing. This devastating event prompted the White House to establish a permanent body to address the continuing government-wide physical security needs for Federal facilities. Today, the ISC is chaired by the Department of Homeland Security (DHS) and consists of a permanent body with representatives from 56 Federal agencies and departments.

In January 2013, the Government Accountability Office (GAO) produced the GAO-13-222 Report *Facility Security - Greater Outreach by DHS on Standards and Management Practices Could Benefit Federal Agencies*. In response to the findings presented in GAO-13-222, the ISC created the Resource Management Working Group to develop guidance to help agencies make the most effective use of resources available for physical security across their portfolio of facilities and examine organizational practices of resource management.

The GAO report examines the sources that inform agencies' physical security programs, the roles and responsibilities of those that may be involved in the planning and managing of physical security resources, and the management practices agencies use to oversee physical security and allocate resources. GAO reviewed and analyzed survey responses from 32 agencies. GAO also interviewed officials and reviewed documents from five of these agencies, which were selected as case studies for more in-depth analysis. The ISC Resource Management Working Group was chartered to:

- Identify practices most beneficial for physical security programs;
- Determine the extent to which Federal agencies currently use these practices; and
- Compile and disseminate best practices that agencies can use on a voluntary basis.

In February 2015, GAO produced the GAO-15-444 Report *HOMELAND SECURITY: Action Needed to Better Assess Cost-Effectiveness of Security Enhancements at Federal Facilities*. The report recommends the Secretary of Homeland Security direct the ISC, in consultation with ISC members, to develop guidance to help Federal entities implement the cost-effectiveness and performance-measurement aspects of, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*. In response to the aforementioned GAO-13-222 Report, the ISC Resource Management Working Group established the *Best Practices for Planning and Managing Physical Security Resources* document. GAO recommended "DHS should direct the ISC to conduct outreach to executive branch agencies to clarify how its standards are to be used, and develop and disseminate guidance on management practices for resource allocation as a supplement to ISC's existing physical security standard."[1] This best

[1] See http://www.gao.gov/assets/660/651529.pdf.

practice document expands on the guidance issued in *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard.* The risk management process (RMP) creates one formalized process for defining the criteria and process that should be used in determining the Facility Security Level (FSL) of a Federal facility, determining risks in Federal facilities, identifying a desired level of protection, identifying when the desired level of protection is not achievable, developing alternatives, and risk acceptance, when necessary. As further discussed in Section 4, the RMP is of the utmost relevance to address cost-effectiveness, performance-measurement, and the planning and managing of physical security resources.

Based on the working group's findings, the ISC presents the *Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide* to the Federal security community.

2 Applicability and Scope

The *Best Practices for Planning and Managing Physical Security Resources* is a guide intended to provide an introduction and understanding of the most efficient processes and procedures to effectively allocate resources to implement physical security programs within Federal departments and agencies. Furthermore, it is meant to assist Federal agencies with the application of best management practices to support budget-conscious allocation of physical security resources across an agency's portfolio of facilities.

This document provides guidance for department and agency heads, designated officials, security managers, security organizations, and Facility Security Committees (FSC) to use when designing a collaborative framework for allocating physical security resources. This includes establishing roles and responsibilities for key personnel (i.e., security, facilities management, emergency preparedness, safety, budget, etc.) involved in assessing the most efficient allocation of physical security resources. These officials should collaborate in developing applicable agency-wide physical security policies using risk management practices that compare physical security across facilities and measure the performance of physical security programs.

As outlined in the Government Accountability Office Reports GAO-13-222 and GAO-15-444, effective program management and performance measurement, including the use of management practices such as: risk management strategies, conducting inspections and tests, and a centralized management structure, is crucial to ensure the effective use of limited resources. While agencies are already using management practices to support oversight of their physical security programs, they can also leverage these management practices for the purpose of allocating resources.

In addition to ISC standards, sections of the United States Code (U.S.C.) and the Code of Federal Regulations (CFR)[2] grant authority for Federal departments, agencies, and security organizations to provide physical security for their facilities and employees.

3 Roles and Responsibilities

It is important that security, information technology, human resource management, information sharing and coordination are leveraged to help allocate resources. There are challenges for facility managers in quickly obtaining funding, so it is imperative that management prioritize funding for physical security along with other agency needs. A centralized approach can also help coordinate physical security across component offices and provide a single point of contact within the agency. The following list of entities is provided with regard to planning and managing resources on an as-needed basis:

- Chief Security Officer (CSO);
- Chief Financial Officer (CFO);
- Chief Information Officer (CIO);
- Facility/resource owner(s);
- Security organization(s);
- Public works;
- Electronic security and protective design engineer(s);
- Procurement and contracting specialist(s);
- Fire/safety representative(s);
- Emergency management; and/or
- Human Resource (HR) representative(s).

3.1 Director of Security or Chief Security Officer

The department/agency Director of Security or Chief Security Officer (CSO) is responsible for the security policies, programs, and operations of the respective agency. The goal is to ensure a safe and secure workplace for the protection of life and property. Responsibilities could include:

- Promulgating regulations;
- Establishing and maintaining department-wide security education and training programs;
- Evaluating and analyzing emerging security issues, regulations, and threats;
- Analyzing financial implications of security programs; and

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

- Establishing procedures, policies, methods, and/or standards for identifying and protecting information, personnel, property, operations, or material from unauthorized disclosure, misuse, theft, assault, vandalism, espionage, sabotage, or loss.[3]

3.2 Facility Security Committee

The FSC plays a critical role in physical security resource management. Together, the FSC and the security organization are responsible for identifying and implementing the most cost-effective countermeasure appropriate for mitigating vulnerability, thereby reducing the risk to an acceptable level.[4] The FSC is composed of one representative from each Federal department or agency that pays rent on an occupied space in a government-owned, leased or managed Federal facility with one vote on decision items.[5] The owning or leasing authority and security organization(s) are members of the FSC with voting privileges if they pay rent on and occupy space in the same facility. FSCs are encouraged to include the child-care center director (as applicable) as a non-voting member. Each Federal department or agency headquarters shall provide guidance to its FSC representative.

3.2.1 Facility Security Committee Chairperson

The FSC chairperson is the primary tenant's senior representative and may designate a senior staff member with decision making authority to serve as the FSC chairperson. However, the senior representative retains the responsibility for the FSC. Should the senior person with the primary tenant decline to serve as the FSC chairperson, the FSC members shall select a chairperson by majority 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;

---

[3] Please see https://www.opm.gov/policy-data-oversight/classification-qualifications/classifying-general-schedule-positions/standards/0000/gs0080.pdf, last accessed 20 March 2014

[4] *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*

[5] Please see *Facility Security Committees: An Interagency Security Committee Standard*

- 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; and
- Casting votes for their organization.

3.2.2 Facility Security Committee Members

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

- Representing organizational interests;
- Attending FSC meetings;
- Obtaining guidance and authorization to vote on issues with funding implications;
- Obtaining assistance from organizational security element; and
- Casting votes for their organization.[6]

In single tenant facilities, the Federal department or agency with funding authority is the decision maker for the facility's security. In consultation with the security organization, the department/agency Designated Official (DO) is responsible for security decision-making.[7]

3.3 Security Organization

The security organization is a 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 a specific facility. It may consist of a Federal law enforcement agency that provides integrated security and law enforcement services to federally owned and leased buildings, facilities, properties and other assets[8] and oversight by a Security Officer or Security Specialist. When a facility has one Federal tenant with security functions (including law enforcement or security guard personnel performing protection/patrol duties) 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 security functions, the FSC should select a lead Federal tenant to serve as the security organization.

