

Securing Government Assets through Combined Traditional Security and Information Technology:

An ISC White Paper

November 2013

Interagency Security Committee

DRAFT

Prologue

Convergence cannot be attained through the implementation of technology.
It is attained through defined business processes and adherence to policies and procedures.

Document Control: This document is unclassified. There is no prohibition on distribution.

Table of Contents

Table of Appendices

Table of Figures

Table of Tables

This page left intentionally blank.

1 Background

Technology permeates nearly every facet of the modern industrialized world. The traditional security community is not immune to its influence. Providing reliable security for federal government assets presents numerous challenges for today's security professional. To address physical security, today's security professional uses protection in depth through layered security as one of many tools to mitigate risks. Most often, security professionals procure and employ IT assets and infrastructure to obtain protection in depth for tangible and intangible assets for which the security organization is responsible. The layered security approach may include Closed-Circuit Video Equipment (CCVE) or video systems, intrusion detection systems (IDS) and electronic physical access control systems (PACS) either as stand-alone or an integrated environment to accomplish the tasks of deterrence, detection, delay, and response, and to serve as a force multiplier for security staff assigned to achieve those and other tasks.

Technological advances in system components, coupled with the interconnection capability, moved from Recommended Standards technology (e.g., RS-232, RS-422, RS-485, etc.) to Internet Protocol (IP) telecommunications standards (e.g., IPv6). Employing state-of-the-art systems, today's security professional relies heavily upon IT infrastructure to host and interconnect the various components of a CCVE/video system, IDS, and PACS. Employing 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 a convergence between the traditional security community (operational management), and the IT community (enabler).

Accomplishing convergence relies upon a joint, concerted effort of the traditional security and IT communities to achieve the goal of securing USG assets both tangible and intangible. This effort is analogous to those undertaken by the Chief Acquisitions Officer (CAO), Chief Financial Officer (CFO), Chief Human Capital Officer (CHCO), and other lines of business to establish office automation (OA) systems and supporting architecture to execute and achieve mission goals. However, the contrast between the IT systems supporting the agency's Chief Security Officer (CSO) and other lines of business is that the security systems supporting the CSO's mission are more operational in nature (i.e., 24-hours a day, 365-days a year), and enable a vital part of the layered security within a holistic security schema.

To facilitate an understanding of the necessary interaction between traditional security and information technology (IT) communities, the Interagency Security Committee (ISC) developed the recommendations contained herein to provide traditional security and IT professionals with mechanisms to support security programs while integrating information assurance management controls.

This page left intentionally blank.

2 Applicability and Scope

This document establishes a set of recommendations that are informative, seeking to assist the security and information technology communities to achieve convergence within an agency.

This document is intended to be used in conjunction with The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard.

Although this paper will mainly focus on the interaction between the security and IT communities, recommendations for interactions with other communities may be interspersed within.

This page left intentionally blank.

3 Assessment

To mitigate risks, CSO's conduct Facility Security Assessments (FSA) to identify and to assist in the development of effective countermeasures. Assisted by the guidance provided in the ISC Base Documents, the CSO begins to plan and identify the tools and apparatus to provide effective mitigation of those risks identified by the formal assessment. CSO's often employ electronic technology devices to implement cost effective countermeasures that serve as a force multiplier for security operations.

Today's Federal Government CSO is faced with an assortment of laws, regulations, or policies governing how electronic technology devices may be employed. Keeping with the subject, this section will focus on the policies that overlap with the IT and other communities that include but are not limited to guidance from the Office of Management and Budget (OMB) (most often issued through memoranda), Federal Information Processing Standards (FIPS), Homeland Security Presidential Directives (HSPD), and the ISC Base Documents. This section assumes CSO's will implement countermeasures in full compliance with applicable sections of the United States Code (U.S.C.), Code of Federal Regulations (CFR), Federal Management Regulations (FMR), Americans with Disabilities Act (ADA) requirements, Occupational Safety and Health Administration (OSHA) regulations, Fire and Life Safety (NFPA) codes guidance, and all applicable Executive Orders and Presidential Directives.

3.1 Recommended Approach

Implementing mitigation measures identified by the completion of a comprehensive FSA cannot be accomplished in a vacuum. In addition to the CSO, there are other stakeholders who should be involved. CSO's should include individuals from the IT community (when technology is being considered as a mitigation measure), facility management (ensuring facility management is cognizant of risks identified and mitigating measures), human resources (should mitigation measures impinge on employees, or effect collective bargaining/union agreements), and general counsel (should the CSO believe any legal, union, or privacy issue need addressing). Having first-hand knowledge of their individual agencies, CSO's should consider other stakeholders who may need to be included in planning and execution of mitigation efforts.

The CSO should coordinate with intra-agency stakeholders, or at stakeholders located at individual facilities, to establish a standing core team to address all aspects of mitigation measures under consideration. Inclusion of stakeholders in project planning and milestone reviews will assist the CSO to ensure recommendations are viable, cost effective/efficient, and are in compliance with agency and government wide policies, mandates and standards. At a minimum, the CSO should include portions of or the core team as a whole in the development of initial requirements development, pre-lease site visit, pre/post assessment, pre-occupancy, modified requirements development, vendor selection, project start-up, all construction walk-thru/meetings, commissioning, and pre/post occupancy punch list.

The core team will assist the CSO's efforts by providing expertise in security countermeasures, technology, enterprise level solutions and capabilities, legal guidance, as well as integration and interoperability. Further, the core team should assist the CSO to management expectations within their agency. Table 1 provides an example of a Core Team.

Where multitenant facilities are being addressed, the CSO should overlay this approach with the guidance provided in the FSC Standard.

