INTERAGENCY SECURITY COMMITTEE

Security Convergence: Achieving Integrated Security

An Interagency Security Committee Best Practice

2022 Edition

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Interagency Security Committee

Dedicated to Dr. William "Will" Morrison

This first edition of *Security Convergence: Achieving Integrated Security* is dedicated to our good friend and colleague, Dr. William "Will" Morrison, a vital contributor to the Interagency Security Committee (ISC) who worked tirelessly for the betterment of federal facility security everywhere.

Dr. Morrison served on numerous ISC subcommittees and working groups, including as Chair of the Convergence Subcommittee since 2011. A Certified Protection Professional, he personified security convergence, representing the ISC through unwavering collaboration with the government's Chief Information Officer community - particularly in the identity, credentialing, and access management mission space. Dr. Morrison knew the importance of taking a unified approach to operational technology such as Physical Access Control Systems (PACS), and he readily shared his time and expertise to help many ISC members with their PACS programs.

Dr. Morrison's dedication, professionalism, and mentorship are best symbolized in this closing line of an email last year: "When you have a chance to take a deep breath, let's talk again and solve the world's problems."

Message from the Interagency Security Committee Chief

The Interagency Security Committee (ISC) vision statement is: "*Federal facilities, the people who work at them, and those who visit them are safe and secure throughout the country*." The ISC achieves its vision by establishing security policies, standards, and recommendations to enhance the quality and effectiveness of security in and protection of federal facilities. The ISC is chaired by the Cybersecurity and Infrastructure Security Agency (CISA), Executive Assistant Director for Infrastructure Security, and consists of 65 departments and agencies working collaboratively to achieve its vision.

As Chief of the ISC, I am pleased to introduce *Security Convergence: Achieving Integrated Security, An Interagency Security Committee Best Practice, 2022 Edition,* which replaces the ISC document titled *Securing Government Assets through Combined Traditional Security and Information Technology: An Interagency Security Committee White Paper, February 2015*. This publication provides best practices, methodologies, and recommendations to enable federal executive branch departments and agencies to achieve integrated security through planning, promoting, and implementing unity of effort across disciplines, including physical security, information security, cybersecurity, and information technology.

Reviewed annually and updated as needed, this best practice represents exemplary leadership from the Convergence Subcommittee and collaboration across the entire ISC membership.

Daryle J. Hernandez
Chief, Interagency Security Committee
Cybersecurity and Infrastructure Security Agency

Table of Contents

Message from the Interagency Security Committee Chief **1**

Table of Contents **3**

1.0 Introduction **5**

2.0 Background **6**

3.0 Applicability and Scope **6**

4.0 Key Definitions **7**

5.0 Achieving Integrated Security **9**

5.1 Security Requirements 10

6.0 A Mission Centric Planning Model **11**

6.1 Defense-in-Depth 12

6.2 Risk Management 14

6.2.1 The Interagency Security Committee's Risk Management Process (RMP) . 14

6.2.2 The NIST RMF 15

6.2.3 Security Convergence of the ISC's RMP and NIST's RMF 16

6.3 Organizational Alignment 17

6.3.1 Governance Approach 17

6.3.2 Organizational Approach 18

6.3.3 Procedural Approach 18

6.4 Cultural Adaptation 19

6.4.1 Training 20

6.5 Performance Management 21

6.5.1 Performance Measurement Implementation 21

6.5.2 Operational Technology Assessments 21

6.6 Supply Chain Risk Management 22

6.6.1 SCRM for National Security Systems 22

6.6.2 Defending Against Software Supply Chain Attacks 23

6.6.3 Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists 23

6.6.4 ICT SCRM Task Force Products 24

Appendix A: Acronyms 25

Appendix B: Training Resources 29

Appendix C: Reference 31

Acknowledgements 33

1.0 Introduction

The evolution of technology permeates nearly every facet of the modern industrialized world and the traditional security community is not immune to its influence. Providing reliable security for federal government assets presents numerous challenges for today's security professionals. Security professionals often procure and employ operational technology to create a layered security approach to protecting federal facilities and personnel. Layered security may include Video Surveillance Systems (VSS), Intrusion Detection Systems (IDS), and electronic Physical Access Control Systems (ePACS), either as a stand-alone component or as an integrated environment.

Employing operational technology, security professionals rely heavily upon the information technology (IT) infrastructure to host and interconnect the various components of VSS, IDS, and ePACS. Utilizing IT infrastructure to interconnect Electronic Security System (ESS) components across Local Area Networks (LAN), Wide Area Networks (WAN), Metropolitan Area Networks (MAN), or the Internet requires convergence between the traditional security disciplines and the IT community.

In February 2021, attackers used credentials obtained from the dark web to gain access to a water plant. Using the plant's TeamViewer software, the attackers manipulated the pH in the city's water to dangerous levels by increasing the sodium hydroxide quantity by 100 times. Fortunately, a facility worker was able to reverse the change before it could take effect.

Webster's dictionary defines convergence as "the act of converging and especially moving toward union or uniformity", or "the merging of distinct technologies, industries, or devices into a unified whole". Thus, for organizations seeking to achieve integrated security, security convergence becomes a collaborative effort to integrate physical security, information security, cybersecurity, information assurance, and information technology to protect assets.

Security Convergence: Achieving Integrated Security, An Interagency Security Committee (ISC) Best Practice, 2022 Edition provides:

- Guidance to assist federal executive branch departments and agencies in achieving integrated security through best practices and methodologies.
- Recommendations for planning, promoting, and implementing a unified effort between several related areas, including information security, physical security, cybersecurity, and information technology.
- A planning model for the merging of parallel risk management processes, the optimization of organizational alignment, as well as recommended training and performance management.

This document ultimately seeks to create a paradigm shift by promoting the integration of organizational security disciplines to address the convergence of IT and security functions.

2.0 Background

On April 19, 1995, at 9:02 a.m., a major explosion occurred in Oklahoma City. The source of the blast was a truck packed with explosives parked outside of the Alfred P. Murrah Federal Building. The blast destroyed the facility, which housed 14 federal agencies and The America's Kids Daycare Center. This tragedy remains the worst domestic-based terrorist attack against the U.S. Government in our history: 168 lives were lost, including 19 children, and more than 800 people were injured. The blast destroyed or damaged 324 buildings within a 16-block radius.

The day after the attack, the president realized federal facilities were vulnerable. There were no minimum-security standards across the executive branch nor existing federal authority to assess vulnerability, develop standards, or ensure compliance with security standards. The president directed the Department of Justice (DOJ) to assess the vulnerability of federal facilities to acts of terrorism and violence and develop recommendations for minimum standards. A working group was formed to identify possible threats, vulnerabilities, and consequences to federal facilities. The group issued the "Department of Justice Vulnerability Assessment of Federal Facilities" report, which recommended the creation of the ISC and outlined 52 minimum security standards and the method of categorizing buildings by security level.

In October 1995, the president signed Executive Order (EO) 12977 establishing the ISC, which has developed and published over 20 policies, standards, and recommendations to identify, assess, and prioritize risks at federal facilities.

By EO 13286, the Department of Homeland Security (DHS) has been the home of the ISC since its transfer from the General Services Administration (GSA) in March 2003.