Security organizations are responsible for identifying and analyzing threats and vulnerabilities and recommending appropriate countermeasures. The decision to implement those

---

[6] *Facility Security Committees: An Interagency Security Committee Standard*, 2nd Edition.

[7] Please see the *Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* for more information.

[8] Please see https://www.dhs.gov/federal-protective-service-0, last accessed 14 February 2014.

recommendations and mitigate the risk or to accept risk as part of a risk management strategy is that of the FSC. As previously noted, the FSC and the security organization are responsible for identifying and implementing the most cost-effective countermeasure appropriate for mitigating vulnerability, thereby reducing the risk to an acceptable level.[9] 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 facility's security organization will conduct a risk assessment to identify risk(s). When a facility does not have an assigned security organization or Federal tenant with a security element housed in the facility, the FSC shall select a Federal department or agency to provide the services of the security organization.

As outlined in the RMP, the security organization is required to conduct risk assessments at least every five years for Level I and II facilities and at least every three years for Level III, IV and V facilities. The FSL determination ranges from a Level I (lowest risk) to Level V (highest risk). The FSL will be reviewed and adjusted, if necessary, as part of each initial and recurring risk assessment. The responsibility for making the final FSL determination rests with the tenants (i.e., FSC or DO in single tenant facilities), who must devise a risk management strategy and, if possible, fund the appropriate security countermeasures to mitigate the risk. The final security-related decisions are made by the FSC in consultation with the owning or leasing department or agency and the security organization(s) responsible for the facility. The representative of the tenant agency may be the DO or another official approved by the department or agency to make such determinations (e.g., the Director of Security might make all determinations to ensure consistency).

In accordance with ISC standards, if the FSC 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.

When the security organization(s) and the owner/leasing authority do not agree with the tenant agency representative or Designated Office with regard to the FSL determination, the ISC, as the representative of the Secretary of Homeland Security, will facilitate the final determination. The FSL determination should be documented, signed, and retained by all parties to the decision.

[9] *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*

3.3.1 Collaborating with Supporting Organizations

Coordination with other organizations is paramount when determining resource requirements. Getting the right people involved will save valuable time and effort as plans and strategies are developed for new and existing resources. The following are a few organizations the FSC or DO should coordinate with concerning resource management:

- General Counsel often has broad roles encompassing crisis management, compliance, reporting, management and public policy advocacy.
- The CFO is responsible for the financial matters of the agency and will report to and work closely with the agency head. In addition, CFOs partner with the various organizations within the agency and interact closely with senior leadership to develop and implement comprehensive strategies for the agency.
- CIOs manage how information is stored, processed and communicated to help an agency achieve its goals.
- The Contracting Officer is a vital component of any plans for procurement or allocating resources. The responsibilities of the contracting officer include:
    - Negotiating with suppliers to draft procurement contracts: Negotiating, administering, extending, terminating, and renegotiating contracts;
    - Formulating and coordinating procurement proposals;
    - Directing and coordinating activities of workers engaged in formulating bid proposals;
    - Evaluating or monitoring contract performance to determine necessity for amendments or extensions of contracts, and compliance to contractual obligations;
    - Approving or rejecting requests for deviation(s) from contract specifications and delivery schedules;
    - Arbitrating claims or complaints occurring in performance of contracts;
    - Analyzing price proposals, financial reports, and other data to determine reasonableness of costs;
    - Negotiating collective bargaining agreements, if necessary; and
    - Serving as the liaison officer to ensure fulfillment of obligations by contractors.
- Facility Managers help ensure that organizations operate efficiently through planning and directing building-related services.

4 Resource Requirements

Resources are products, services or systems necessary to produce an outcome(s) that satisfies the needs of a person, group or organization. Resource requirements across the Federal government are implemented to ensure the accurate and timely development and deployment of products and

services to meet mission-critical objectives and life safety requirements. For example, contract protective security officer (PSO)[10] services are required to control access to a facility and resources such as security devices can be deployed to protect information technology (IT) infrastructure of the facility.

The initial phase of resource management involves conducting an asset inventory assessment to determine the assets necessary to meet agency critical mission requirements and identification of those assets directed by law or executive guidance for special protection measures (e.g. ammunition). Once these assets have been identified, a risk assessment should be conducted to evaluate operational needs. The assessment should be reflective of the overall mission for a given Federal agency. Furthermore, the assessment should identify capabilities needed to perform required functions, highlight deficiencies in the security procedures and protective system(s) and document the results of the analysis. Some of these capabilities may already be addressed with existing products, systems or services currently deployed by an agency. Additionally, a risk assessment serves to identify deficiencies in current and projected capabilities.

4.1 General Description of Operational Capability Process

The complexities of systems integration, interoperability, and the dynamic nature of operations (missions) and administrative functions are vast and far-reaching. Thus, it is necessary to determine current operational and administrative requirements, with respect to sustainability, to include maintenance of current capabilities, and the development of future capabilities to support the operational objectives of an agency while providing the maximum amount of security. This process is called operational capability.

Operational capability includes, but is not limited to, the following:

- Determining critical and sensitive operational and administrative needs (assets);
- Conducting risk assessments;
- Identifying vulnerabilities;
- Determining how to mitigate risk;
- Managing and accepting risk;
- Collaborating with supporting organizations;
- Determining resource support procedures.
- Conducting market research;
- Procuring products and services;
- Defining proposed resource outcomes and cost-effectiveness;

[10] For the purposes of this document, the term “protective security officer” is used to describe security guards, security officers, security patrol officers, or any other like-term.

- Considering life-cycle, warranty and preventive maintenance; and

Through these considerations and practices, physical security and its effectiveness can be continuously assessed and future projections can be made. The Facility Security Committee makes strategic and operational decisions, and aids in the development of diverse but well-considered options. The guidance provided by the FSC should also augment the adaptability of a Federal agency providing risk mitigation.

4.1.1 Determining Critical and Sensitive Operational or Administrative Needs

The organization/agency first needs to identify the critical mission(s) and the asset(s) (i.e., personnel, equipment) required to accomplish those missions. Second, identify the sensitive or administrative needs and the asset(s) required to accomplish/support those missions and functions. Tracking the resources applied to physical security efforts provides program managers with an understanding of the necessary resources, including expenditures and personnel, required for effective physical security program operations. Program managers can use this information to determine program growth, increases in cost, efficiency gains, and output costs. Essentially, this information provides an overview of the resources required to achieve program goals and to accomplish overall program mission goals. When considered in conjunction with output and outcome measures, they help determine the benefit of using various resource levels. Moreover, program managers should use this information to plan and justify resource requirements for future efforts.[11]

Establishing the FSL is a crucial step in determining critical and sensitive operational and administrative needs and associated protective measures for those needs. The FSL categorization then serves as the basis for implementing protective measures under other ISC standards. The FSC, in consultation with the security organization, is responsible for making the final FSL determination based on five criteria:

- Mission criticality;
- Symbolism;
- Facility population;
- Facility size; and
- Threat to tenant agencies.