1 **Table 1: Core Team Members and Descriptions**

CORE TEAM	
Team Member	**Role/Responsibility**
Chief Security Officer (CSO), or designee	Provide and ensure compliance with all national and agency specific guidelines to include but not limited to credentialing, facility access, logical access, and security systems.
Chief Information Officer (CIO), or designee	Vet and or approve hardware/software implementation and or integration onto agency network by following agency specific policy or guidance.
Security Specialist	Ensure FSA is complete, ISC recommendations are accurate, national and agency policies and directives are incorporated, and compliance with agency specific requirements.
Internet Technology (IT) Specialist	Validate agencies switch and IP port selections for logical/physical access and or security components utilizing the agencies network as well as ensuring security of agencies network systems by working in conjunction with contractors on-site.
Facility Manager	Ensuring adherence with all municipal and state regulations in regards to systems implementation (e.g., fire safety codes).
Facility Engineer	Provide expertise on facility infrastructure including but not limited to primary electrical and phone trunks, power grids/sources, demarcation locations and acts as the conduit with utility providers.
Property Owner/Lessor	Provides guidance and approval of equipment installation on/or within facility, acts as liaison with municipal and state inspectors.
Security Integrator/Contractor	Performs physical installation of security components as well as provides guidance on security implementation, future/end state, and national directives.

2

3

4 Planning and Budget

Planning and budgeting for Electronic Security Systems (ESS) is critical to the success of any project, or systems development life cycle (SDLC) supporting a security program. In addition to following internal agency guidelines for the planning, budgeting, and lifecycle management of ESS, CSOs should consider guidance provided in Federal Identity, Credential and Access Management (FICAM) efforts [FICAM Roadmap], chapter 10 (§10.1, Physical Access Implementation Planning) for planning and budgeting guidance for those systems.

Appendix A provides §10.1 of the [FICAM Roadmap].

This page left intentionally blank.

5 Information Technology Community

The Federal Information Security Management Act of 2002 (FISMA 2002) (hereafter "FISMA") requires each federal agency to develop, document, and implement an agency-wide program to provide information security (information assurance) for the information and information systems (IT) that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. It should be an Agency's practice to secure its information consistent with the provisions of FISMA based on availability of IT Security resources to the extent that FISMA and OMB guidance reflect best security practices.

Agencies are mandated to ensure adequate security controls are in place and operating to safeguard the confidentiality, integrity, and availability (known within the IT community as "CIA") of IT systems, commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to, or modification of, these systems. This includes assuring systems' security through the use of cost-effective management, personnel, operational, and technical controls.

As required by FISMA, the National Institute for Standards and Technology (NIST) provides technical standards and guidance to executive agencies on IT security. Most of the objectives identified below can be implemented using NIST guidelines in coordination with the agency's IT (and information assurance) department.

Federal agencies must meet the minimum security requirements through the use of the security controls in NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems [NIST SP 800-53]. NIST SP 800-53 contains the management, operational, and technical safeguards or countermeasures prescribed for an information system, enabling agencies to assess security controls considering the Risk Management Framework (RMF). The assessment identifies security controls in place, providing a determination on the level and quality of employed risk management framework, and provides information on strengths and vulnerabilities on physical security IT systems.

The controls selected or planned must be documented in a system security plan. NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology System provides guidance for the development of the System Security Plans (SSP) for IT systems in use within the federal government. The SSP provides an overview of the security requirements of the IT system and describes the controls in place or planned for meeting those requirements. The SSP also delineates responsibilities and expected behavior of all individuals who access or manage the system.

Physical security operations enabled or supported by IT systems determined to be classified Intelligence Community (IC) IT systems, shall comply with Intelligence Community Directive 503 (ICD 503) as required by the National Security Act of 1947, as amended.

The Identity, Credentialing, and Access Management Subcommittee publication, Personal Identity Verification in Enterprise Physical Access Control Systems [PIV in EPACS] provides recommended guidance to address NIST SP 800-53 requirements.

CSO's should assign an Information Systems Security Official (ISSO) that assumes responsibilities for ensuring that adequate IT Security is provided by:

- Assuring IT security control requirements are identified for all of the department's information systems and supported throughout the Life Cycle Management process.
- Supporting assessment and authorization activities for the department's major systems.
- Continuously monitoring management, technical and operational security controls to ensure they remain in place, are operational and effective.

5.1 Issues and Objectives for the CSO and CIO

As the policy and operations management official for the ESS, the CSO should collaborate with the CIO to establish standards for component connectivity over IT infrastructure.

- The CSO and CIO should develop a Memorandum of Agreement (MOA) documenting all components and boundaries of the ESS. Further, the MOA should define the cooperative work efforts and responsibilities of OCSO and OCIO. The MOA should contain the Configuration Management (CM) Policy, an approved products list (APL), the SSP, operation procedures and an approval process for interconnections to ESS systems.

As a service provider, the OCIO Staff should deliver and manage the infrastructure (e.g., Servers, Local Area Network (LAN), Wide Area Network (WAN), Metropolitan Area Network (MAN), etc.) on which the ESS components operate and intercommunicate, ensuring a heightened security environment for security operations (e.g., Virtual Private Network (VPN), IP Security (IPSec), etc.).

- The CSO and CIO should develop an Interagency Service Agreement (ISA) defining the cooperative work efforts between the Security Personnel and IT Personnel and established for the system owner (i.e., CSO) and the service provider (i.e., IT). In addition, a Service Level Agreement (SLA) specifying the levels of availability, serviceability, performance, or operation of the ESS should be developed and established between the system owner (i.e., CSO) and the service provider (i.e., CIO).

As the system owner, the CSO shall approve all interconnections to ESS components

- The CSO and CIO shall establish a Configuration Control Board (CCB) to enforce the Agency's Configuration Management (CM) Policy when it applies to ESS. The CCB should be chaired by the CSO as designated in the SSP. The board should be comprised of knowledgeable and qualified stakeholders in the ESS. The CCB shall review all new interconnections, system changes to ensure compliance with Agency CM and information assurance Policies. In lieu of an Agency CM Policy, NIST Special Publication 800-128, Guide for Security-Focused Configuration Management of Information Systems [NIST SP 800-128] provides guidance on developing CM policies and CCBs.
- When ESS resides or connects to the Agency's IT infrastructure, the CCB shall ensure any interconnections and system upgrades, are vetted through the Agency's main information systems CCB as directed by the CIO.

The CIO should coordinate with the CSO on all future upgrades and recapitalization plans to minimize or eliminate the effect on systems supporting security operations.