The convergence of cyber across all security functions has been a focus area for ISC members since the 2015 publication of *Securing Government Assets Through Combined Traditional Security and Information Technology White Paper.* The ISC recognized the necessity for additional guidance and reengaged its Convergence Subcommittee to develop this guidance. Given the ISC's diverse membership, the Subcommittee was able to draw upon a variety of subject matter experts to consolidate security convergence information into a single best practices document.

3.0 Applicability and Scope

Consistent with EO 12977, *Security Convergence: Achieving Integrated Security, An Interagency Security Committee Best Practice, 2022 Edition* aims to assist security and IT professionals responsible for the security and safety of executive branch buildings and facilities in the United States occupied by federal personnel for nonmilitary activities These facilities include existing owned, to-be-purchased, or leased facilities; standalone facilities; federal campuses; and, where appropriate, individual facilities on federal campuses and special-use facilities.

4.0 Key Definitions

Key definitions have been compiled from the following sources and notated accordingly:

ANNOTATED SOURCES:

1) National Institute of Science and Technology (NIST) Definitions
2) *The Risk Management Process: An Interagency Security Committee Standard* (2021)
3) NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (2015)
4) Introduction to Physical Security PY011.16 (cdse.edu)

TERM	DEFINITION
Convergence	Moving toward union or uniformity; the merging of distinct technologies, industries, or devices into a unified whole (Webster's Dictionary).
Cybersecurity[1]	The ability to protect or defend the use of cyberspace from cyber-attacks.
Facility Security Level (FSL)[2]	A categorization based on the analysis of several security-related facility factors that serves as the basis for implementing countermeasures specified in ISC standards.
Information Assurance (IA)[1]	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.
Information and Communications Technology (ICT)[3]	Encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information.
Information Security[1]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.
Information Technology (IT)[1]	Any equipment, interconnected system, or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.

TERM	DEFINITION
Operational Technology[1]	Programmable systems or devices that interact or manage devices that interact with the physical environment. These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.
Physical Security[4]	Active and passive measures designed to deter and prevent unauthorized access to personnel, equipment, facilities, information, and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity.
Risk Acceptance[2]	The explicit or implicit decision to not take an action that would affect all or part of a particular risk.
Risk Assessment[2]	The process of evaluating credible threats, identifying vulnerabilities, and assessing consequences.
Risk Management[2]	A comprehensive approach to allocating resources for the protection of a facility, assets, and occupants to achieve an acceptable level of risk. Risk management decisions are based on the application of risk assessment, risk mitigation, and, when necessary, risk acceptance. **Extended definition**: Process of identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level at an acceptable cost.
Risk Management Methodology[2]	A set of methods, principles, or rules used to identify, analyze, assess, and communicate risk, and mitigate, accept, or control it to an acceptable level at an acceptable cost.
Risk Management Strategy[2]	A proactive approach to reduce the often-negative impacts of various risks by choosing within a range of options that include complete avoidance of any risk that would cause harm or injury, accepting the risk, controlling the risk by employing risk mitigation options to reduce impacts, or transferring some or all the risk to another entity based on a set of stated priorities.
Supply Chain[1]	A linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.
Supply Chain Risks[1]	Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations, (e.g., mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation.

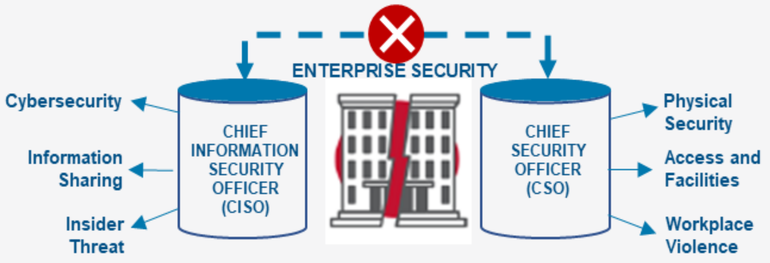
TERM	DEFINITION
Supply Chain Risk Management (SCRM)[1]	The systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain, (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).

5.0 Achieving Integrated Security

Integrated security helps organizations detect, delay, mitigate, and prevent threats. Attack surfaces continue to expand and become more complex due to the increasing proliferation of Operational Technology/Internet of Things (OT/IoT) devices into the operational/business and security functions. The OT/IoT advances have connected individual security devices to the vast virtual ecosystem, expanding the potential attack surface of facilities and making traditional physical security and safety systems more vulnerable. In this interconnected, cyber-physical ecosystem, a successful attack in one environment could impact the other. Federal departments and agencies face the challenge of providing security for both physical and cyber assets, targeted separately or simultaneously, resulting in compromised systems and infrastructure. However, in many federal departments and agencies, asset security is often controlled by separate authorities resulting in a siloed approach (Figure 1). When security elements operate independently with minimal or no collaboration, the department or agency's overall security is reduced.

ORGANIZATIONAL CHALLENGE:
SILOED SECURITY FUNCTIONS

Together, cyber and physical assets represent a significant amount of risk to physical security and cybersecurity– each can be targeted, separately or simultaneously, to result in compromised systems and/or infrastructure. Yet physical security and cybersecurity divisions are often still treated as separate entities. When security leaders operate in these siloes, they lack a holistic view of security threats targeting their enterprise. As a result, attacks are more likely to occur and can lead to impacts such as exposure of sensitive or proprietary information, economic damage, loss of life, and disruption of National Critical Functions (NCFs).



☒ Security functions operate independently with limited collaboration on enterprise-wide risks.

☒ Lines of communication are unclear and impede coordination and collaboration.

☒ Senior leaders and teams lack visibility of interconnected physical and cyber assets.

☒ Organization is unable to quickly identify, prevent, and respond to complex threats.

Figure 1: Siloed Security Function Challenges

5.1 Security Requirements

The Federal Information Security Management Act of 2014 (FISMA), as amended, requires each federal agency to develop, document, and implement an agency-wide program to provide information security for information systems. Departments and agencies must also provide technology that supports the operations and assets of the agency, including those provided or managed by another agency, a contracted third-party vendor, or another source.

As required by FISMA, the National Institute for Standards and Technology (NIST) provides technical standards and guidance to executive departments and agencies on IT security. Federal departments and agencies must meet the minimum-security requirements using the security controls in NIST Special Publication (SP) 800-53 Rev. 5, *Security and Privacy Controls for Federal Information Systems* (2020). Security controls are the safeguards or countermeasures within a system or organization that protect the confidentiality, integrity, and availability of the system and its information and that manage information security risk. The controls selected or planned must be documented in a System Security Plan (SSP) in accordance with NIST SP 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems* (2006).

The composite of federal standards and controls documents represented in NIST SP 800-37 Rev 2, *Risk Management Framework (RMF) for Information Systems and Organizations* (2018), provides guidelines for managing information security and privacy risk, as applicable to systems and organizations. The guidelines clarify the security and privacy risks inherent when operating a system and managing risk at an acceptable level based on countermeasures, and mandate senior official authorization when bringing a system into operation. Applying the NIST RMF and granting and maintaining an Authority to Operate (ATO) is akin to granting a clearance or certifying a facility for certain activities.