[11] *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*

A sixth consideration may be made for intangible factors, if appropriate. The FSL will be used to determine the baseline level of protection (LOP). From there, risk and vulnerability assessments will be conducted to ensure the LOP is adequate to safeguard operational needs and assets.[12]

When the security organization(s) and the owner/leasing authority do not agree with the tenant agency representative (i.e., FSC) or Designated Official with regard to the FSL determination, the ISC, as the representative of the Secretary of Homeland Security, will facilitate the final determination. The FSL determination should be documented, signed, and retained by all parties to the decision.

4.1.2 Conducting Risk Assessments

Risk and vulnerability assessments are frequently the initial step in developing or modifying current processes and programs. These assessments are conducted to ascertain areas for improvement in order for PSOs to successfully and efficiently accomplish operational tasks. Assessments are realized through research, test phases, security surveys, etc. Based on the compiled information, security specialists formulate needs and requirements. Assessment products are the basis for applicable technology evaluations, solution alternatives analysis, operational requirements definitions, and ultimately the acquisition program(s).

The objectives of a risk assessment are threefold: evaluate credible threats (including criminal) and capabilities, identify vulnerabilities, and assess consequences. Upon completion of the risk assessment, gaps in existing protective security systems should be identified. This is done through the application of operational experience in physical security, knowledge of related processes, familiarity with security equipment/systems, and measures of success/effectiveness. The findings of the risk assessment must be thoroughly documented in the assessment report, along with recommendations to address them.[13]

4.1.3 Identifying Vulnerabilities

As the risk assessment is conducted, the security personnel should pay close attention to vulnerabilities and weaknesses that would make an asset more susceptible to damage from a threat or hazard. Vulnerabilities include deficiencies in security countermeasures, information technology systems, security protection systems and loss prevention programs. They contribute to the severity of damage when an incident occurs.

A vulnerability assessment provides the organization/agency the design-basis threat (DBT) specific to the agency's mission and assets.[14] Once the required LOP and associated DBTs have

---

[12] *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*

[13] *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*

[14] For more information please reference *The Design-Basis Threat: An Interagency Security Committee Report*

been established, the agency will be able to design a strategy to protect the critical missions, sensitive operational or administrative needs, and their associated assets. Vulnerabilities and gaps are identified through the application of security experience, awareness of related processes, familiarity with security equipment/systems and measures of success/effectiveness.

As outlined in previous ISC standards, the FSC should request that risk assessments be conducted by the security organization at least every five years for Level I and II facilities and at least every three years for Level III, IV and V facilities. The FSL determination ranges from a Level I (lowest risk) to Level V (highest risk). The FSL must be reviewed and adjusted, if necessary, as part of each initial and periodic risk assessment (or as changes occur) to ensure appropriate countermeasures are in place as the agency and/or facility circumstances evolve. By continually assessing its facilities, the agency is able to better mitigate risks and vulnerabilities. New vulnerabilities can arise for a number of reasons:

- New goals (e.g., 100% screening at all access points);
- New conditions (e.g., new or improved threats, deterioration/discontinuation of existing capabilities, hardware/software end-of life);
- New or updated processes/regulations (e.g., new laws, new organizational responsibilities, new relationships);
- Availability of new technologies that enable previously unattainable capabilities or introduce more cost-effective solutions to existing capabilities, etc.

4.1.4 Determining How to Mitigate Risk

As defined in *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard,* risk mitigation is the application of strategies and countermeasures to reduce the threat of, vulnerability to, and/or consequences from an undesirable event. Given the LOP requirements and the DBT level to a specific asset/mission, there are five strategies available to security decision makers to mitigate risk: avoidance, reduction, spreading, transfer and acceptance. Risk mitigation is accomplished by decreasing the risk level by eliminating or intercepting the adversary before they attack, blocking opportunities through enhanced security or reducing the consequences if an attack should occur (i.e., detect, deter, defend, defeat). Without question, the best strategy for mitigating risk is a combination of all three elements: decreasing threats, blocking opportunities and reducing consequences.

Effective mitigation strategies should address how specific assets would be affected by threats, vulnerabilities, and identified risks. Solutions for the identified risks typically enhance three facets of security: policies and procedures; physical/electronic security systems; and security personnel.

4.1.5 Managing and Accepting Risk

By utilizing cost-benefit analyses, FSCs will determine the best methods to mitigate or accept the assessed risk(s) posed to the facility. The decision to provide resources, accept the risk or a combination of the two should be based on the FSL, a risk assessment, and the baseline or customized LOPs.

By determining the necessary LOP for the asset according to a risk assessment, cross-leveling between unmitigated risks to one asset can be avoided by transferring security measures from an asset that is over protected. Identified excess resources in one risk area can be reallocated to underserved areas, thus ensuring the most cost-effective security program is implemented. Where practicable, this technique will ensure that a facility is employing appropriate safeguards and countermeasures while efficiently managing resources.

In conducting cost-benefit analysis, some risks may be deemed acceptable by the FSC. If the probability and consequences of a particular risk are minor, given costs and benefits associated with risk reduction measures, no action is deemed to be warranted at a given point in time. Whenever risks are accepted, the FSC must document the decision and the supporting rationale.[15]

4.1.6 Procuring Products and Services

The General Services Administration (GSA) serves as the primary acquisition and procurement arm of the Federal government. The agency offers equipment, supplies, telecommunications, and integrated information technology solutions to Federal agencies. Agencies are responsible for acquisition policy, process, general workforce training and development, acquisition planning, operational execution, staffing and resources, control or performance outcomes. It is important agencies conduct due diligence on researching and evaluating the systems and equipment that is procured within their respective agency.

4.1.7 Conducting Market Research

Market research is the process of analyzing data to help understand which products and services will achieve the desired protective system, and how to get the best economic value for the required protective system equipment. Market research can also provide valuable insight by:

- Reducing security risks;
- Drawing attention to current and upcoming problems in an agency; and
- Identifying cost savings on products and services.

[15] *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*

Government agencies are responsible for determining "best value" when making procurement decisions related to the Catalogue Purchasing Program. A government agency may purchase products or services directly from GSA Advantage and may negotiate additional terms and conditions to be included in contracts relating to purchasing services. This is provided if the purchase is based on the best value available and is in the government's best interest. In determining which products or services are in the government's best interest, the agency shall consider the following factors:

- Installation costs and hardware costs;
- The overall life-cycle cost of the requested equipment;
- The estimated cost of employee training and estimated increase in employee productivity;
- Estimated software and maintenance costs; and
- Compliance with applicable Federal standards adopted by GSA or a subsequent entity as validated by criteria established by ISC or other entity with administrative authority.

4.1.8 Defining Proposed Resource Outcomes and Cost-Effectiveness

After conducting the risk assessment and market research, a proposal must be presented to management for approval. The proposal must demonstrate how the suggested recommendations will be cost-effective (i.e., mitigate risk) for the agency. By conducting proper research and coordinating with other agencies and organizations, agencies may find more cost-effective solutions. In an ever-changing economy, agencies must be creative and look for ways to enhance security (i.e., reduce risk) while also reducing cost.

4.1.9 Considering Life-Cycle, Warranty and Preventive Maintenance

Product life-cycle management (PLM) is the succession of strategies used by security management as a product goes through its functional life. The condition in which a product is sold changes over time and must be managed as it ages. A warranty is a statement by the seller or product manufacturer that it will perform in the manner specified for a guaranteed period of time. In the event that a product or service fails to perform as promised, the warranty may cover repairs or exchanges of the product. Agency procurement personnel are generally responsible for equipment purchases, repair, replacement and/or disposal. When proposing a purchase, it is advisable to first consult the agency's/component's procurement office.

