Presidential Policy Directive 21 Implementation:

An Interagency Security Committee White Paper

February 2015

Interagency Security Committee

This page intentionally left blank.

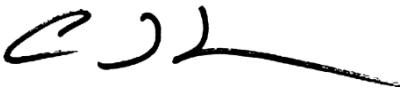
Message from the Interagency Security Committee Executive Director

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

As Executive Director of the ISC, I am pleased to introduce the new ISC document titled *Presidential Policy Directive 21 Implementation: An Interagency Security Committee White Paper* (White Paper). This ISC White Paper aims to evaluate the efficacy of current ISC facility screening criteria against Presidential Policy Directive 21: *Critical Infrastructure Security and Resilience* (PPD-21) requirements in an effort to execute the President's vision..

Consistent with Executive Order 12977 (October 19, 1995), *Presidential Policy Directive 21 Implementation: An Interagency Security Committee White Paper* is intended to be applied to all buildings and facilities in the United States occupied by Federal employees for nonmilitary activities. These include existing owned, to be purchased or leased facilities; stand-alone facilities; Federal campuses; individual facilities on Federal campuses; and special-use facilities.

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



Austin Smith

Executive Director, Interagency Security Committee

This page intentionally left blank.

Table of Contents

Message from the Interagency Security Committee Executive Director iii

1 Background, Scope, and Authority 1

1.1 Background 1

1.2 Scope 1

1.3 Authority 2

2 Analysis 1

3 Recommended Approach 3

3.1 Assessment Methodology 3

3.2 Threat Identification and Mitigation 3

3.2.1 Threat Definition 3

3.2.2 Countermeasures Development 4

3.3 Facility Security Level Determination 5

3.4 Compliance 5

3.5 Training 5

4 Administration 6

List of Abbreviations/Acronyms/Initializations 7

Glossary of Terms 8

Interagency Security Committee Participants 9

1 Background, Scope, and Authority

1.1 Background

Presidential Policy Directive 21: *Critical Infrastructure Security and Resilience* (PPD-21), released on February 12, 2013, states the Federal government has a responsibility to strengthen the security and resilience of its own critical infrastructure against both physical and cyber threats. It further states that "…all Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and security of their respective internal critical infrastructure that supports primary mission essential functions."

Following the release of PPD-21 and Executive Order (EO) 13636: *Improving Critical Infrastructure Cybersecurity*, the Interagency Security Committee (ISC) established a working group to review *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* and evaluate its effectiveness pertinent to strengthening the security and resilience of Federal critical infrastructure. The Working Group evaluated the efficacy of current ISC facility screening criteria against PPD-21 requirements in an effort to execute the President's vision. It used the updated and overarching national policy found in PPD-21 and EO 13636 acknowledging the increased role of cybersecurity in securing physical assets.

On May 8, 2013, the ISC convened the PPD-21 Working Group consisting of representatives from the following organizations:

- General Services Administration (GSA)
- Department of Homeland Security (DHS)/Cybersecurity and Communications (CS&C)
- DHS/Science and Technology (S&T)
- DHS/Operations (OPS)
- DHS/Federal Protective Service (FPS)
- Central Intelligence Agency (CIA)
- Department of Transportation (DOT)
- DOT/Federal Aviation Administration (FAA)
- Smithsonian Institution (SI)

1.2 Scope

This white paper provides a current assessment of issues addressed with the release of PPD-21 which addresses cyber threats in relation to physical security measures for Federal facilities.

The Working Group was charged with evaluating security criteria for Federal critical infrastructure supporting mission-essential functions to meet PPD-21 requirements for security and resilience, coordinating with the Integrated Task Force (ITF), and creating a strategy for compliance.

1.3 Authority

Executive Order (EO) 12977, the order establishing the Interagency Security Committee, outlined the role and scope of the ISC. Within the context of EO 12977, the ISC is charged with and given authority to "…develop and evaluate standards for Federal facilities, develop a strategy for ensuring compliance with such standards, and oversee the implementation of appropriate security measures in Federal facilities…"[1]

Within the scope of overseeing the implementation of security standards, the Order went on to encourage agencies and departments within the Federal government to lend assistance to and comply with the standards set forth by the ISC. Furthermore, EO 12977 granted authority to the Interagency Security Committee, stating "…each executive agency and department shall cooperate and comply with the policies and recommendations of the Committee issued pursuant to this order...." [2] It further orders "the Administrator shall be responsible for monitoring Federal agency compliance with the policies and recommendations of the Committee".[3] The authority to administer the ISC has since been delegated to the Secretary of the Department of Homeland Security[4].

Based upon the authority of EO 12977, the ISC has developed an approach to assist Federal agencies in complying not only with the original EO 12977 but with the updated requirements of PPD-21. In the nearly 20-year history of the Interagency Security Committee, many of the best practices and standards have been employed by numerous agencies within the Federal government. Thus, the ISC is in a unique position to help lead this effort.