Security professionals use *The Risk Management Process for Federal Facilities (RMP): An ISC Standard* to develop recommended physical security countermeasures for a facility. Recent revisions have included the identification and implementation of security countermeasures for Building Access and Control Systems (BACS)[1]. Additionally, the *ISC Design-Basis Threat (DBT) Report* provides an estimate of the threat federal facilities face across a range of undesirable events. The DBT details the threat of cyber-attacks to include unauthorized access, interruption of services, and modification of services to federal facility Information and Communication Technology (ICT).

In August 2020, a group of hackers breached security camera data from a Silicon Valley security provider. The breach allowed the hackers access to live feeds from over 150,000 surveillance cameras installed in hospitals, police departments, prisons, and manufacturing plants.

Organizations should first identify the level of risk associated with individual positions and then determine what level of security is required before assigning a designation. Position designation is achieved by assessing the duties and responsibilities of the position to determine the risk level, (i.e., the degree of potential damage to the efficiency or integrity of the service from potential misconduct of an incumbent) and sensitivity level, (i.e., the potential for the incumbent to bring a material adverse effect on the national security and the degree of that potential effect).

[1] More information on countermeasures and BACS can be found in *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* Appendix A and B.

Designations are also put in place for:

- Information systems: low, moderate, high determination
- Facilities: Facility Security Level (FSL) I-V, open storage secret, sensitive compartmented information facility

6.0 A Mission Centric Planning Model

The act of moving towards a unified effort starts with planning and will include or involve a wide variety of offices or processes within an organization. This Mission Centric Planning Model (Figure 2) offers organizations a tool or roadmap to develop the necessary framework to achieve integrated security. At its center is the mission focus surrounded by six interconnected specific planning elements:

- Defense-in-Depth
- Risk Management
- Organizational Alignment
- Cultural Adaptation
- Performance Management
- Supply Chain Risk Management

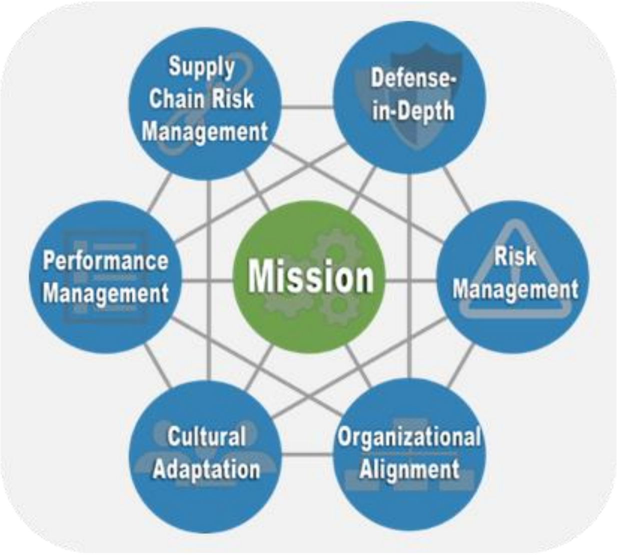


Figure 2: Mission Centric Planning Model

6.1 Defense-in-Depth

Organizations should develop a layered security strategy known as defense-in-depth. NIST defines defense-in-depth as “the security strategy for integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.”[2] The goal is to prevent an undesirable event from occurring through the exploitation of a single vulnerability or defeat of a single line of security measures by implementing a layered defense strategy. At a minimum, defense-in-depth planning must include the layers identified in Figure 3.

Successful application of a defense-in-depth strategy relies on a robust security awareness and training program for recognizing and reporting potential indicators of insider threats, adhering to physical security policies, and following organizational practices for managing the most common pervasive cybersecurity risks. A General Accounting Office (GAO) analysis of United States Computer Emergency Readiness Team (US-CERT) and the Office of Management and Budget (OMB) data for 2019 indicates that over 60% of information security incidents may have been prevented by greater employee awareness and training in identifying phishing and compliance with organizational cyber policies (Cybersecurity | U.S. GAO).

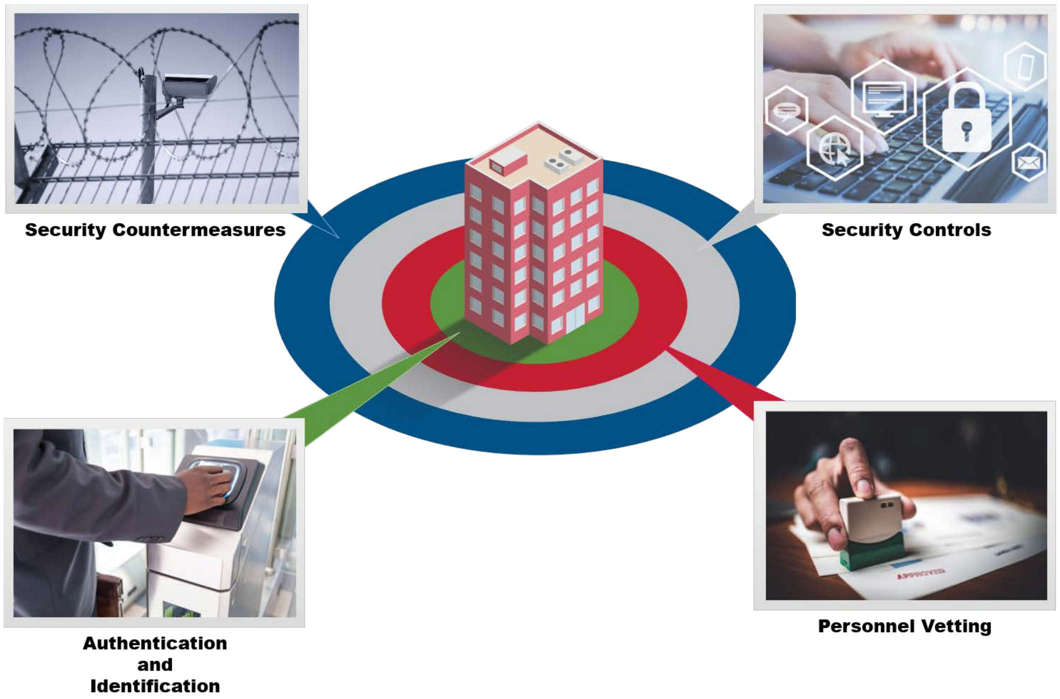


Figure 3: Defense in Depth

[2] NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations (2020*)

Security countermeasures: Countermeasures are designed to detect, delay, mitigate or prevent unauthorized access to personnel, equipment, facilities, and information to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity. These countermeasures may include physical access control systems, locks, barriers, fences, VSS, IDS, or established security policies such as visitor management procedures. Organizations meet this requirement through the application of the ISC RMP. Organizational training cited and required annually in the *ISC Risk Management Process, Appendix B: Countermeasures*, may include specific security policies such as facility access control requirements, hostile surveillance awareness, and how to identify and report suspicious activity/incidents.