Preventive maintenance is routine care designed to avert more costly repairs. By regularly inspecting and providing preventive maintenance to security equipment and systems, a security manager may be able to sidestep serious problems which arise as a result of neglect or over-use. Many agencies regard preventive maintenance as a critical part of caring for security equipment and systems. This practice is generally viewed as cost-effective, sound, and highly advisable for security organizations. Evidence of regular maintenance can also increase the life-cycle and performance of the products. Any number of things can fall under preventive maintenance. Some items to consider are: Closed-Circuit Television (CCTV), vehicle barriers, x-ray machines,

magnetometers and intrusion detection systems (IDS). Each of these security countermeasures is designed to reduce the risk of security threats.

4.1.10 Determining Resource Support Procedures

When reviewing maintenance processes and procedures, some topics to consider are:

- How will the system (hardware and software) be maintained?
- Who will maintain it?
- How, where, and by whom will spare parts be provisioned?
- How, where, and by whom will operators be trained?

These questions must be considered when developing a resource management plan in order to achieve successful implementation. It is imperative that the resource management plan encompass all phases of a product's useful life, from the initial planning stage to deployment to the end user.

4.2 Threat

Determining aggressor types (e.g., criminals, protesters, terrorists, etc.) and associated tactics (e.g., explosives/incendiary devices, unauthorized entry, surveillance, etc.) for a given agency's mission/assets is essential to implementing the proper security measures. Such measures are designed to protect facilities, people, and information systems from security breaches. Federal facilities require security countermeasures and policies to reduce the threats and challenges inherent from these threats. It is important to understand the five objectives of aggressors:

- Instilling fear in victims;
- Inflicting injury or death;
- Destroying or damaging facilities, property, equipment, or resources;
- Stealing equipment, material, or information; and
- Creating adverse publicity.

An organization must analyze its assets and the threats these assets face from aggressors and their tactics. Security assessments enable the agency to reduce security threats by deploying the most appropriate security measures, countermeasures, and policies.

4.3 Maintenance

It is important to identify the types of maintenance to be performed on various assets and who will perform the maintenance. An organization should establish methods for upgrades and technology insertions. Also, agencies should have plans for post-development hardware and software support requirements. Other best practices include:

- Describing the approach to supply field operators and maintenance technicians with necessary tools, spares, diagnostic equipment, and manuals;
- Defining the standard support equipment to be used by the system. Discuss any need for special test equipment or software development environment; and
- Training users to be capable of using the proposed system; and
- Describing how the system will be transported to the field, identifying any constraints. Identify facilities needed for staging and training.

4.4 Force Structure

An agency's security force structure will be determined by the number of posts (i.e., manpower) and protective systems/sub-systems (i.e., physical/electronic security systems) needed, including the number of monitoring stations and training units. Organizations and units that will employ the systems being developed and procured should be identified, estimating the number of users in each organization or unit.

4.5 Schedule

To the degree that scheduling is a requirement, define target dates for system availability. If a distinction is made between initial capability and full operational capability, clarify the difference between the two in terms of system capability and/or numbers of fielded systems.

4.6 Resource Affordability

Ensure the budget allows for any costs incurred supporting a proposed resource purchase (i.e., "first-costs" such as jack installation for new computers). Once a budget has been established, it is essential to continually test the viability of its assumptions by employing cost management. If the resource was not included in the budget, the CFO and Contracting Officer should be consulted regarding the procurement of resources.

When procuring or disposing of resources, the following questions should first be considered:

- Is it good for the customer?
- Are the right people involved?
- Is it cost-effective?
- Does it mitigate risk?
- Who is taking ownership?

4.7 Personnel

Adequate manpower is essential to the success of any security-in-depth plan[16]. Therefore, organization leaders must ensure they have the necessary personnel to assess, plan, and manage the security operations for their organization. Security-in-depth can reduce the overall need for manpower by deterring an attack through visual countermeasures, delaying overall entry time to a facility by an assailant, or creating physical barriers to deny unauthorized access.

Security manpower includes professionals (i.e., full-time PSOs) and those assigned specific security duties (e.g., escort duties) on other than a full-time basis. It should be emphasized to all employees that they are directly responsible for securing organizational property and information in their work area and for property they have signed for or under their direct control.

Security functions can be performed by government employees, law enforcement officers, civilians, contractors, or military personnel. However, it would be prudent to engage with the agency's human resource office and legal counsel to identify whether the security functions are inherently governmental. Key considerations in determining manpower composition and numbers include:

- Identifying the areas, buildings, and other structures in the organization. Further, identify those resources and structures considered high value or mission essential, and establish parameters and priorities for their protection.
- Identifying the organization's authorities, mission(s), roles and responsibilities.
- Identifying the number of persons (civilian or military) required, the ranks and grades for each, and providing a brief duty description for each, if there are functions that are inherently governmental. If a function is not inherently governmental and contract support is authorized, providing a brief description of responsibilities (statement of work) and identifying any special clauses that may pertain to the function, and coordinate with the organization's contracting officer.
- Considering whether the organization will need to conduct outreach and training, to include periodic security awareness days. Establishing and managing a capability to conduct and track (e.g., via a learning management system) mandatory annual and refresher security training will likely require full-time personnel.
- Considering resources for periodic security management meetings that include all organizational locations. Teleconferencing capabilities are viable options for including personnel teleworking.
- Identifying/planning for PSOs to patrol facilities; conducting personnel, vehicle, and package searches; accessing control badging and screening; monitoring alarms; and

[16] DoD 5200.08-R, April 9, 2007 - Physical Security Program https://fas.org/irp/doddir/dod/5200_08r.pdf

response. General instructions that apply to the PSO personnel (fixed site or mobile patrols) should be developed. Ensuring detailed instructions, such as special orders information, are included in plans and that PSOs are familiar with these orders. Other essential items to consider for security personnel that impact staffing requirements include:

  - Composition and organization of the force;
  - Essential posts and routes;
  - Weapons and personal protective equipment;
  - Training and certifications;
  - Specialized Requirements (e.g., explosive detection or patrol);
  - Communications equipment; and
  - Transport.

- Establishing plans for contingency scenarios, including emergencies. This should include detailed response plans to all-hazard events. Items to consider include:
  - Individual actions;
  - Security force actions; and
  - Emergency management personnel actions.
- Coordinating with other entities or offices to facilitate mutual support agreements in emergencies, such as:
  - Other Federal agencies;
  - State and local agencies;
  - Military installations; and
  - Private industry.

4.8 Contracts

In some cases, an agency or department may choose to fill security positions using contract employees. Additional scrutiny and detail is necessary for those contracts supporting the security mission. This is true for both the Federal leadership overseeing the contract and for the company fulfilling it. At a minimum, contractors must meet all Federal, State, and/or local employment statutes and, if they will be armed, licensing and liability insurance requirements. Moreover, resource considerations must be made for all critical tasks assigned to contract protective security officers including, but not limited to: equipment, uniform, and training.[17] It is mandated within GSA controlled/leased space that all contract guards be vetted through FPS; in space independently leased by a Federal department/agency, it is recommended that the lessor adhere to established internal department/agency policies and ISC best practices.