[1] Executive Order 12977: Interagency Security Committee, Sec. 5(a)(2).

[2] Executive Order 12977: Interagency Security Committee, Sec. 6(b).

[3] Executive Order 12977: Interagency Security Committee, Sec. 6(c).

[4] Executive Order 13286: Amendment of Executive Orders and Other Actions, Sec. 23.

2 Analysis

The PPD-21 Working Group analyzed *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (RMP) to identify any issues that could create vulnerabilities or obstacles to security and resilience efforts for Federal facilities supporting primary mission essential functions (PMEF) in an all hazards environment. As noted in the 2014 Department of Homeland Security Quadrennial Review (QHSR):

> The Nation's critical infrastructure provides the essential services that underpin the American way of life. The concept of critical infrastructure as discrete, physical assets has become outdated as everything becomes linked to cyberspace. This "cyber-physical convergence" has changed the risks to critical infrastructure in sectors ranging from aspects energy and transportation to agriculture and healthcare. Moreover, this interconnected cyber-physical infrastructure consists of multiple systems that rely on one another to greater degrees for their operations and, at times, operate independent of human direction. One example of this type of interconnected system is the global supply chain, where information and communications technologies are providing real-time location services, traffic updates, emergency notifications, and more. Critical infrastructure owners and operators also continue to experience increasingly sophisticated cyber intrusions, which provide malicious actors the ability to disrupt the delivery of essential services, cause physical damage to critical infrastructure assets, and potentially produce severe cascading effects.

The Working Group considered the current processes that independently assess the physical and cyber threats for security-related systems associated with Federal facilities. It was noted that neither the current Design Basis Threat (DBT) Report nor the Physical Security Criteria contained in the RMP articulate cyber elements that should be considered and appropriately managed as they relate to Federal facilities. What follows are the major issues identified by the group.

The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard must address interrelated hazards that could lead to a debilitating impact on primary mission essential functions. A significant concern is the cybersecurity threat to Industrial Control Systems (ICS)[5] and the interdependencies and cascading effects on physical security in Federal facilities. There are generally three types of systems located in the majority of Federal facilities, listed below. These systems support facilities that depend on or complement the Nation's critical infrastructure. An ever increasing reliance upon these cyber-based systems creates potential vulnerabilities that, if exploited, could have physical consequences for Federal facilities and important concomitant capabilities (e.g., mission execution). The following is a brief description of the types of systems that support or address critical functions related to Federal facilities:[6]

Building Automation Systems (BAS) – Centralized, interlinked networks of hardware and software that monitor and control the environment in commercial, industrial, and institutional facilities. While managing various building systems, the automation system ensures the operational performance of the facility as well as the comfort and safety of building occupants. Examples include:

- Supervisory Control and Data Acquisition (SCADA) Systems; and

[5] NIST Special Publication 800-82, Rev 1, *Guide to Industrial Control Systems (ICS) Security*, May 2013

[6] Government Facilities Sector, *Sector Specific Plan 2010*

- Distributed Control Systems (Environmental Control Systems).

Electronic Security Systems (ESS) – Systems designed to prevent theft or intrusion and protect property and life. Examples include:

- Intrusion Detection Systems (IDS);
- Access Control Systems (ACS);
- Video Management Systems (VMS); and
- Intercom Systems.

Emergency Communications Systems – Systems for the protection of life by indicating the existence of an emergency situation and communicating the information necessary to facilitate an appropriate response and action.[7] Examples include:

- Fire Emergency Voice/Alarm Communications Systems (EVACS);
- Two-Way, In-Building Emergency Services Communications Systems; and
- Distributed Recipient Mass Notification Systems (DRMNS).

Each of these types of systems continues to become more reliant on computer controls, the connectivity of sensors and controllers, and network access, either authorized or unauthorized. Current assessments of Federal physical and cyber critical infrastructure are done independently. There is no current assessment methodology that addresses the integration of physical and cyber characteristics.

[7] As defined in NFPA 72-2010, Chapter 24

3 Recommended Approach

Physical security assessors, in collaboration with information technology specialists, are required to evaluate a variety of systems during the risk assessment process. This includes utility penetration points and controls; telecommunications equipment and rooms; and physical access controls and electronic security systems, components, and controls. Each of these elements may or may not have a cyber-based operating system and/or internet connectivity. Given these variables, the Working Group recommends an integrated approach whereby physical security and cybersecurity professionals are involved in all phases of developing an appropriate risk assessment methodology, conducting risk and vulnerability assessments, and recommending appropriate countermeasures and/or protocols. In doing so, Federal facilities will be more secure and resilient in the face of threats from all hazards.