- The OCSO and OCIO should have a CM policy in place to address purpose, scope, roles, responsibilities, and procedures to facilitate the implementation of the CM policy and associated controls. The purpose of CM is to maintain the integrity of products through the product development life cycle from requirements specifications through design, development, testing, and production. CM is not an isolated practice: it exists to support product development and maintenance. The CM approval process includes designation of key management stakeholders responsible for reviewing and approving proposed changes to the information system, and security personnel who conduct an impact analysis prior to the implementation of any changes to the system. At a minimum, the Security Department's ISSO and senior physical security official should be designated as key stakeholders representing the CSO.

Require a security/vulnerability assessment as part of the Risk Management Framework (RMF) process (formally known as Certification and Accreditation (C&A)) for an IT system supporting security operations. An Authorizing Official will accept responsibility for the operation of the IT system and accept any risks identified through the RMF process. In some agencies, the CIO may serve as the Authorizing Official (AO), exercising final approval for the operation of an IT system supporting security operations. Individual agency policies must be consulted to confirm the official having final approval authority for the operation of IT systems supporting security operations.

- Agency Security and IT departments should have a Risk Assessment (RA) Policy in place that addresses purpose, scope, roles, responsibilities, and procedures to facilitate the implementation of the RA policy and associated RA controls. The purpose of the RA is to verify the security controls specified in the requirements adequately mitigate risk to the system and to identify any residual risk. It also provides assurance to the Security and IT departments that the system is capable of adequately protecting and processing sensitive information with known and acceptable risks. The RA is an essential component of both the security plan and the accreditation documentation. Often, an agency's IT department Authorization is the official management decision given by senior agency officials to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls.

- As a function of the RA Policy, an analysis of the threat to the information system must include analysis of the vulnerabilities associated with the system environment. The goal of this step is to develop a list of system vulnerabilities that could be exploited by potential threat-sources. A vulnerability is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised—accidentally triggered or intentionally exploited—and result in a security breach or a violation of the information system security policy. Table 2 below provides sample vulnerabilities, threat-sources, and threat actions:

Table 2: Vulnerabilities, Threat-Sources, and Threat Actions

Vulnerability	Threat-Source	Threat Action
Terminated employees. Users are not removed from the system	Terminated employees	Dialing into the company's network and accessing company proprietary data
Firewall allows inbound telnet, and guest ID is enabled on XYZ server	Unauthorized users (e.g., crackers, terminated employees, computer criminals, terrorists)	Using telnet to XYZ server and browsing system files with guest ID
The vendor has identified flaws in the security design of the software product; however, new patches have not been applied to the system	Unauthorized users (e.g., hackers, disgruntled employees, computer criminals, terrorists)	Obtaining unauthorized access to sensitive system files based on known system vulnerabilities
Data center uses water sprinklers to suppress fire; tarpaulins to protect hardware and equipment from water damage are not in place	Fire, negligent persons	Water sprinklers being turned on in the data center

Assist the CSO to obtain and secure the IT infrastructure necessary to accommodate uninterrupted access to, and use of ESS components.

- The initiation of an IT project begins with clearly identified requirements and an associated program need. It culminates in a closely coordinated effort between the program benefiting from the project and the IT Department to prepare a supportable business case for review and approval.
- As an addition to interagency guidance, this document provides background information at a level of detail sufficient to familiarize senior managers with the opportunities that may be realized through leveraging information technology. The problem to be addressed should be clearly expressed and, at a minimum, the business case should provide:
    - The project title;
    - A high-level description of what program function is being performed;
    - Why this IT project is being undertaken;
    - What is to be accomplished;
    - Efforts made to re-use what has already been accomplished by other projects;
    - Commitments, benefits, and performance measures;
    - High-level project milestone schedule and costs; and
    - Other issues or considerations that impact the decision, including significant assumptions and constraints.

- The process of developing a business case and submitting the project for approval begins, in fact, long before the development of detailed project plans because it is part of the annual strategic planning and budget formulation process. The development of business case documentation also will support the agency's information technology plan development and compliance with OMB A-11 guidance for developing Exhibit 300s. Once given approval to proceed, and having received appropriate funding, project managers begin the process of establishing an integrated project team and developing a project management plan.

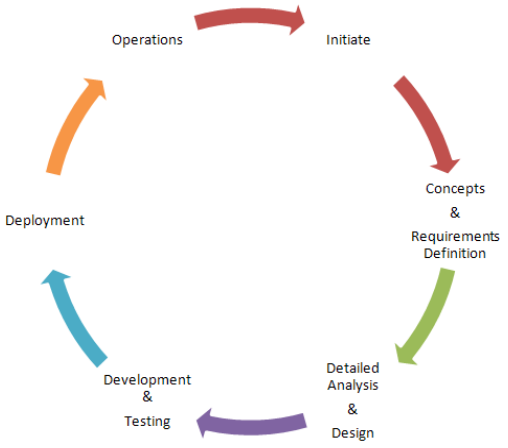
Provide guidance to responsible OCIO and OCSO teams to ensure standardization of PACS/ESS software, database, system, communication, and security compliance throughout the agency enterprise. Include methods and approaches to consolidating multiple legacies PACS/ESS to IP-enabled enterprise systems that can communicate through one or two central locations in lieu of individually managed stovepipe systems. Introduce PIV provisioning and PKI solutions to fully utilize the PIV cards as stated in the federated PACS guidance.

- The agency should establish Life Cycle Management (LCM) policies that define essential elements and assigns responsibilities governing the initiation, definition, design, development, deployment, operation, maintenance, enhancement, and retirement of the PACs. Life Cycle Management (LCM) is based on the rationale that certain events in the conceptual design, development, implementation, operation, enhancement, or replacement of PACs must be systematically planned, managed, and monitored. These events require specific management decisions and actions to ensure the system is developed and managed efficiently and economically, and that it meets program requirements. LCM emphasizes decision processes that influence system cost and usefulness. These decisions must be based on full consideration of program functional requirements and economic and technical feasibility in order to produce an effective system.