[17] Interagency Security Committee, *Best Practices for Armed Security Officers in Federal Facilities*

The statement of work for each contract should discuss the goods/services the contract will provide, where the goods/services will be provided, when the goods/services will be provided, etc. It is also important to review the threat assessment for the facility as it relates to contract security staff. The assessment should specifically consider the likelihood of the potential risk posed by insider threats associated with granting contractor personnel access to the unit area, personnel, and equipment. Also, the threat assessment must consider the likelihood of threats directed against contractor personnel providing goods and services. Key items for consideration from both the contracting and Federal perspectives include:

- What is the FSL of the site where the contract will be performed?
- What is the criminal threat level where contract will be performed?
- How reliable are the contractor personnel? Are contractor personnel cleared/vetted/US citizens?
- Has the contractor been noncompliant with security directives on previous contracts?
- Will the contract be performed at or near mission critical facility/capability locations?
- Can contractors gain unauthorized access to critical areas/locations?
- What facility areas have/require controlled access?
- Is the contracted service critical to the organization's mission? Would delay/loss of contracted service have a critical effect on the mission?
- Is the contractor working with personnel, systems or materials that are mission essential, sensitive, or high value?
- What sensitive information can contractor personnel gain knowledge of in performance of their duties?
- Does the request for proposals/statement of work contain controlled unclassified information?
- What materials/equipment does the contractor need in order to meet contract requirements?
- Does the contractor require supporting equipment/vehicles, or just personally carried items?
- Does the contractor require access to sensitive areas to perform duties?
- Will contractor personnel have access to hazardous materials (e.g., fuel, ammunition, medical waste, etc.)?
- Are there existing access control procedures sufficient to ensure contractor personnel are properly identified/authorized/limited?
- Will contract PSOs be deemed essential personnel during contingency situations for continuity of operations (COOP) purposes?
- Will contract personnel be awarded hazard pay?
- What will the procedures be for reporting security violations? What corrective actions will be taken?

5 Physical Security Equipment

This section discusses and provides best practices for use in planning and managing Federal agencies' physical security resources. The ISC *Risk Management Process for Federal Facilities* Standard defines the criteria and processes that those responsible for the security of a Federal facility should use to determine the facility security level and provide an integrated, single source of physical security countermeasures for all non-military Federal facilities. The Standard also provides guidance for customization of security countermeasures.

The theory and application of physical protection systems includes the functions of deterring, detection, delay, and response. Physical security involves security-in-depth, the use of multiple layers of interdependent systems such as physical barriers, IDS, CCTV surveillance, security guards, access control, lighting, etc. These techniques are designed to detect, deter, delay and/or deny unauthorized access to facilities, equipment, and resources.

Accordingly, best practices should be considered in the planning and management of physical security resources for the protection of Federal facilities. Emphasis should be placed on allocating security resources using risk management, leveraging of the capabilities of security technology, coordinating protection efforts and sharing information with other stakeholders. In addition, security managers should also measure performance and test security initiatives, assign assets in alignment with the agency mission, and strategically manage physical security related human resource and budget resources.

Managing physical security resources is a holistic process which includes strategic planning, identifying goals and performance objectives, as well as justifying and applying a realistic budget for a comprehensive security program. One best practice is to centrally manage physical security through a Director of Security or CSO with agency-wide responsibilities for the agency's physical security vision, strategy, programs, and related matters. The Director of Security should be responsible for developing and implementing the agency-wide security program, with authority to take critical physical security resource allocation needs to the agency head or other appropriate executive leadership official(s) for support and approval. The central management of such functions may not be feasible at some agencies due to various factors, but security functions should be consolidated to the greatest extent possible.

As a best practice to ensure adequate security for Federal facilities, agencies should carefully weigh the benefit of each identified security countermeasure for their facility/facilities based on a comprehensive security risk assessment and allocate resources in accordance with their most productive use. However, the allocation of resources often involves budget constraints and other complexities. Generally, there are physical security resource allocation issues related to agency organizations, processes, and tools that hinder the alignment of agency spending to support all recommended security countermeasures.

The agency's Director of Security and its designated security organization should assess, define and utilize a process for determining the customized security measures required at a specific Federal facility. The responsible security organization should conduct appropriate risk assessments and provide a report with recommendations to the Facility Security Committee. The Director of Security and the chairperson of the FSC should clearly articulate how a holistic and comprehensive physical security program contributes to the success of the agency and its mission, and take the appropriate implementation actions in accordance with ISC standards.

There is no single set of best practices that is applicable to all facilities. For some facilities there are clear physical security best practices and allocation of resources. A non-law-enforcement Federal agency in a single GSA-owned, -leased or -operated facility with a 50 foot set-back (i.e., standoff distance) may require basic security countermeasures to meet ISC standards. In contrast, several Federal agencies and commercial tenants in a multi-tenant facility may require security countermeasures that are quite complicated and the allocation of resources may be challenging due to the sharing of space and systems, as well as collaborative decision making for security and safety measures, and associated pro-rated costs. Pro-rated cost determinations and decisions are made by the FSC, as outlined in the *Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*.

Physical security programs address how agencies' internal security offices and their security organization approach various aspects of physical security for Federal facilities. The security organization is responsible for conducting vulnerability and risk assessments to identify threats and vulnerabilities, determining which countermeasures to implement, and coordinating security efforts within the agency and with other agencies, as applicable. The internal security office and/or FSC will review the risk assessment report and make decisions regarding the acceptance, modification, non-acceptance of recommendations, and the acceptance of risk if recommended measures cannot be met.

Due to the differences among agencies, there is no single ideal approach to physical security. Agencies generally use a range of management practices to oversee physical security and should also rely on the institutional knowledge of their security specialists, Federal Protective Service (FPS), and GSA to effectively and efficiently allocate resources.

The *ISC Security Specialist Competencies Guideline*[18] provides a range of competencies that Federal security specialists should possess to perform their basic duties and responsibilities in the following areas:

- Physical barriers;
- Intrusion detection systems;
- Access control systems;

[18]Please reference http://www.dhs.gov/interagency-security-committee-standards-and-best-practices

- CCTV;
- Biometrics;
- Protective lighting;
- Security barriers;
- Storage safes;
- Security locks and locking devices;
- Crime prevention and security awareness;
- Security force specification and management; and
- Security inspection systems.

These physical security countermeasures are described in detail in the *ISC Security Specialist Competencies Guideline*. In addition, other ISC standards and best practice guidance, as well as the institutional knowledge of security and facilities specialists, can be used to implement security policies to meet ISC and other applicable standards (i.e., agency-specific, State and local codes, etc.).

The information outlined in the following sections highlights some best practices in the areas of physical security resource management, including concepts, planning, acquisition, operation and maintenance, and the disposal of physical security resources.

5.1 Key Concepts in Physical Security Resource Management

- Physical security programs should be holistic and the allocation of resources should be integrated into the agency's mission, objectives, goals, and budget process.
- Physical security functions should be consolidated within an internal security office, led by a Director of Security (i.e., CSO), who reports to a high ranking senior executive official who has ready access to the agency head, as needed.
- Director of Security (i.e., CSO) should be responsible for managing and allocating physical resources based on risk assessments and using performance measures to justify security resources across the agency's portfolio of facilities.
- Development and implementation of the physical security program should involve collaboration among top agency management, security, facilities management, emergency preparedness, budget, health and safety specialists, and other stakeholders.
- Physical security programs should be aligned with the agency's mission, strategic goals and multi-year budget cycle.
- Physical security programs should meet the cost-effective expectations of the agency leadership in terms of totally integrated security support and safety services rendered.
- Physical security programs and countermeasures should be balanced with other operational needs and competing interests.