Security controls: Security controls include safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information[2]. Security controls can include administrative, technical, and physical aspects. Organizations meet this requirement through the application of the NIST Risk Management Framework. Organizational training should include recognizing and reporting potential indicators of insider threat along with cybersecurity awareness and reporting. The FISMA[3] requires agency information security programs to include security awareness training on information security risks associated when complying with agency policies and procedures intended to reduce risk. In addition, FISMA requires agencies to provide role-based training to personnel with significant responsibilities for information security.[4]

Personnel Vetting: Through proper vetting, agencies assess potential risks presented by personnel. Depending on the position type, position risk, and sensitivity level, the agency will determine the individual's suitability or fitness to work for or on behalf of the government, eligibility to hold a sensitive position, have access to classified information, and hold a personal identity verification credential.

Authentication/Identification (HSPD-12): Verification of the identity of an individual who is entering a controlled space or accessing controlled government IT systems is key to providing appropriate levels of security. The verification process is supported by up to three factors of authentication:

- Something you know: Personal Identification Number (PIN)
- Something you have: Common Access Card (CAC) or Personal Identity Verification (PIV)
- Something you are: biometrics such as fingerprints or facial recognition

Specifically, this relates directly to Federal Identity, Credential, and Access Management (FICAM) and Homeland Security Presidential Directive 12 (HSPD-12), which provide a common, standardized identity credential allowing secure, interoperable physical and logical access.

One way to accomplish authentication is to acquire a Physical Access Control System (PACS) solution from one of the approved solutions on the GSA FIPS 201 Approved Products List (APL). Departments or agencies can then customize a methodology (Table 1), where the security practitioner can use the FSL designation to support the necessary Levels of Assurance (LOA) for defined logical or physical functional

[3] https://www.cisa.gov/federal-information-security-modernization-act

[4] https://www.gao.gov/products/gao-21-288

areas. LOAs can be based on many factors to demonstrate to the organization requisite controls have been implemented and a credible determination of control effectiveness exists[5].

Table 1. FSL/LOA Methodology Example

FSL	LOA	Authentication Method
1	One Factor (1FA)	PIV-CAC
2	One Factor (1FA)	PIV-CAC
3	One Factor (1FA)	PIV-CAC
4	Two Factor (2FA)	PIV-CAC or PIVAUTH+ PIN
5	Three Factor (3FA)	PIV-CAC or PIVAUTH+ PIN + BIO

6.2 Risk Management

Two parallel but separate processes are currently used to assess and manage physical security and cybersecurity risk: the ISC RMP and the NIST RMF. These processes, (i.e., methodologies), for managing risk are frequently and independently executed throughout government organizations. Recognition that these two processes should work together, and the development of a comprehensive, converged methodology to achieve that synergy, may be the most important component in ultimately achieving integrated security within an organization.

6.2.1 The Interagency Security Committee's Risk Management Process (RMP)

The ISC developed a six-step RMP (Figure 4) to provide an integrated, single source of security countermeasures and guidance on countermeasure customization for all nonmilitary, executive branch federal facilities. The objective of the RMP is to identify an achievable Level of Protection (LOP) commensurate with — or as close as possible to, without exceeding — the level of risk.

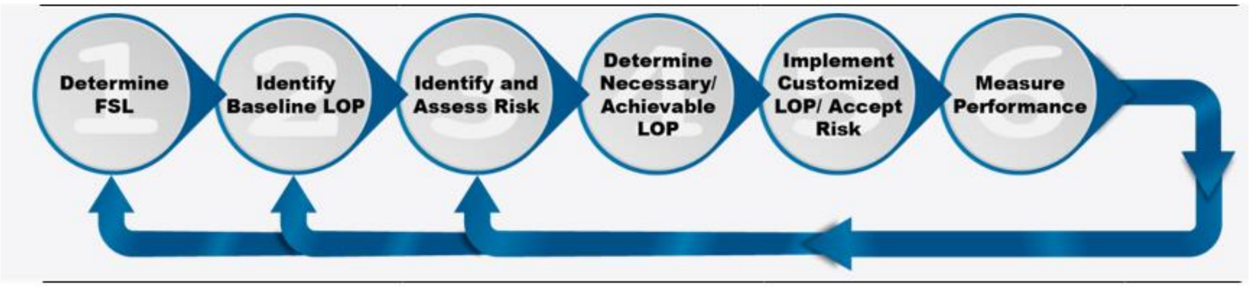


Figure 4: Risk Management Process

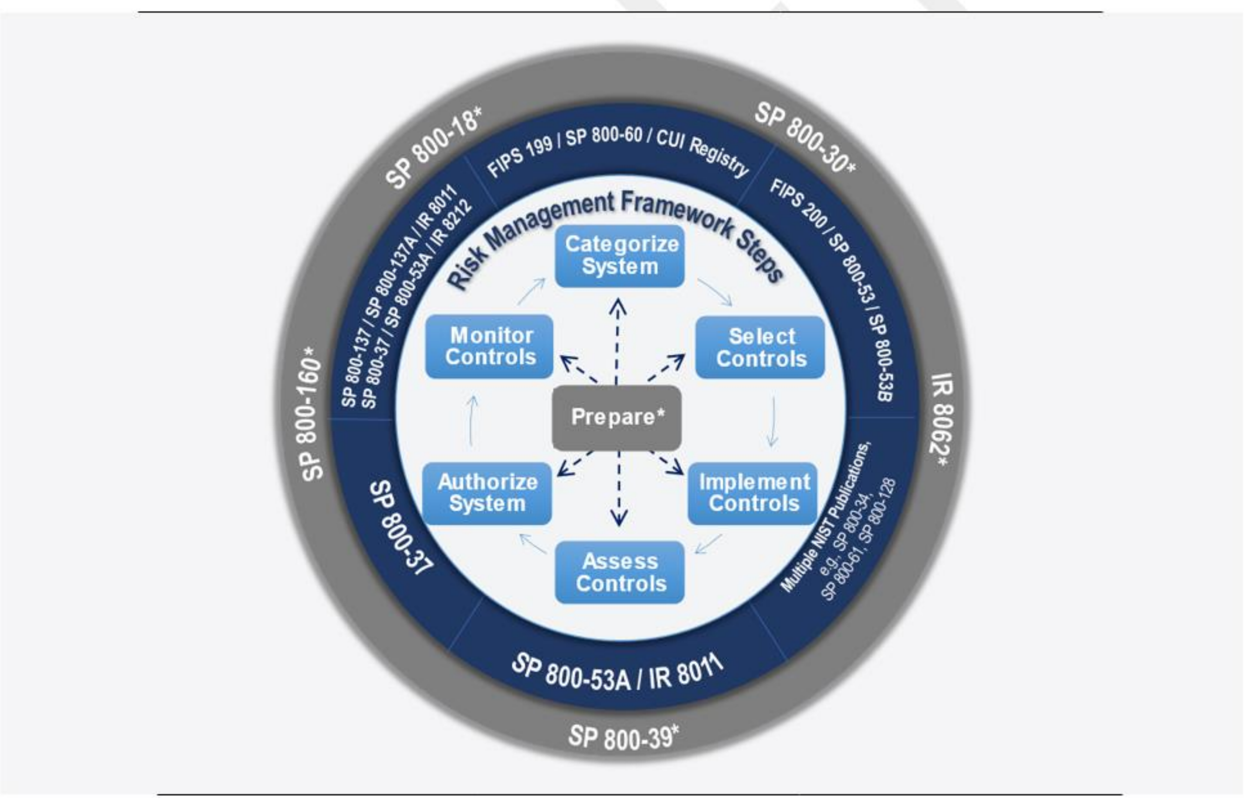
[5] NIST SP 800-37 Rev 2, *Risk Management Framework for Information Systems and Organizations* (2018).