- Life Cycle Management consists of six phases, during each of which defined PACs project work products are created or modified. The phases are shown below in the figure:

Figure 1: Life Cycle Management Phases

  - *Initiation*
  - *Concept & Requirements Definition*
  - *Detailed Analysis & Design*
  - *Development & Testing*
  - *Deployment*
  - *Operations*



LCM phases may be tailored to accommodate the unique aspects of a PACs project if the resulting approach remains consistent with the primary LCM objective of delivering a

timely, quality system within cost. LCM phases show or demonstrate the evolutionary development strategy of PACs projects and the level of detail that provides.

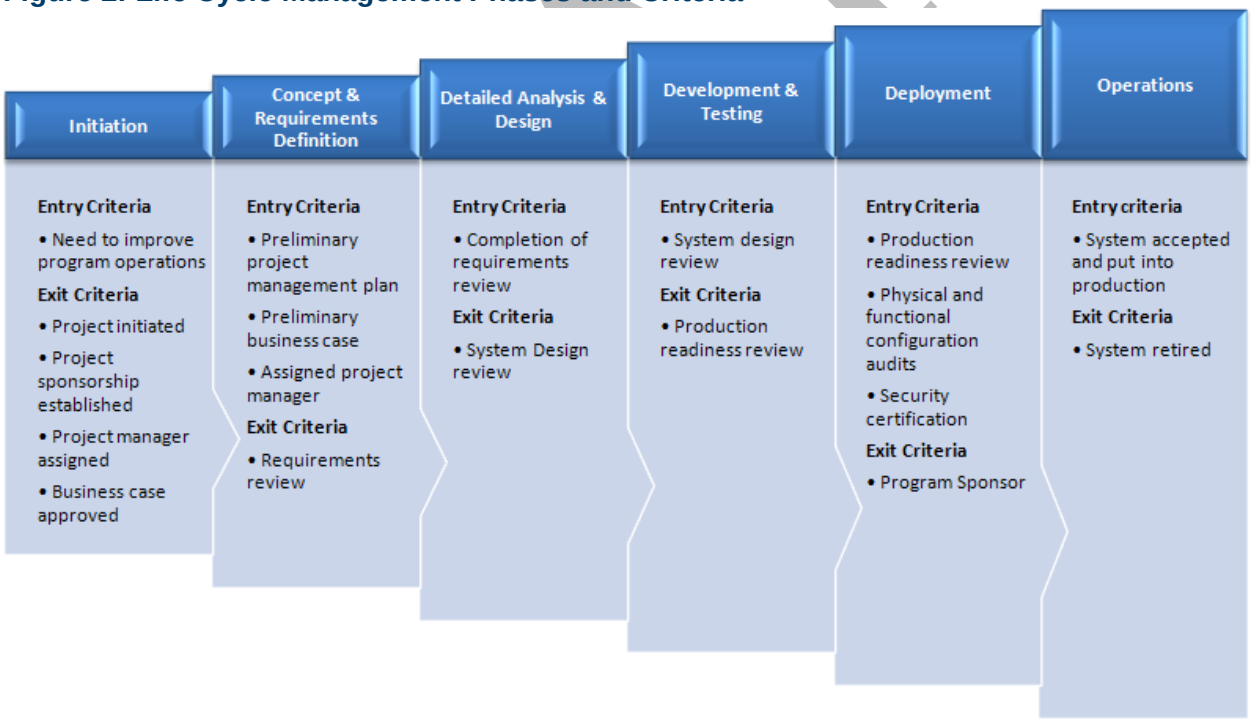
IT Security personnel/staff shall recommend to the CSO enhancements to the CIA of ESS components, as well as any enhancements to facilitate increased system capability, security and resilience.

- The SLA between the PhySec management and IT staff should include requirements to manage configuration changes and recommendations to the information systems. Managing configuration control is identified as the systematic proposal, justification, evaluation, coordination, approval or disapproval, and implementation of all approved changes in the configuration of the item after formal establishment of its baseline configuration.
- Changes must be approved by a Change Control Board (CCB) and maintained within a product change control tool. For the purpose of the ESS, the CCB should include the PhySec designated Information Systems Security Official.

5.2 Life Cycle Management Phases

Life Cycle Management consists of six phases, during each of which defined PACS or IT infrastructure project work products are created or modified. The phases are:

Figure 2: Life Cycle Management Phases and Criteria



Provide a roadmap to successfully implement an enterprise PACS/ESS, leveraging existing agency assets where possible.

- Agency Security and IT departments should develop Acquisition of Information Technology Products policy that includes information systems considerations and that addresses purpose, scope, roles, responsibilities, and documentation procedures to

facilitate system implementation. The policy should ensure products purchased comply with the requirements of OMB memorandum M-11-11, and are included on the General Services Administration (GSA) Approved Products List, and address:

- Allocation of Resources;
- Life Cycle Support;
- Acquisitions;
- Information System Documentation;
- Software Usage Restrictions;
- User-Installed Software;
- Security Engineering Principles;
- External Information System Services;
- Developer Configuration Management; and
- Developer Security Testing.

- Please note designated major systems must identify IT security costs in the OMB Exhibit 300 Capital Plan and Business Case and companion OMB Exhibit 53 on IT expenditures.
- The solicitation documents (e.g., Requests for Proposals) for information systems and services must include security requirements that describe: 1) required security capabilities; 2) required design and development processes; 3) required test and evaluation procedures; and 4) required supporting documentation.

Update agency approved products list to include IP-enabled ESS hardware and software to assist agencies with selecting systems and FISMA requirements.

- As referred in NIST 800-53, PM-5 INFORMATION SYSTEM INVENTORY: The organization develops and maintains an inventory of its information systems. This control addresses the inventory requirements in FISMA. OMB provides guidance on developing information systems inventories and associated reporting requirements.
- Reference: Information Technology Management Reform Act of 1996 (Public Law 104-106), August 1996. Federal Information Security Management Act of 2002 (Public Law 107-347), December 2002.

Establish executive level documentation providing federal standards that apply to government-owned IT systems.

- FISMA requires the management, operational, and technical controls in each information system, contained in the inventory of major information systems, be assessed with a frequency depending on risk, but no less than annually. The FISMA requirement for (at least) annual security control assessments should not be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security certification and accreditation process. Security Assessment Reports (SAR) document assessment results in sufficient detail as deemed necessary by organizations to determine the accuracy and completeness of the reports and whether security controls are

implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements.