- Physical security resource allocation should be periodically assessed, including historical spending records, which may be useful in future resource allocation considerations.

5.2 Planning for Physical Security Resources

- Outline key steps in the planning process to request physical security resources.
- Coordinate security risk assessments with the security organization, GSA, and other Federal tenants (if applicable) to reduce any unnecessary duplication in the conduct of security assessments of facilities.
- Ensure that all facilities are covered by a baseline level of physical security to adequately address risks identified in the RMP.
- Develop linkages among agency's physical security plan, strategic plan, and budget.
- Develop a physical security resource management plan with identified resource needs and evaluate different options to address priority needs.
- Develop and maintain critical skills, staffing and training to assist in the best allocation and utilization of physical security resources.
- Involve physical security professionals and key stakeholders in strategic planning efforts.
- Identify external resources, such as other agency experts, contractors, and/ or consultants, as necessary, when developing plans.
- Participate in a comprehensive review of security master plan development and implementation.
- Balance the need for improved security with other operational needs and competing interests, obtain funding for security technologies and personnel, and balance the funding process with changing security needs.
- Develop projected plans to time and prioritize resource allocation decisions, especially if the budget cycle spans multiple years.
- Allocate security resources using risk management, leveraging the use of security technology, coordinating protection efforts and sharing information with other stakeholders.
- Measure program performance and test security initiatives, aligning assets to mission, and strategically managing human resources.
- Evaluate the cost-effectiveness and efficiency of technologies.
- Use consistent approaches to physical security for similar facilities.
- Incorporate physical security measures that are as aesthetically pleasing as practicable and that blend with the environment, incorporating Crime Prevention through Environment Design (CPTED) measures.

5.3 Physical Security Asset Acquisition

- Identify and employ personnel with institutional knowledge and subject matter expertise in physical security as a primary resource.

- Develop a professional security staff through enhanced selection, retention and training programs.
- Determine asset life-cycle costs.
- Develop a strategic plan for acquiring assets, to include all stakeholders.
- Facilitate budget formulation and execution through the planning, budgeting, and performance management process and contract management activities for the agency.
- Use in-house software, if available.
- Look first for shared services that can be acquired through interagency/reimbursable agreements before independently acquiring or developing new solutions. Acquire new software for physical security resources only after confirming that cost-effective in-house or shared services are not available.
- Benchmark physical security measures and resources with other agencies and industry.
- Establish and maintain an inventory of employee skills and competencies; have a process to address skills/competency gaps; and have devolution and/or transition plans for leadership and other critical positions.
- Build the capability needed to address administrative, educational (i.e., training), and other human resource requirements to support physical security planning strategies.
- Leverage existing infrastructure and resources by ensuring that there is a balance between physical security and safety, and that all requirements for both are met.
- Develop a contingency plan to fund security measures to address newly identified security deficiencies which had not been budgeted for in the fiscal year.
- Use risk mitigation and/or risk acceptance decisions made by the Designated Official/Chair of Facilities Security Committee if there are insufficient budgetary resources to support the security requirements identified as a result of a risk assessment of a facility.

5.4 Operation and Maintenance of Physical Security Resources

- Develop policies to ensure appropriate use of assets.
- Implement an appropriate asset maintenance plan.
- Determine the value of assets.
- Transition and upgrade legacy systems in a cost-effective manner.
- Assess and determine the benefits of prudent management of security life-cycle systems and component replacement for physical security resources.
- Consult and share with other others, especially those with similar missions and facilities, to gain insight into best practices and emerging trends.
- Conduct performance measurement of physical security related human resources, technical resources, and operating systems.

5.5 Disposal of Physical Security Resources

- Consult agency policy and/or asset managers to determine how and when physical security assets should be disposed.
- Dispose of assets safely:
    - Repurpose
    - Donate systems or components
- Communicate the disposition of physical security resources through interactions with internal partner organizations and external agency stakeholders.
- Conduct periodic self-assessment audits of physical security programs.

5.6 Security-Related Information Technology Systems

Understanding current information technology capabilities and constraints, coupled with start-to-finish considerations for physical security/IT integration is integral to effective physical security resource management and planning. A thorough understanding of existing environmental, operational or system-centric limiting factors (e.g., antiquated or incompatible software or hardware, which may include logical access components, networking parameters and residual/unintended effects of increased bandwidth on Local Area Networks, the process of acquisition of authority to operate (ATO), insufficient power or cabling, etc.) will preempt potential design or engineering oversights. As discussed in Section 6.1 of this document, physical security and IT system integration must also be factored into all project deliberations to reduce potential gaps and vulnerabilities, while maximizing resource procurement and allocation.

5.7 Personal Protective Equipment

Organizations must provide appropriate personal protective equipment (PPE) to their employees and ensure they are trained in the proper use, wear, maintenance, storage, and disposal. Before procuring any personal protective equipment two things must be considered: the equipment's intended use and the type of environment it is to be worn and used in. All PPE must meet or conform to required Federal, State, and/or local standards and be of safe design, construction, fit well, and should be maintained in a clean and reliable fashion.[19] The organization should also research and budget for the life-cycle costs of the equipment (purchase, training, maintenance, storage/shelf life, and disposal), as well as understand compatibility issues with any equipment to be used in conjunction with other PPE.

5.8 Organizational Equipment

Agencies should identify equipment that would provide adequate protection when planning and managing physical security resources. Agencies should also consider the maintenance, cost, and

[19] Interagency Security Committee, *Best Practices for Armed Security Officers in Federal Facilities*

life-cycle of their equipment used in their facilities. Employees should receive training before using the equipment. Management should be assured that each employee has an understanding and the ability to properly wear and/or operate the specific equipment before using. Employees should receive re-training if a supervisor believes that the individual is not demonstrating the proper understanding and skill level in the use or operation of the equipment.

When purchasing organizational equipment a proper understanding of the life-cycle costs of the equipment/systems is necessary, to include: procurement, installation, maintenance, training, and disposal. The organization also needs to consider/anticipate future requirements. The capability of current equipment/systems to be expanded (i.e., add CCTV to current surveillance system), and the compatibility/non-compatibility with emerging technologies (expansion vs. replacement).

5.9 Training & Certification

Proper allocation of training budgets and resources requires fundamental and important decisions. As a result, agencies should focus on programs that maximize training investment and demonstrate value. Otherwise, limited resources may be improperly invested in programs that have minimal impact on the organization's missions/goals.

Some considerations to include when planning and managing physical security resources for training and certification programs:

- Identify how training program funding decisions could be enhanced within the agency.
- Outline how budget and resources could be allocated to most effectively address performance deficiencies and mitigate known or anticipated threats.
- Define how spending could be prioritized proactively to deal with the constant challenge of new products, regulations and initiatives that require training.
- Establish links between training activities and missions/goals and explain why training is needed.
- Describe how training should address specific performance deficiencies needed to achieve overall organizational goals.

5.10 Life-Cycle Management

Property accountability and management promotes operational efficiency and encourages adherence to prescribed managerial policies, and supports the organization's plan to safeguard its assets by establishing internal controls. All persons entrusted with government property must be made aware of and understand their responsibilities, which include proper care and stewardship, as well as potential legal and financial ramifications for misuse or loss.