6.2.2 The NIST RMF

The NIST RMF provides a comprehensive, flexible, repeatable, and measurable seven-step process for any organization to manage information security and privacy risks for organizations and systems while emphasizing:

- Managing risk by installing security and privacy capabilities into IT systems through the application of security and privacy controls.
- Maintaining awareness of the security and privacy state of systems on an ongoing basis through enhanced monitoring processes.

The RMF also provides essential information to senior leaders and executives to facilitate decision-making regarding the acceptance of risk to organizational operations, organizational assets, individuals, other organizations, and the nation arising from the operation and use of systems. The RMF links to a suite of NIST standards and guidelines to support the implementation of risk management programs to meet the requirements of FISMA (Figure 5).



SP 800-18*
SP 800-30*
IR 8062*
SP 800-39*
SP 800-160*
FIPS 199 / SP 800-60 / CUI Registry
FIPS 200 / SP 800-53 / SP 800-53B
Multiple NIST Publications, e.g. SP 800-34, SP 800-61, SP 800-128
SP 800-53A / IR 8011
SP 800-37
SP 800-137 / SP 800-137A / IR 8011
SP 800-37 / SP 800-53A / IR 8212
Risk Management Framework Steps
Categorize System
Select Controls
Implement Controls
Assess Controls
Authorize System
Monitor Controls
Prepare*

Figure 5: NIST RMF Publications and Resources

6.2.3 Security Convergence of the RMP and RMF

Development of a converged methodology between the ISC's RMP and the NIST's RMF assists organizations to effectively understand and manage the overall risk of their facilities and associated operational technology. Figure 6 below provides a suggested structural flow for merging the RMP and RMF that can be adjusted according to departmental and agency policies to achieve a more integrated risk management approach.

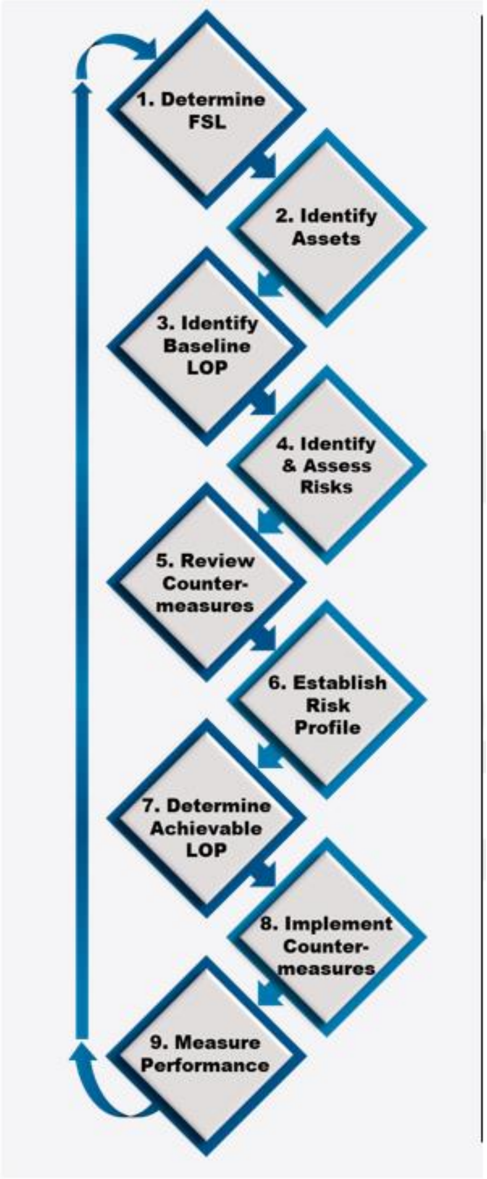

1. Determine FSL
2. Identify Assets
3. Identify Baseline LOP
4. Identify & Assess Risks
5. Review Counter-measures
6. Establish Risk Profile
7. Determine Achievable LOP
8. Implement Counter-measures
9. Measure Performance

Figure 6: Merging or joining the RMP and RMF

1) Determine the FSL using the ISC's RMP Standard.
2) Identify and categorize all information systems and the person/office responsible for maintaining them.
3) Identify baseline LOP required to protect assets. The LOP will be based on the FSL rating and the potential impact on the system's confidentiality, integrity, and availability.
4) Identify and assess risks to the facility and its systems to determine if the baseline LOP is sufficient or if customization is required.
5) Determine necessary LOP and if an IT solution can/will be used for any countermeasures.
6) Review NIST RMF and establish a risk profile for IT systems and software selected for countermeasures. Devise each project based on the steps of the RMF: prepare, categorize, select, implement, assess, authorize, and monitor.
7) If the necessary LOP cannot be achieved, determine the highest achievable LOP.
8) Implement countermeasures and document all the processes needed to maintain their operation.
9) Measure performance of countermeasures and controls for effectiveness and make changes as needed. As changes to the system or facility are made, revisit previous steps in the RMF to ensure any changes to the implementation and resulting risk are understood and within the organization's risk tolerance.

6.3 Organizational Alignment

Integrated security depends upon cooperative partnerships between multiple professionals including IT specialists, facility engineers, resource managers, physical security specialists, and cybersecurity specialists. Proper organizational alignment is key, and departments or agencies should ensure organizational alignment recognizes, supports, and sustains a converged approach to security that addresses the threats stemming from attacks targeting both physical and cyber assets. Approaches to accomplish this include one or more of the following: Governance, Organizational, and Procedural.

Many variables exist that may influence organizational alignment including size, mission, culture, and budget. The Office of Management and Budget (OMB) Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management (ICAM),* provides a benchmark on how an organization can "harmonize its enterprise-wide approach to governance, architecture, and acquisition."[6]

6.3.1 Governance Approach

Benchmarking the ICAM Governance model found in OMB M-19-17, organizations may establish a formal governance structure, (e.g., council, panel, committee, or Facility Security Committee Working Group), responsible for the management, oversight, and accountability of security within an organization. The governance provides a centralized point for achieving integrated security through convergence of the various disciplines. To ensure representation from the right entities within the organization, key members and programs may include:

- Chief Security Officer
    - Personnel Security
    - Physical Security
    - Operations Security
- Chief Information Officer
    - Policy/Governance
    - IT Operations/Services
    - Technology/Innovation
- Chief Information Security Officer
    - Cyber/IT Security
- Insider Threat Senior Official
- Legal
- Senior/Chief Risk Officer
- Occupational Health & Safety

[6] "Enabling Mission Delivery through Improved Identity, Credential, and Access Management" (OMB M-19-17, 2019).

6.3.2 Organizational Approach

Departments or agencies may designate an integrated, agency-wide, single office or team to lead and coordinate the organization's security efforts across the multiple internal domains. The Integrated Security Strategy Program Manager within the National Aeronautics and Space Administration (NASA) is one example of how the organizational structure may be successfully implemented.