- Figure 3 provides an example of a **Security Assessment Report** (SAR).

Develop standard definitions for system roles such as owner, end-user, administrator, etc.

- Each agency should consider different sets of account management rules based on user roles and responsibilities. For example, differentiating between the rules that apply to privileged users and rules that apply to general users. Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency identifies authorized users of the PACs and specifies access rights/privileges. The organization grants access to the PACs based on: (i) a valid need-to-know/need-to-share determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage.[1]

Develop an SSP for the ESS equipment.

- Agency Security Departments should develop and implement a security plan for PhySec and PACS systems that provides an overview of the security requirements for the systems and a description of the security controls in place or planned for meeting those requirements. Designated Officials within the organization review and approve the plan. The security plan should document controls and be aligned with the organization's information system architecture and information security architecture.

- This document outlines the plan and associated information developed by the CSO for mitigating risk to the security of the security systems. This plan is developed to reduce the risk and magnitude of harm that could result from the loss, destruction, misuse, unauthorized access to, modification, or unavailability of information for these sub systems.

- This plan should be a living document requiring frequent reviews, updates, modifications and plans of action to implement security controls throughout the system lifecycle. The SSP should be utilized and analyzed during the Risk Management Framework (RMF) process (formerly known as Certification and Accreditation) and be verified that it addresses all the security categories required to counter threats and vulnerabilities. In addition, this plan assists in determining whether current and planned security measures are adequate.

- This Document sets forth activities planned to ensure successful completion of the RMF by the Program Sponsor and the CIO. This plan documents the process for ensuring adequate and cost effective security protection for these systems.

- NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology System* provides guidance for the development of the system Security Plans (SSP) for IT systems in use within the federal government. The SSP provides an overview of the security requirements of the IT system and describe the controls in place

[1] NIST Special Publication 800-18 [NIST SP 800-18], Rev. 1 is germane

or planned for meeting those requirements. The SSP also delineates responsibilities and expected behavior of all individuals who access or manage the system.

- At a minimum the SSP should contain the following parts:
  - Roles and Responsibilities:

    The SSP should delineate the roles and responsibilities of various personnel. This is a basic and brief listing of the roles but may change as different agencies utilize different organizational structure and titles:

    - Chief Information Officer;
    - Information Technology System Owner;
    - Information Owner;
    - Senior Agency Information Security Officer;
    - Information System Security Officer;
    - Authorizing Official; and
    - System Boundaries.
  - The SSP should clearly define system boundaries based on the risk assessment. Security controls then can be implemented based on Agency policies, current threats and cost benefit analysis. By utilizing Security Controls selected in accordance with NIST 800-53¸ information systems should at a minimum meet FIPS200 requirements for federal information systems and additional requirements based on the risk assessment.
  - Plan Development:
    - The SSP should include a plan development explaining how the SSP maximizes the use of NIST standards to effectively implement security controls throughout the lifecycle of the system. There should be a policy on how the SSP will be controlled and accessed prior to initiation of the activity.
    - System Security Plan (Attached Sample)

Figure 3: Security Assessment Report Example

CNTL	CONTROL NAME	Priority	LOW	MOD	SATISFIED	OTHER	N/A	LOW Common Control	MOD Common Control	Policy & Procedure References	Recommendations (POA&M to Fix, Waiver, or Exception to Accept Risk)	FY08	FY09	FY10	FY11	FY12	FY13
AU-11	Audit Record Retention	P3								TSG IT-930-02 IT-930-TN02		o			T		
AU-12	Audit Generation										REV 3 Added			R	I	T	
AU-13	Monitoring for Information Disclosure		NS	NS							REV 3 Added						
AU-14	Session Audit		NS	NS							REV 3 Added						
CA-1	Security Assessment and Authorization Policies and Procedures							C	C	TSG IT-930-02 TSG IT-930-01	OCIO Security Program Reviews Policy Control w/Sinet Pkg Systems must implement			U	U		
CA-2	Security Assessments	P2		(1)				C	C		Volatile Control. Annual Assessment - See FISMA Scorecard	o		T	T	T	T
CA-3	Information System Connections									IT-930-TN22		o			T		
	CA-4 Security Certification (Withdrawn See CA-2)											o					
CA-5	Plan of Action and Milestones	P3								TSG IT-930-02 TSG IT-930-01 **QTR Report to OCIO & OPMB**	Volatile Control. Quarterly Reporting	o		U	U	U	U
CA-6	Security Accreditation	P3										o			T		
CA-7	Continuous Monitoring	P3								TSG IT-930-02 Appendix E.2 TSG IT-930-01 **QTR Report to OCIO**	Volatile Control. Annual Scans	o		T	T	T	T
CM-1	Configuration Management Policy and Procedures							C	C	TSG IT-930-02 IT-920-TN02 IT-920-TN03 IT-940-01 IT-960-TN01 IT-960-TN02 IT-960-TN16 IT-960-TN18	OCIO Security Program Review Policy Control w/Sinet Pkg Systems must implement			U	U		
CM-2	Baseline Configuration			(1) (2) (4)				C	C	IT-960-TN24	OCIO Identifies all standard CIS / FDCC Baselines		---	T	T	T	T
CM-3	Configuration Change Control		NS	(2)						TSG IT-930-02 IT-920-TN02 IT-960-TN01	Sinet reports FDCC status All Major Systems must report baseline Status			T	T	T	T
CM-4	Security Impact Analysis	P2								TSG IT-930-02 Appendix E.8 IT-920-TN02 IT-960-TN01	Volatile Control. Annual Assessment REV 3 Added for Low			R	I	T	
CM-5	Access Restrictions for Change		NS										---			T	
CM-6	Configuration Settings			(3)						IT-960-TN16 IT-960-TN31	All Major Systems must report deviations against SI baselines See FISMA Scorecard CM Sinet reports FDCC baseline		---	T			T
CM-7	Least Functionality			(1)						IT-960-TN16 IT-960-TN31	REV 3 Added for Low		---			T	
CM-8	Information System Component Inventory			(1) (5)						IT-920-TN02 IT-960-TN01 IT-960-TN16			---	T			T
CM-9	Configuration Management Plan		NS								REV 3 Added for Moderate			R	I	T	

6 Acceptance of the Personal Identity Verification Interoperable Credential in the Federal Government

In May 2009, the Federal Chief Information Officer Council (FCIOC) issued guidance for the minimum federal requirements for Personal Identity Verification Interoperable (PIV-I) Credentials. Entitled *Personal Identity Verification Interoperability for Non-Federal Users* (herein called PIV-I Guidance), the guidance "…provides solutions for overcoming the barriers to federal reliance on non-federal identity cards." The PIV-I Guidance provides "…a minimum set of requirements that will allow Non-Federal Issuer identity cards to technically interoperate with Federal government PIV systems and be trusted by Federal government relying parties."