Accountability and management of equipment and systems supporting the physical security program is critical. All property acquired, leased, or otherwise obtained should be managed

throughout the asset's life-cycle: from initial acquisition and receipt, through accountability and custody, until formally relieved of accountability by authorized means, including disposition, or through a completed evaluation and investigation for property loss.

Equipment and systems to be considered for inclusion in a property management system include: badging and access control systems, locks, mobile barriers, weapons, vehicles, communication devices and systems, intrusion detection systems, x-ray equipment, magnetometers, civilian working dogs, CCTV, security containers, and sensors.

An automated property management system provides: the ability to prioritize replacements based on the age of the equipment, a tracking mechanism for associated maintenance contracts and training costs, methods to easily identify what equipment is available for cross-leveling to support the security of a higher priority asset/facility, and the capability to identify where an individual piece of equipment is located and who is responsible for it. If the agency does not possess an automated property management system, the division should manually maintain an electronic inventory of physical security assets to include value, recipient, location, condition, quantity, etc. The Director of Security (i.e., CSO or top security executive) should also consider requesting that an automated system be established through the appropriate officials within the agency.

Equipment and systems should be accounted for by name, part number, description, model number, and national stock number (NSN). If an NSN does not exist on the GSA schedule, coordinate with the appropriate logistics/property managers to have one created. Some equipment and systems have multiple components. An agency should have the capability to track an item by the component, as well as the overall piece of equipment or system. That way if there is a defective part, it can easily be identified by component, as well as establish priorities and timelines for repairs and replacements.

6 Resource Integration

Incorporating physical and information security is a key element to managing and planning physical security resources. Integration helps to provide important insight because it assimilates two mechanisms previously known to be compatible but separate. These security functions help to provide risk awareness, set strategies and policies, collaborate and develop security plans, and put such plans into effect. Agencies identifying and assessing previously unknown risks could benefit from the management and planning of security resources, which is a vital capability in establishing physical/information security integration.

6.1 Physical Security/Information Technology Integration

Organizational failure to properly integrate and align traditional physical security approaches, IT projects, systems and components significantly increases the possibility for redundancy in programmatic efforts. It can also create gaps or perpetuate existing vulnerabilities in the

organization's security construct. Moreover, lack of integration between the systems can result in the under-utilization of existing or new capabilities. To ensure success as a management-driven effort, organizational leaders must ensure close and continual collaboration and coordination between organizational security offices and information technology entities/offices.

Accomplishing convergence – ensuring proper resource appropriation, fiscal stewardship, allocation, and implementation of an effective multi-disciplined, technologically-integrated layered-security approach – requires a non-negotiable focus on and dedication to design by committee/subject matter experts (SMEs). All new construction projects, facility upgrades, security enhancements and technology upgrades must take into consideration tangential (even if previously unidentified) opportunities for value added and integration (and conversely, potential for redundancy and detrimental resource utilization/under-utilization).

Requirements and capabilities training is a key variable in promoting and advancing the idea of convergence. Regular collaboration between traditional security and IT professionals will identify gaps and engender technical discussions on opportunities for collaboration. Educating senior organizational leaders/decision-makers in basic security and IT concepts, advancements and trends, and highlighting integration efforts and successes serves to reinforce the necessity for multi-faceted project review processes.

In organizations where convergence proves to be very difficult to implement on a large scale, professionals from both disciplines are encouraged to engage in a high visibility/high return on investment (ROI) inaugural integration endeavor.

As an example, a plausible, "ground-floor" yet critical integration effort may include moving towards the centralized management of data entry and provisioning or credentialing processes. Utilizing a single point of institutional entry (PIE) shared software application, centralized initial personnel tracking and servicing (HR, payroll, benefits, etc.) data entry, issuance of facility physical access credentials or badges, and granting of IT-based privileges (logical access) eliminates administrative redundancies, increases operational effectiveness and reduces potential vulnerabilities by enhancing an organization's common operating picture (COP) and common operating environment (COE).

Successfully implemented and managed, the results of most integration efforts will prove immediately (or in the near-term) tangible and beneficial both to the individual employee and the organization. In support of "socialization"/advertising efforts and optimally reducing cultural resistance to future integration efforts, both are acceptable outcomes.

Appropriate physical security/information technology systems collect and correlate events from existing security devices and information systems to allow PSOs to identify and proactively resolve potentially harmful situations. Physical security information technology integration enables numerous organizational benefits, including increased control, improved situational awareness and management reporting. Ultimately, the appropriate physical security information

technology integration helps organizations to reduce costs through improved efficiency and to improve security through increased intelligence.

A complete physical security information technology integration software system encompasses six vital capabilities:

1. Collection: Device management independent software collects data from any number of disparate security devices or systems.
2. Analysis: The system analyzes and correlates the data, events, and alarms to identify the real situations and their priority.
3. Verification: Physical security information technology software presents the relevant situation information in a quick and comprehensible format for an operator to verify the situation.
4. Resolution: The system provides standard operating procedures (SOP), step-by-step instructions based on best practices and an organization's policies, and tools to resolve the situation.
5. Reporting: The physical security information technology software tracks all of the information and steps for compliance reporting, training and potentially in-depth investigative analysis.
6. Audit trail: The physical security information technology software also monitors how each operator interacts with the system, tracks any manual changes to security systems and data and calculates reaction times for each event.

7 References

- Department of Homeland Security, Protective Services of FPS: https://www.dhs.gov/federal-protective-service-0
- GAO-13-222 Report "Facility Security - Greater Outreach by DHS on Standards and Management Practices Could Benefit Federal Agencies"
- Interagency Security Committee, *Best Practices for Armed Security Officers in Federal Facilities*
- Interagency Security Committee, *Security Specialist Competencies: An Interagency Security Committee Guideline*
- Interagency Security Committee, *The Design-Basis Threat: An Interagency Security Report*
- Interagency Security Committee, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*
- NIST Special Publication 800-18 Revision 1 Guide for "Developing Security Plans for Federal Information Systems"
- Office of Personnel Management Position Classification Standard For Security Administration Series, GS-0080
- GAO-15-444 Report "HOMELAND SECURITY: Action Needed to Better Assess Cost-Effectiveness of Security Enhancements at Federal Facilities"
- DoD 5200.08-R, April 9, 2007 - Physical Security Program https://fas.org/irp/doddir/dod/5200_08r.pdf

8 Resources

- NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security, Revision 2: Initial Public Draft
- GSA Pricing Desk Guide, 4th Edition
- National Institute of Building Sciences, Whole Building Design Guide, DOD Criteria: http://www.wbdg.org/references/pa_dod.php
- Reed Construction Data, RSMeans Business Solutions: http://www.rsmeans.com/consulting/index.asp
- Unified Facilities Criteria (UFC) DoD MINIMUM ANTITERRORISM STANDARDS FOR BUILDINGS, UFC 4-010-01 9 February 2012, Change 1, 1 October 2013 http://www.wbdg.org/ccb/DOD/UFC/ufc_4_010_01.pdf
- Deputy Secretary of Defense Memorandum – Antiterrorism Building Standards for Leased Space, December 7, 2012

Interagency Security Committee Participants

ISC Chair
Caitlin Durkovich
Assistant Secretary for Infrastructure Protection
U.S. Department of Homeland Security