Best Practice: NASA, Integrated Security Strategy Program Manager

In 2008, the NASA Assistant Administrator for Office of Protective Services created the position of an **Integrated Security Strategy Program Manager** to establish and utilize an integrated security strategy approach for all protective services operations. This strategy encompasses all security disciplines across the agency, mission directorates, centers, and projects/programs. The strategy increased efficiencies through a more integrated approach to governing and managing the agency's security.

As an example, NASA Center Protective Services Offices conducts the FSL determination with support from the CIO, Center Facilities Office, and designated representatives of the assessed facility to ensure operational technology, CIO designated High Value Assets (HVA), and critical interdependencies for FSL III and FSL IV designated facilities are identified and afforded the same LOP as the asset/mission or facility.

6.3.3 Procedural Approach

An effective procedural approach establishes formal relationships between the various participants through official charters, Memorandum of Agreement (MOA), or Interagency Service Agreement (ISA).

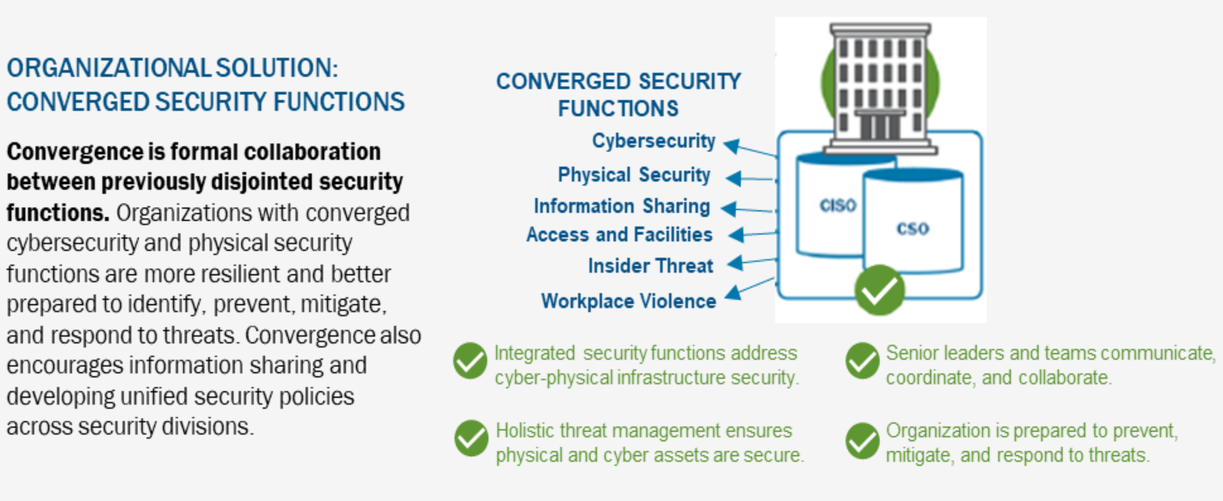
- An MOA/ISA establishes the formal relationships and processes and defines the cooperative work efforts and responsibilities of the Office of the Chief Security Officer (OCSO) and the Office of the Chief Information Officer (OCIO).
    - The MOA/ISA should define the cooperative work efforts between physical security, IT personnel, the system owner, (e.g., CSO), and the service provider, (e.g., CIO), and include configuration management, an APL, the SSP, and operating procedures.
    - In addition, a service level agreement specifying availability, serviceability, performance, and operation of the electronic security system (ESS) should be developed and established between the system owner, (e.g., CSO), and the service provider, (e.g., CIO).
- A procedural approach requires a **shared recognition** of what is most critical to the organization's mission and the corresponding level of acceptable risk.
- Under a procedural approach, physical security and cybersecurity are fully incorporated into all aspects of the organization's work to help drive decision-making and risk mitigation as demonstrated by the USCIS procedural approach.

Best Practice: USCIS Procedural Approach

In 2020, The United States Citizen and Immigration Services (USCIS) used the "procedural approach" to create a cross-functional team to provide a collaborative effort between the USCIS Office of Information Technology (OIT) and the Office of Security and Integrity (OSI). The collaboration operates under a single charter to plan, develop, prioritize, and deploy ePACS across all facilities within USCIS. This collaboration included the modernization of the Physical Access Control System (PACS) to meet the Federal Identity, Credentials, and Access Management (FICAM) and HSPD-12 criteria and then integration of PACS on the USCIS network. Leveraging a single application programming interface for managing the systems now allows OIT the ability to manage PACS hardware, software, and firmware, ensuring the systems operate at peak performance. It also provides OIT the ability to manage access to systems software and hardware via networking protocols to protect information systems from cyber security threats. Finally, this concept provides the OSI team the ability to track, audit, and ensure only authorized personnel have access to the facilities and assets they are responsible for protecting.

6.4 Cultural Adaptation

Senior leaders set the vision and tone for organizations and are key to instituting cultural change. Because the current siloed security model cannot efficiently mitigate today's complex threats and attack vectors (Figure 7), organizations must begin to evolve their senior-most security leadership to assume responsibility for all aspects of enterprise security.



ORGANIZATIONAL SOLUTION: CONVERGED SECURITY FUNCTIONS

Convergence is formal collaboration between previously disjointed security functions. Organizations with converged cybersecurity and physical security functions are more resilient and better prepared to identify, prevent, mitigate, and respond to threats. Convergence also encourages information sharing and developing unified security policies across security divisions.

✓ Integrated security functions address cyber-physical infrastructure security.

✓ Senior leaders and teams communicate, coordinate, and collaborate.

✓ Holistic threat management ensures physical and cyber assets are secure.

✓ Organization is prepared to prevent, mitigate, and respond to threats.

Figure 7: Converged Security Benefits

Once senior leadership embraces the approach to converge security disciplines and assess roles and responsibilities, the future of organizational security functions should be communicated to key stakeholders. The organization may choose to host a facilitated workshop for stakeholders from physical security, information technology, cybersecurity, and others to discuss the future of security in their organization. This transparent approach improves the awareness and understanding of those affected by the development of integrated security and allows them to address their concerns with leadership.

6.4.1 Training

Focused training is an important vehicle for developing a capable workforce, expanding vocabularies, and bridging differences between various professional disciplines. Departments or agencies may consider developing internal training to support integrated security initiatives. The following recommended topics provide examples of what to include in organizational training modules.

Basic Security System Terminology

Description: The course will help the end-user/stakeholder identify basic security system terminology.

Learning Objectives: Upon successful completion of this course, the end-user/stakeholder should be able to:

1. Identify basic physical security terminology.
2. Define basic electronic security terminology (to assist with understanding related components of Electronic Security Systems such as basic parts of Access Control Systems or Video Surveillance Systems).
3. Identify basic cybersecurity terminology.
4. Explain how the combination of physical security and cyber security is a step towards integrated security.
5. Communicate across the security enterprise with appropriate standards/approvals in place.

Security Convergence Approach Principles and Methodologies

Description: The course will help the end-user/stakeholder describe the relationship and interdependencies between physical security and cybersecurity elements.

Learning Objectives: Upon successful completion of this course, the student should be able to:

1. Identify cyber-physical systems.
2. Describe the interdependencies between the physical security and cybersecurity elements.
3. Summarize concepts and components that bridge cyberspace with physical space.
4. Apply/establish a framework aligning physical security and cybersecurity.