To enable interaction (i.e., interoperability) with federal infrastructure, the PIV-I Guidance calls on various National Institutes of Standards and Technology (NIST), and Office of Management and Budget (OMB) guidance documents to define the requirements that must be satisfied to become a federal government trusted PIV-I Credential. The PIV-I Guidance requires the topology must enable differentiation between a federal government issues credential (i.e., PIV Credential) and a PIV-I Credential; however, the electronic portion of the PIV-I is virtually the same as that of the U.S. Government (USG) issued PIV Credential.

Divergence from the USG PIV Credential is also found in the identification and background vetting process associated with Non-Federal Issuer's issuance of a PIV-I. The PIV-I Guidance states:

> The Federal background vetting process (e.g., NACI) is performed in order to determine an individual's suitability/fitness to work for or on behalf of the Federal government and is not applicable to Non-Federal Issuer identity cards. For purposes of PIV Interoperability, Non-Federal Issuers need to concern themselves only with satisfying the identity proofing requirements for E-Authentication Assurance Level 4.

The basis for issuing an Assurance Level 4 credential is found in NIST Special Publication 800-63-2, Electronic Authentication Guideline (August 2013), [NIST SP 800-63-2] that requires:

> In person appearance and verification of: a) a current primary Government Picture ID that contains Applicant's picture, and either address of record or nationality of record… and; b) either a second, independent Government ID document that contains current corroborating information…, OR verification of a financial account number… confirmed via records… Note: Address of record shall be confirmed through validation of either the primary or secondary ID.[2]

In Congressional testimony, the Office of Personnel Management (OPM) stated that the National Agency Check with Written Inquiries (NACI) is "…the minimum investigation required for identification purposes."[3] OPM further stated:

[2] NIST SP 800-63-22 defines valid as, "In reference to an ID, the quality of not being expired or revoked" (p. 15).

[3] Hearing on Federal Security: ID Cards and Background Investigations, April 9, 2008. Kathy L. Dillaman, Associate Director, Federal Investigative Services Division, Office of Personnel Management, before the Committee on Oversight and Government Reform Subcommittee on Government Management, Organization, and Procurement, U.S. House of Representatives.

> [The] National Agency Check (NAC) portion of any background investigation includes searches of the investigation databases maintained by OPM, the Department of Defense (DOD), and the Federal Bureau of Investigation (FBI), and the fingerprint-based national criminal history check.[4]

OPM continued holding that the NACI "…also generates letters of inquiry to former employers, supervisors, educational institutions, and other references to identify suitability or security concerns." As stated in the FCIOC's PIV-I Guidance, NACI's are not conducted to meet the minimum federal requirements for issuance of PIV-I Credentials at level of assurance (LA) level 4 (the highest assurance level).

One focus of the Identity, Credentialing and Access Management Subcommittee (ICAMSC)[5] is to leverage the use of PIV-I credentials within USG facilities and information technology (IT) resources.[6] Table 3 provides the Federal Identity, Credentialing and Access Management (FICAM) Roadmap and Implementation Guidance Document's Version 2.0 (The Document) comparison of the PIV and PIV-I Credentials. In its comparison of the USG issued and Non-Federal Issuer issued credentials, the document reflects that the identity proofing and background investigation requirements for the PIV-I satisfy LOA 4, defined by OMB memorandum M-04-04 as "Very high confidence in the asserted identity's validity…,"[7] and reiterated by NIST SP 800-63-2. Further, the PIV-I Credential satisfies "…multi-factor authentication as defined in NIST SP 800-116."[8]

The Document directs that "…PIV-interoperable [PIV-I] specifications do not apply to individuals for whom HSPD-12 policy is applicable per M-05-24 . . . (i.e., federal employees and contractors with long-term access to federal facilities and information systems)."[9] The document further adds:

> Each Federal Executive Branch Agency is responsible for the following ICAM transition initiatives: . . . **Initiative 6: Fully Leverage PIV and PIV-I credentials**; Includes a wide variety of activities required to meet the intent of HSPD-12 for the usage of PIV credentials, as well as activities to leverage externally-issued credentials that are compliant with PIV-I specifications and can be trusted by the Federal Government at E-authentication level 4.

[4] The NACI requires the submission of fingerprints to the FBI National Criminal History Check (NCHC) database to check for criminal records based on fingerprint comparison.

[5] The Identity, Credentialing and Access Management Subcommittee (ICAMSC), is a subcommittee of the Federal Chief Information Officer Council's Information Security and Identity Management Committee (ISIMC). The ICAMSC is the successor to the now defunct Federal Identity and Credentialing Committee (FICC).

[6] Federal Identity, Credentialing and Access Management (FICAM) Roadmap and Implementation Guidance Document's Version 2.0: Performance gap #6, #11 (p. 142), #18, and #22 (p. 143).

[7] Although the PIV-I can be verified electronically to comply with federal guidance, national level guidance does not provide a capability to ascertain if a Non-Federal Issuer is properly conducing identification vetting.

[8] National Institutes of Standards and Technology Special Publication 800-116 (NIST SP 800-116), A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS), defines **Multi-Factor Authentication** as "authentication based on more than one factor. In some contexts, each factor is a different authenticator. In other contexts, each factor is one of "something you know, something you have, something you are" (i.e., memorized fact, token, or biometric) and thus the number of factors is 1, 2, or 3" (p. 9).