3.1 Assessment Methodology

To identify vulnerabilities, physical security assessors need to evaluate the same systems already included in the physical security assessment, but also determine if the systems are dependent, operated, or connected through cyber or virtual means. Specifically, inquiries must be made regarding each component's operation and connectivity to a network, the type and impact of potential vulnerabilities, whether the system is/can be operated remotely or locally, and what security controls are in place (e.g., encryption, firewalls, business system antivirus software, etc.).

3.2 Threat Identification and Mitigation

The Interagency Security Committee (ISC) convenes the Design Basis Threat (DBT) Subcommittee and the Countermeasures Subcommittee to address and update threats and corresponding security criteria. These bodies should be the focal and starting points for developing additional security criteria to mitigate cyber threats. Both Subcommittees have processes in place for updating their products, and these can be expanded to include considerations relevant to Presidential Policy Directive 21 and Executive Order 13636.

3.2.1 Threat Definition

In order to effectively determine possible vulnerabilities, the Design Basis Threat Subcommittee will need to incorporate cyber threat into the list of undesirable events. A Cyber Threat is defined as:

> Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.[8]

Identification of this threat category should include potential target attractiveness features and possible scenarios. Upon successful identification of these characteristics, security assessors will in turn identify vulnerabilities to those threats and categorize facilities based upon the identified target attractiveness feature(s). The Subcommittee can utilize Federal, state, local, tribal, territorial, and/or private sector subject matter experts to assist in development of these products.

[8] NIST SP 800-53, CNSSI-4009

3.2.2 Countermeasures Development

Based on the identified threats, the Countermeasures Subcommittee can design a set of effective countermeasures to mitigate risks to cyber systems. Appendix B of *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* requires assessors to evaluate multiple areas within a facility.[9] Assessors must determine utility penetration points for commercially provided systems such as commercial power, water/waste water, natural gas, etc. Inclusion of telecommunication and internet-based connections will fit into the points identified. Moreover, the controls needed to access these systems and the provider controls driven by national standards of service delivery should be identified. A short list of possible areas and the relation to cyber connectivity are provided below. Assessors and the ISC should incorporate these areas and inquiries into their established practices to begin identification of these important components within the facility.

- **Building Automation Systems (BAS)** – Facility systems may be controlled, monitored, and operated utilizing commercially furnished software. These systems and their reliance upon network connectivity/sustained operation of the network should be identified and potential connection, encryption, and accessibility (e.g., access management) should be determined during the assessment.

- **Electronic Security Systems (ESS)** – A majority of these systems are located on the business process network and have remote connectivity/accessibility. Physical security assessors should determine if the system is afforded the same protections as the network and if the network is adequately protected with encryption, access management, and firewalls.

    - Many analog Video Management Systems (VMS) are being replaced with wireless components and power over ethernet capabilities. If not properly protected, the cameras, signals, and image storage can be accessed remotely. Physical security assessors should determine if the system is entirely digital, the nature of the accessibility, and what protections, both physical and logical, are in place.

- **Fire Alarm Control Panel** – Many of the new systems are linked to remotely monitored locations, and the processes and signals are digital. Physical security assessors should determine the nature of connection, accessibility, and protections in place.

- **Security, Fire, and Building Automated System Control Centers** – The majority of newly constructed and redesigned control centers are moving to entirely digital and/or network-based platforms complete with commercial software integration. These systems may have remote connectivity, accessibility, and protections; the assessor should identify each of these elements.

Each of the areas listed above are examples of potential physical security gaps, given dependence on network accessibility, software programs, or digital media transmission. By evaluating these simple elements and documenting their characteristics, assessors may begin to

[9] Please see Risk Management Process: Appendix B, section *B.5.1 How to Apply the Physical Security Criteria*.

understand the reliance upon emerging cyber-based systems. Physical security assessors should be required to consult cybersecurity professionals within their agency or other components to determine the necessary countermeasures and protections to provide mitigation against these threats.

3.3 Facility Security Level Determination

Facility Security Level (FSL) scoring criteria listed in *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* for "Threat to Tenant Agencies" should be evaluated to determine how to account for the identified cybersecurity threat.

The Interagency Security Committee is responsible for setting standards for assessing and managing risk to Federal facilities. The first step in the assessment process is the determination of the FSL. Once this level is established, agencies can identify and prioritize facilities supporting primary mission essential functions (PMEF). This level corresponds to a baseline level of protection (LOP) consisting of a myriad of security criteria recommendations. Each of these recommendations or standards requires physical security assessors to determine whether the protective posture at the facility meets the set criteria. Decisions to mitigate or accept risk will be determined by applicable Facility Security Committees (FSC), security organizations, or senior agency representatives.