Develop and Implement Integrated Security Solutions

Description: The course provides the stakeholder with the tactics, techniques, and procedures to develop a planning model or structure to align physical security and cybersecurity goals while delivering best practices and lessons learned.

Learning Objectives: Upon successful completion of this course, the student should be able to:

1. Analyze and employ integrated security solutions.
2. Align physical security and cybersecurity policies and goals.
3. Develop integrated security best practices.

6.5 Performance Management

6.5.1 Performance Measurement Implementation

Implementing performance measures can benefit organizations at different levels, especially where security activities compete with other organizational programs for limited resources.

Performance measurement offers program managers at the headquarters-level a way to evaluate a program's capabilities and effectiveness while demonstrating the need to obligate funds for the integration of security disciplines. Additionally, implementing performance measures can complement the existing requirement for executive branch departments and agencies to implement physical security performance measures[7].

Field-level managers may use performance measures to demonstrate program effectiveness to stakeholders, assess emergency preparedness capabilities, oversee security equipment maintenance and testing programs, and determine the adequacy of resources to support operational security requirements. Together, physical security and cybersecurity-related performance measures provide valuable information used to support funding requests, accomplish program goals, identify areas for improvement, process change, or identify a need for additional training.

6.5.2 Operational Technology Assessments

An Operational Technology Assessment (OTA) program is a useful performance measurement that may be employed by departments and agencies. The OTA focuses on the physical and cyber risks at federal facilities and includes an evaluation of relevant threat actors, capabilities, and events applicable to facility and security technologies. The assessment also considers the potential impact of adversaries utilizing technology to increase their success and potential lethality as well as the protective measures employed by the facility and supporting systems. Further, the OTA gauges the basic configuration and management of systems installed at the facility, including an in-depth evaluation of the potential vulnerability of facility and security technologies to adversaries leveraging them for undesirable events at a targeted facility.

[7] *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, Appendix E: Use of Physical Security Performance Measures*, (ISC, 2021)

The assessment team should include subject matter experts from physical security, cybersecurity, and information security. Reports should be provided to the Facility Security Committee, tenant representative for single-tenant facilities, and organizational-level integrated security management leadership. OTA categories may include:

- Surveillance systems
- Safety management systems
- Lighting control systems
- ePACS
- Vertical transportation systems
- Routine business and emergency communications systems
- IDS
- Building automation system management dashboard and supervisory console
- Heating, ventilation, and air conditioning control systems
- Power and energy management systems

To optimize resources, organizations should collaborate on implementation between the OTA and annual FISMA reviews to ensure implementation of effective security controls in conjunction with the OTA.

6.6 Supply Chain Risk Management

NIST SP 800-161 *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (2015) guides federal departments and agencies in identifying, assessing, and mitigating ICT supply chain risks at all levels of their organizations. The publication integrates ICT SCRM into federal agency risk management activities by applying a multitiered, SCRM-specific approach, including guidance on assessing supply chain risk and applying mitigation activities. Appendix E provides a template that organizations should include in their ICT SCRM plans. Departments and agencies must also ensure compliance with appropriate directives such as EO 13873, *Securing the Information and Communications Technology and Services Supply Chain*, and EO 14034, *Protecting Americans' Sensitive Data from Foreign Adversaries*.

ICT SCRM Task Force's Threat Scenarios Report: https://www.cisa.gov/publication/ict-scrm-task-force-threat-scenarios-report

This report includes an identification of threats to the ICT supply chain and provides an assessment of impacts and mitigating controls that may reduce the impact of these threats. The objective is to provide practical, example-based guidance on supplier SCRM threat analysis and evaluation. This guidance can be applied during procurement or source selection by government and industry to assess supply chain risks and develop practices/procedures to manage the potential impact of these threats.

6.6.1 SCRM for National Security Systems

Committee on National Security Systems (CNSS) Directive 505 provides requirements for the U.S. Government to implement and sustain SCRM capabilities for national security systems. CNSSD 505 also guides organizations that own, operate, or maintain NSS to address supply chain risk; implement and sustain SCRM capabilities; assign responsibilities; establish the minimum criteria for the continued development, deployment, and sustainment of an SCRM program (or capability) for the protection of NSS, or non-NSS that directly support NSS.

6.6.2 Defending Against Software Supply Chain Attacks

A software supply chain attack occurs when a cyber threat actor infiltrates a software vendor's network and employs malicious code to compromise the software before the vendor sends it to their customers. The compromised software then compromises the customer's data or system. These types of attacks affect all users of the compromised software and may have widespread consequences for departments and agencies.[8]

CISA's 2021 publication, *Defending Against Software Supply Chain Attacks*, a collaborative effort between CISA and NIST, provides an overview of software supply chain risks and recommendations for software customers and vendors when using the NIST Cyber Supply Chain Risk Management (C-SCRM) framework and the Secure Software Development Framework to identify, assess, and mitigate risks.

6.6.3 Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists

Establishing and utilizing vetted, qualified sources of supplies can limit an organization's exposure to risk. Incorporating C-SCRM focused qualification criteria into existing or new qualification list processes can provide a targeted and effective means of ensuring that an ICT supplier or product is sufficiently trustworthy.[9] The FIPS 201 Evaluation Program and APL provide a great example of a qualified list.

FIPS 201 EVALUATION PROGRAM AND APL

In June 2006, the OMB issued Memorandum M-06-18 that requires federal agencies to procure only qualified products and services listed on the GSA APL when implementing HSPD-12 into their environment. Procurement of approved products and services facilitates the government-wide objective of a federated and interoperable FICAM segment architecture, and ensures compliance, consistency, and alignment of commercially available products and services with the requirements and functional needs of FICAM implementer. The APL provides federal agencies with products and services that have been approved for FICAM implementation based on rigorous security vulnerability and interoperability testing performed by the FIPS 201 Evaluation Program (ID Management, 2019). Product testing evaluates and certifies services and commercial products used in credentialing systems, physical access control systems, and public key infrastructures.

[8] *Defending Against Software Supply Chain Attacks* (CISA, 2021)

[9] *Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists* (CISA, 2021).

6.6.4 ICT SCRM Task Force Products

The ICT SCRM Task Force, established by CISA in December 2018, produced two publicly available documents (below) to help assess an ICT vendor's trustworthiness, as well as a report that evaluates ICT supply chain threats.

1. *Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists* (CISA, 2021): This document provides a list of criteria and factors that can be used to inform an organization's decision to build or rely on a qualified list for the acquisition of ICT products and services.

2. *Vendor SCRM Template* (CISA, 2021): This document provides a set of questions regarding an ICT supplier/provider's implementation and application of industry standards and best practices that can help guide supply chain risk planning in a standardized way. The template provides clarity to organizations on reporting and vetting processes when purchasing ICT hardware, software, and services.