[9] Footnote 3, page iv.

OMB memorandum M-11-11 dated February 3, 2011, mandates that all Federal Executive Branch (FEB) entities align with the document.[10] Therefore, each FEB entity must implement a capability to accept PIV-I Credentials for access to their assets (i.e., facilities and/or information technology resources). The document also states,

> **Acceptance and use of PIV-I credentials**. While PIV-I credentials are technically interoperable with the PIV infrastructure, an agency needs to decide if any additional requirements or processes should be required for acceptance and use of the PIV-I card.

Moreover, the document continues:

> There are certain situations in which a federally-issued PIV-I credential can address the unique needs of a specific group within an agency's population. If an agency chooses to issue PIV-I credentials, they must fully comply with all applicable PIV-I specifications and policies.

In 2005, Congress passed and the President signed into law the REAL ID Act of 2005 (P.L. 109-13, Division B) (hereafter "REAL ID"). REAL ID created the requirements for issuance standards for the issuance of identity documentation, and "…prohibits Federal agencies . . . from accepting a driver's license or personal identification card issued by a U.S. State for any official purpose unless the license or card has been issued by a State that meets the requirements set forth in the Act [REAL ID]."[11] Section 202 of REAL ID further required the vetting of an individual's identity prior to issuance of identity documentation. Initial seed documentation such as birth certificates can be cumbersome. However, positive proof of an individual's identity is the inferred focus of REAL ID.

Authenticity of an individual's identity is established at birth, and through various stages of an individual's life, additional documentation such as a social security card, driver's license, a student identification, or an employment identification (e.g., company access control token/card), is acquired, each using another to verify and bind an individual's identity to identification documents. As the PIV Credential established as a result of HSPD-12, identification documents that comply with REAL ID can be considered trusted, non-fraudulent documentation reflecting the individual's true and legal identity.

On March 7, 2011, the DHS issued a final rule on the Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes. In the final rule, the DHS extended the compliance deadline, thereby granting States until January 15, 2013, to satisfy the requirements of REAL ID. As of the writing of this document, less than 20-States have issued a driver's license or identification card that complies with REAL ID. DHS does not currently provide, nor are there plans to provide, a readily available reference that reflects what is the criterion that must be met to satisfy the requirements of REAL ID (i.e., what minimum requirements must be met to satisfy REAL ID). Further, at the time of the release of this document, DHS was posting a list of States which "have met the [REAL ID] Act's

[10] "The government-wide architecture and completion of agency transition plans must align as described in the Federal CIO Council's "Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance" (Bullet number 5, p. 2).

[11] DHS Final Rule: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes (see Background).

requirements". That web site can be found at http://www.dhs.gov/real-id-faq-determinations. The title of the page is "REAL ID Frequently Asked Questions for DHS Determinations".

CSO's must develop and implement procedures for accepting PIV-I credentials for access to USG assets. Where Supervisory Control and Data Acquisition (SCADA) systems are in service or employed within a department or agency, the CSO should provide at a minimum concurrence approval for the use of PIV-I credentials with IT systems whether the PIV-I is used remotely or on-site.

Table 3: PIV and PIV-I Characteristics Comparison

Characteristic	PIV	PIV-I
Terminology	An identity card that is fully conformant with federal PIV standards. Only cards issued by federal entities can be fully conformant. Federal standards ensure that PIV cards are interoperable with and trusted by all Federal Government relying parties.	An identity card that meets the PIV technical specifications to work with PIV infrastructure elements such as card readers, and is issued in a manner that allows Federal Government relying parties to trust the card.
Visual Card Topology	• Fully conforms to the PIV card visual topology defined in FIPS 201 and SP 800-106. • Contains all mandatory items on the front and back of the card. • All optional items are formatted and placed in accordance with the standard, if used.	• Must be visually distinct from PIV card topology to ensure no suggestion of attempting to create a fraudulent PIV card. • Must contain, at a minimum: - Issuing/Sponsoring Organization - (e.g., company name) - Card holder Photograph - Card holder Full Name - Card Expiration Date
Technical Requirements	Fully conformant with federal PIV standards (i.e., FIPS 201 and related documentation).	Must conform to the NIST technical specifications for a PIV Card as defined in SP 800-73 and meet the cryptographic requirements of FIPS 140 and SP 800-78.
Identifier(s)	• Mandatory CHUID data object conformant with requirements in SP 800-73. • Unique Federal Agency Smart Credential Number (FASC-N) assigned to each individual. • Conformant GUID present in the • CHUID.	• Valid RFC 4122 generated Universally Unique Identifier (UUID), in accordance with SP 800-73, in the GUID field of the CHUID. • FASC-N with Agency Code equal to 9999, System Code equal to 9999, and Credential Number equal to 999999, indicating that the UUID is the primary credential identifier.

Identity Proofing and Background Investigation	• Identity proofing satisfies SP 800-63, Level of Assurance (LOA) 4. • NACI background investigation or equivalent.	• Identity proofing satisfies SP 800-63, LOA 4. • No background investigation required.
Digital Certificate Issuance	PIV certificates are issued in direct compliance with federal certificate policies (i.e., COMMON).	PIV-I certificates are issued under their own policies that are cross-certified at the Federal Bridge at specific assurance levels and may be honored by relying agencies at those levels.
Card Authentication Key (CAK)	The CAK is optional on PIV cards.	The CAK is mandatory on PIV-I cards.

1

2

This page left intentionally blank.

7 References

Table 4: Referenced Documents

Document	Description
[FICAM Roadmap]	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance Version 2.0, December 2, 2011.
[NIST SP 800-18]	Information Security, Rev. 1.
[NIST SP 800-53]	Recommended Security Controls for Federal Information Systems and Organizations.
[NIST SP 800-63-2]	Electronic Authentication Guideline
[NIST SP 800-128]	Guide for Security-Focused Configuration Management of Information Systems.
[OMB M-06-18]	Acquisition of Products and Services for Implementation of HSPD-12, (June 30, 2006).
[PIV in EPACS]	DRAFT - Personal Identity Verification in Enterprise Physical Access Control Systems Version 2.0.2. January 31, 2013.