To accomplish the determination for each of the specified criteria, physical security assessors must observe the conditions present at the facility and/or utilize construction plans or another credible source to determine the protective posture. Many of these areas/systems are co-located with or linked to cyber infrastructure components. Physical security assessors often evaluated integrated (cyber/physical) systems in the past, but focused solely upon the physical controls and access rather than the protection, integrity and accessibility of cyber-enabled systems. In an effort to integrate the two different types of access and protective measures, the Working Group determined the personnel accomplishing the assessment should consider site-specific physical and cyber areas to ensure a more comprehensive risk management process.

3.4 Compliance

The ISC has created a Compliance Working Group comprised of subject matter experts to address issues related specifically to compliance. The Working Group should develop a method to evaluate the existing level of compliance with Presidential Policy Directive 21 and published ISC standards; determine current implementation standards; develop screening criteria to evaluate compliance; identify resources required to fulfill the mission of compliance; and document a comprehensive strategy for compliance.

3.5 Training

In order to effectively implement this strategy, the ISC Training Subcommittee should seek to advise and assist member agencies in achieving training programs that capture the processes and requirements articulated in Presidential Policy Directive 21 and advise the ISC on the minimum training recommendations necessary to achieve a standard of performance acceptable overall to the security efforts of the Interagency Security Committee. The Subcommittee can review training products and/or programs currently available and those under development to ensure

compliance with ISC standards and sufficiently provide personnel with the information and skills to enhance success.

4 Administration

Consideration shall be given to applicable laws, presidential directives, and Federal regulations, including the protection of privacy, civil rights, and civil liberties while moving forward with implementation of this strategy. In addition, Federal departments and agencies shall protect all information consistent with applicable authority and policies. Consideration should also be given to incorporate or address evolving guides, policies, and frameworks[10] that are under development in response to Executive Order 13636 to reduce cyber risks to critical infrastructure.

[10] NIST Improving Critical Infrastructure Cybersecurity, EO 13636, *Preliminary Cybersecurity Framework*

List of Abbreviations/Acronyms/Initializations

TERM	DEFINITION
ACS	Access Control System
BAS	Building Automation System
CIA	Central Intelligence Agency
CS&C	Cybersecurity and Communications
DBT	Design-Basis Threat
DHS	Department of Homeland Security
DOT	Department of Transportation
DRMNS	Distributed Recipient Mass Notification System
EO	Executive Order
ESS	Electronic Security System
EVACS	Emergency Voice/Alarm Communications System
FAA	Federal Aviation Administration
FPS	Federal Protective Service
FSL	Facility Security Level
ICS	Industrial Control System
IDS	Intrusion Detection System
ISC	Interagency Security Committee
ITF	Integrated Task Force
LOP	Level of Protection
OPS	Operations
PMEF	Primary Mission Essential Function
PPD-21	Presidential Policy Directive 21
QHSR	Quadrennial Homeland Security Review
RMP	Risk Management Process
S&T	Science and Technology
SCADA	Supervisory Control and Data Acquisition
VMS	Video Management System

Glossary of Terms

TERM	DEFINITION
Cyber Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Cybersecurity	The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communication systems and the information contained therein to ensure confidentiality, integrity, and availability; includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems.[11]
Facility Security Committee	A committee that is responsible for addressing facility-specific security issues and approving the implementation of security measures and practices.
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.
Federal Facility	Government leased or owned facilities in the United States (inclusive of its territories) occupied by Federal employees for nonmilitary activities.
Industrial Control System	An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.[12]
Level of Protection	The degree of security provided by a particular countermeasure or set of countermeasures.
Primary Mission Essential Function	Those department and agency Mission-Essential Functions that must be performed to support or implement the performance of the National Essential Functions before, during, and in the aftermath of an emergency.[13]
Vulnerability	A weakness in the design or operation of a facility that an adversary can exploit.

[11] As defined in the NIPP

[12] As defined in NIST Special Pub. 800-53A, Rev. 1

[13] As defined in NSPD-51/HSPD-20

Interagency Security Committee Participants

Interagency Security Committee
Bernard Holt
Deputy Executive Director

Interagency Security Committee Representative
Anthony Evernham

Working Group Participants
Thomas Allen
Department of Transportation

Sue Armstrong
Department of Homeland Security, Federal Protective Service

Chuck Boling
Central Intelligence Agency

Odie Butler
Department of Veterans Affairs

Christopher Coleman
General Services Administration

Hugh Meehan
Smithsonian Institution

Will Morrison
Department of Transportation, Federal Aviation Administration

Michael Mulligan
Department of Homeland Security, Office of Cybersecurity & Communications

Michael Scarola
Department of Homeland Security, Operations

Matthew Weese
Department of Homeland Security, Federal Protective Service

Trent DePersia
Department of Homeland Security, Science & Technology