ISC Acting Executive Director
Bernard Holt
Interagency Security Committee

Working Group Chair
Elvis Chase
Office of Personnel Management

Working Group Members
Victor Nettles
Federal Protective Service

Calvin Byrd
Nuclear Regulatory Commission

Andrew Daub
Department of Defense/ U.S. Transportation Command

Wandra Nickson
Department of Defense/Defense Information Systems Agency

Donna Rivera
Department of Defense/Office of Under Secretary of Defense

Mike Hanson
Department of Defense/Department of the Navy

Anthony Evernham
Interagency Security Committee

Lindsey Blair
Interagency Security Committee

Antonio Reynolds Sr.
Interagency Security Committee

Megan K. Drohan
Interagency Security Committee

List of Abbreviations/Acronyms/Initializations

TERM	DEFINITION
ATO	Authority to Operate
CCTV	Closed-Circuit Television
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CIO	Chief Information Officer
COE	Common Operating Environment
COP	Common Operating Picture
COOP	Continuity of Operations
CPTED	Crime Prevention through Environment Design
CSO	Chief Security Officer
DBT	Design Basis Threat
DHS	Department of Homeland Security
DO	Designated Official
EO	Executive Order
FPS	Federal Protective Service
FSC	Facility Security Committee
FSL	Facility Security Level
GAO	Government Accountability Office
GSA	General Services Administration
HR	Human Resource
IDS	Intrusion Detection System
ISC	Interagency Security Committee
IT	Information Technology
LOP	Level of Protection
NSN	National Stock Number
PIE	Point of Institutional Entry
PLM	Product Life-cycle Management
PPE	Personal Protective Equipment
PSO	Protective Security Officer
RMP	Risk Management Process
ROI	Return on Investment
SME	Subject Matter Expert
SOP	Standard Operating Procedures
USC	United States Code

Glossary of Terms

TERM	DEFINITION
Access Control	For the purposes of this document, any combination of barriers, gates, electronic security equipment, and/or guards that can deny entry to unauthorized personnel or vehicles.
Aggressor	Any person seeking to compromise an asset. Aggressor categories include protesters, criminals, terrorists, and subversives.
Asset	A resource requiring protection
Asset Value Rating	A measurement of the importance of an asset to its user.
Baseline Level of Protection	The degree of security provided by the set of countermeasures for each Facility Security Level that must be implemented unless a deviation (up or down) is justified by a risk assessment.
Closed Circuit Television	A television system in which signals are transmitted from a television camera to the receivers by cables or telephone links.
Crime Prevention through Environment Design	The proper design and effective use of the built environment that can lead to a reduction in the fear and incidence of crime and an improvement in the quality of life.
Critical Asset	Any facility, equipment, service or resource considered essential to agency operations in peace, crisis, and war and warranting measures and precautions to ensure its continued efficient operation, protection from disruption, degradation, or destruction, and timely restoration. Critical assets may be government or private assets (industrial or infrastructure critical assets), domestic or foreign, whose disruption or loss would render critical assets ineffective or otherwise seriously disrupt operations. Critical assets include traditional "physical" facilities and equipment, non-physical assets (such as software systems), or "assets" that are distributed in nature (such as command and control networks, wide area networks or similar computer-based networks).
Critical Infrastructure	Infrastructure deemed essential to agency operations or the functioning of a Critical Asset.
Design-Basis Threat	The threat upon which a system of countermeasures protecting assets is based. The design-basis threat includes the aggressor tactics and the associated weapons, explosives, tools, and agents.

Design Criteria	For the purposes of this document, the basis for defining a protective system that mitigates vulnerabilities to assets. Design criteria include assets, threats, levels of protection, and design constraints.
Designated Official	The highest ranking official of the primary occupant agency of a Federal facility, or alternatively, a designee selected by mutual agreement of tenant agency officials.
Equipment	As part of a protective system, countermeasures such as electronic security system elements and other devices used by personnel for detection and assessment of threats or weapons tools, explosives, or chemical, biological, or radiological agents.
Facility Security Committee	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.
Facility Security Committee Chairperson	The primary tenant's senior representative or designated senior staff member with decision making authority.
Facility Security Level	A categorization based on the analysis of several security-related facility factors, which serves as the basis for the implementation of physical security measures specified in ISC standards.
General Design Strategy	The basic approach to developing a protective system to mitigate the effects of a given tactic. It governs the general application of construction, building support systems, equipment, manpower, and procedures.
Intrusion Detection System	A device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.
Level of Protection	The degree to which an asset (e.g., a person, a piece of equipment, or a mission, etc.) is protected against injury or damage from an attack.
Level of Risk	The combined measure of the threat, vulnerability, and consequence posed to a facility from a specified undesirable event.
Likelihood Rating	Measures how likely an aggressor is to attempt to compromise a given asset.
Local Area Networks	A group of computers and associated devices that share a common communications line or wireless link.

Manage or Managing	To succeed in accomplishing or achieving, especially with difficulty; contrive or arrange
Manpower	Countermeasures that relate to the use of guards or other personnel necessary to implement or operate elements of the protective system.
Metropolitan Area Networks	A network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network but smaller than the area covered by a wide area network.
Operational Capability	The process of determining current operational requirements and the development of future mission capabilities, given the strategic and operational objectives of an agency.
Plan or Planning	The establishment of goals, policies, and procedures for a social or economic unit.
Primary Tenant	The Federal tenant identified by Bureau Code in Office of Management and Budget Circular No. A-11, Appendix C, occupies the largest amount of rentable space in a Federal facility.
Procedures	Countermeasures that relate to actions taken by people, including guards and building occupants, to implement or operate elements of the protective system.
Protective Effectiveness Factor	Reflects the effectiveness of countermeasures in mitigating the vulnerabilities associated with a given threat.
Protective System	An integrated system of countermeasures designed to protect assets against threats to specific levels of protection. Protective systems include building elements, site work elements, equipment, and manpower and procedures.
Resource Allocation	A plan for using available resources in an economic way, to achieve goals for the future.
Risk	A measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence. Potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences; potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence.
Risk Acceptance	The explicit or implicit decision not to take an action that would affect all or part of a particular risk.
Risk Analysis	The process of determining risk levels for assets.
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. The process of evaluating how changes in countermeasures application affect risk levels and costs for the purpose of decision making.
Risk Mitigation	The application of strategies and countermeasures to reduce the threat of, vulnerability to, and/or consequences from an undesirable event.
Security-in-Depth	A determination by the senior agency official that a facility's security program consists of layered and complimentary security controls sufficient to deter, detect, and document unauthorized entry and movement within the facility.
Security Organization	The government agency or an internal agency component either identified by statute, interagency memorandum of understanding /memorandum of agreement or policy responsible for physical security for the specific facility.
Site-work Elements	Countermeasures that are applied beyond 1.5 meters (5 feet) from a building, excluding countermeasures categorized under equipment.
Standard Operating Procedure	Established or prescribed methods to be followed routinely for the performance of designated operations or in designated situations.
Subject Matter Expert	A person with bona fide expert knowledge about what it takes to do a particular job.
Tactics	The specific methods of achieving the aggressor's goals to injure personnel, destroy assets, or steal material or information.
Threat	The intention and capability of an adversary to initiate an undesirable event.
Threat Effectiveness Rating	Reflects the capabilities of aggressors to find weaknesses in security measures and to exploit them considering their sophistication, motivation, and risk acceptance.
Undesirable Event	An incident that has an adverse impact on the facility occupants or visitors, operation of the facility, or mission of the agency.
Vulnerability	A 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.
Wide Area Networks	A computer network in which the computers connected may be far apart, generally having a radius of half a mile or more.

This page left intentionally blank.