Appendix A: Acronyms

Acronym	Meaning
APL	Approved Products List
ATO	Authority to Operate
BACS	Building Access and Control System
BCS	Building Control Systems
CAC	Common Access Card
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CNSS	Committee on National Security Systems
CSO	Chief Security Officer
C-SCRM	Cyber Supply Chain Risk Management
DBT	Design Basis Threat
DHS	Department of Homeland Security
EO	Executive Order
ePACS	Electronic Physical Access Control System
ESS	Electronic Security System

Acronym	Meaning
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FSL	Facility Security Level
HSPD12	Homeland Security Presidential Directive 12
IA	Information Assurance
ICAM	Identity, Credential, and Access Management
ICT	Information and Communications Technology
IDS	Intrusion Detection Systems
IoT	Internet of Things
ISA	Interagency Service Agreement
ISC	Interagency Security Committee
IT	Information Technology
LAN	Local Area Network
LOA	Levels of Assurance
LOP	Level of Protection

Acronym	Meaning
MAN	Metropolitan Area Network
MOA	Memorandum of Agreement
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OCSO	Office of the Chief Security Officer
OMB	Office of Management and Budget
OTA	Operational Technology Assessment
PACS	Physical Access Control System
PAK	PIV Authentication Key
PIN	Personal Identification Number
PIV	Personal Identity Verification
RMF	Risk Management Framework
RMP	Risk Management Process
SCRM	Supply Chain Risk Management
SP	Special Publications
SSP	System Security Plans

Acronym	Meaning
VSS	Video Surveillance Systems
WAN	Wide Area Network

Appendix B: Training Resources

RMP On-Line Training

The following online training is available on the Homeland Security Information Network and the Federal Emergency Management Agency website:

- IS-1170 Introduction to the Interagency Security Committee and Risk Management Process
- IS-1171 Introduction to Interagency Security Committee Documents
- IS-1172 Interagency Security Committee Risk Management Process: Facility Security Level Determination
- IS-1173 Interagency Security Committee Risk Management Process: Levels of Protection and Application of the Design Basis Threat Report (FOUO). Note: A Homeland Security Information System (HSIN) account is required to access this course.
- IS-1174 Interagency Security Committee Risk Management Process: Facility Security Committees

RMF On-Line Training

Center for Development of Security Excellence (CDSE) provides independent learning opportunities on the RMF through the following courses:

- CS102.16 Risk Management Framework (RMF) Step 1: Categorization of the System
- CS103.16 Risk Management Framework (RMF) Step 2: Selecting Security Controls
- CS104.16 Risk Management Framework (RMF) Step 3: Implementing Security Controls
- CS105.16 Risk Management Framework (RMF) Step 4: Assessing Security Controls
- CS106.16 Risk Management Framework (RMF) Step 5: Authorizing Systems
- CS107.16 Risk Management Framework (RMF) Step 6: Monitoring Security Controls
- CS160.16 Cybersecurity for Security Personnel

Risk Management Framework for Systems and Organizations Introductory Course is offered by the NIST Computer Security Resource Center.

Cyber Supply Chain Risk Management

Cyber Supply Chain Risk Management for the Public is a free course provided through the Federal Virtual Training Environment with no log-in requirements.

Cybersecurity Training Series

The National Counterintelligence and Security Center (NCSC) Cyber Training Series (dni.gov)

- Cyber Explore- Fundamentals of Cyber
- Cyber Aware – Anatomy of a Hack
- Cyber Exploits – Understand the Threat

Cybersecurity and Infrastructure Security Agency (CISA) Training

Cybersecurity and Infrastructure Security Agency (CISA) Training offers a wide array of training programs to government and private sector partners that includes:

- Cybersecurity
- Critical Infrastructure Training
- Insider Threat Training and Awareness
- Federal Virtual Training Environment
- PCII Authorized User Training
- Security and Awareness Training
- Risk-Based Performance Standard Training

Appendix C: Reference[10]

CISA

- “Cybersecurity and Physical Security Convergence Guide”
- Defending Against Software Supply Chain Attacks
- Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists
- “Supply Chain Risk Management Essentials”
- Vendor Supply Chain Risk Management Template
- “Public Safety Communications and Cyber Resiliency Toolkit”

ISC

- “Securing Government Assets Through Combined Traditional Security and Information Technology White Paper”
- *The Risk Management Process for Federal Facilities: An ISC Standard*

NIST

- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
- FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
- NISTIR 8011 Vol. 4, *Automation Support for Security Control Assessments: Software Vulnerability Management*
- NISTIR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*
- NISTIR 8212, *ISCMA: An Information Security Continuous Monitoring Program Assessment*
- SP 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*
- SP 800-30, *Guide for Conducting Risk Assessments*
- SP 800-34 Rev 1, *Contingency Planning Guide for Federal Information Systems*
- SP 800-37 Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*

[10] See Organization pages for most current versions of documents.

- SP 800-53 Rev 5, *Security and Privacy Controls for Information Systems and Organizations*
- SP 800-53A Rev 4, *Assessing Security Controls in Federal Information Systems and Organizations*
- SP 800-53B, *Control Baselines for Information Systems and Organizations*
- SP 800-60 Vol 1 Rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- SP 800-61 Rev. 2, *Computer Security Incident Handling Guide*
- SP 800-116 Rev.1, *Guidelines for the Use of PIV Credentials in Facility Access*
- SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
- SP 800-137A, *Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment*
- SP 800-160 Vol 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*
- SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
- SP 800-171 Rev. 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*

Office of the Director for National Intelligence

- Protect your Organization from the Foreign Intelligence Threat
- CNSS Directives Library (CNSS 505)

Other

- Federal Information Security Management Act (FISMA) of 2002 and 2014
- Homeland Security Presidential Directive 12 (HPSD-12)
- Office of Management and Budget Memorandum M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management

Acknowledgements

The ISC would like to thank the participants of the ***Convergence Subcommittee.***

Convergence Subcommittee

William Morrison
Chair
Federal Aviation Administration

Sue Armstrong
Co-Chair
Cybersecurity and Infrastructure Security Agency

Contributing Authors

Sam Alva
Cybersecurity and Infrastructure Security Agency

Kevin Choate
General Services Administration

Megan Knodell
Cybersecurity and Infrastructure Security Agency

Tarla Toomer
Department of Energy

William Windsor
Department of Homeland Security

Sophia Ziad
Department of Justice

Subcommittee Members

Robert Behm
Department of Labor

Tara Brown
Federal Emergency Management Agency

Dale Clark
Department of Commerce

Mark Clarke
Department of Justice

Danny Dagher
Cybersecurity and Infrastructure Security Agency

Shahpour Eskandary
Federal Emergency Management Agency

Michael Fluck
Internal Revenue Service

Antonio Gallegos
Cybersecurity and Infrastructure Security Agency

Jennifer Hammen
Department of Homeland Security

Mike Henig
Federal Emergency Management Agency

Michael Hawkins
Cybersecurity and Infrastructure Security Agency

Kurt Imre
United States Marshals Service

Nicholas Mikalis
Department of Homeland Security

James Nicholas
National Aeronautics and Space Administration

Yeshi Pisarcik
Internal Revenue Service

Interagency Security Committee

Daryle Hernandez, Chief

Deana Bollaci
Convergence Subcommittee Facilitator

Scott Dunford
Convergence Subcommittee Facilitator

Shawn Fiebiger
Convergence Subcommittee Facilitator

Jami Craig
Technical Editor

Glennell Kelly
Program Analyst

Martin Kobylarczyk
Program Analyst

Tom Seaman
Program Analyst