This page left intentionally blank.

8 ISC Participants

The Interagency Security Committee wishes to thank the members of the Convergence Subcommittee for the development of this white paper.

Subcommittee Chair

Will Morrison, CPP
Federal Aviation Administration

ISC Facilitator

Bernard Holt

Members

Marc Brooks
Department of Defense

James Hammond, Jr.
Central Intelligence Agency

Darryl Hawthorne
US Marshals Service

Kathi Kennedy
Central Intelligence Agency

Brett Knutson
US Marshals Service

Jeff McClure
Department of Energy

Hugh Meehan
Smithsonian Institute

Jason Rosen
National Aeronautics and Space Administration

Levron Schuchalter
General Services Administration

Todd Tangye
General Services Administration

This page left intentionally blank.

List of Abbreviations/Acronyms/Initializations

TERM	DEFINITION
ADA	Americans with Disabilities Act
AO	Authorizing Official
APL	Approved Products List
CAC	Common Access Card
CAK	Card Authentication Key
CAO	Chief Acquisitions Officer
CCB	Configuration Control Board
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CHCO	Chief Human Capital Officer
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CSO	Chief Security Officer
CCVE	Closed-Circuit Video Equipment
CHUID	Card Holder Unique Identifier
CM	Configuration Management
DBT	Design-Basis Threat
DHS	Department of Homeland Security
DoD	Department of Defense
E-Authentication	Electronic Authentication
ESS	Electronic Security System
FASC-N	Federal Agency Smart Credential Number
FBI	Federal Bureau of Investigation
FCIOC	Federal Chief Information Officer Council
FEB	Federal Executive Branch
FICC	Federal Identity and Credentialing Committee
FICAM	Federal Identity, Credentialing and Access Management
FIPS	Federal Information Processing Publication
FISMA	Federal Information Security Management Act

TERM	DEFINITION
FMR	Federal Management Regulations
FSA	Facility Security Assessment
FSC	Facility Security Committee
FSL	Facility Security Level
GSA	General Services Administration
GUID	Global Unique Identifier
HSPD	Homeland Security Presidential Directive
IC	Intelligence Community
ICAM	Identity, Credentialing and Access Management
ICAMSC	Identity, Credentialing and Access Management Subcommittee
ICD	Intelligence Community Directive
ID	Identification
IDS	Intrusion Detection System
IP	Internet Protocol
IPv6	Internet Protocol version 6
ISSO	Information Systems Security Official
FICAM	Federal Identity, Credential, and Access Management
IP	Internet Protocol
IPSec	Internet Protocol Security
ISA	Interagency Service Agreement
ISC	Interagency Security Committee
IT	Information Technology
LAN	Local Area Network
LCM	Life Cycle Management
LOA	Level of Access
MAN	Metropolitan Area Network
MIST	Modified Infrastructure Survey Tool
MTBF	Mean Time Between Failure
MTTR	Mean Time To Recovery
NAC	National Agency Check
NACI	National Agency Check with Written Inquiries

TERM	DEFINITION
NCHC	National Criminal History Check
NFPA	National Fire Protection Association
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
OA	Office Automation
OCIO	Office of the Chief Information Officer
OCSO	Office of the Chief Security Officer
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PACS	Physical Access Control System
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification Interoperable
PSC	Physical Security Criteria
RA	Risk Assessment
RFP	Request for Proposal
RMF	Risk Management Framework
RS	Recommended Standards
SAR	Security Assessment Report
SCADA	Supervisory Control and Data Acquisition
SDLC	System Development Life Cycle
SLA	Service Level Agreement
SSP	System Security Plan
UUID	Universal Unique Identifier
US (or U.S.)	United States
USC	United States Code
USG	United States Government
VPN	Virtual Private Network
WAN	Wide Area Network

1

2

This page left intentionally blank.

Glossary of Terms

TERM	DEFINITION
Agency	An inclusive term that includes federal executive branch cabinet-level departments and agencies, and bureaus.
Authorizing Official	A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Base Documents	The collection of Federal Government and ISC documents known as the Modified Infrastructure Survey Tool (MIST), the Facility Security Level (FSL) Determinations for Federal Facilities, Facility Security Committee Standards (FSC), Physical Security Criteria for Federal Facilities (PSC), and the Design-Basis Threat Report (DBT).
Chief Information Security Officer (CISO)	An Agency official, responsible to the Chief Information Officer (CIO) for the development of policies, procedures, and control techniques to address information assurance for an Agency.

TERM	DEFINITION
Chief Security Officer (CSO)	The senior official having authority over traditional security programs for a department, agency, or bureau. The CSO is responsible to the agency's senior management (i.e., Secretary, Administrator, or Director) for the development, implementation, and oversight of security policies effecting traditional security.
Closed-Circuit Video Equipment (CCVE)	Electro-mechanical equipment employed by security professionals to provide video surveillance capabilities, including cameras, television/monitors, recording equipment, et alia.
Convergence	A collaborative effort to enhance security through integrating operational Physical Security, and Information Assurance processes, to protect federal government assets.
Electronic Security System (ESS)	Electro-mechanical equipment employed by security professionals to provide for the security posture for an organization (e.g., Closed-Circuit Video Equipment (CCVE), Intrusion Detection System (IDS), Physical Access Control System (PACS)).
Facility Security Assessment	An analysis performed by a security specialist, examining and evaluation a facility's (or campus, etc.) infrastructure and operations, considering possible threats, risks, vulnerabilities, and existing countermeasures, procedures and operations to determine the proposed Facility Security Level, recommended mitigation strategies and potential risk acceptance.
Federal Identity, Credential, and Access Management (FICAM)	An effort of the Federal Chief Information Officer Council (FCIOC) to establish a common framework and approach for the implementation of Homeland Security Presidential Directive 12 (HSPD-12) and other affiliated national-level directives.
Information Assurance	Processes, policies, and procedures employed to ensure the Confidentiality, Integrity, and Availability (or CIA) of information technology (IT) infrastructure, to included data stored within IT systems.
Information Owner	The official responsible for the statutory and operational authority for specified information and responsible for establishing the controls for its generation, collection, processing, dissemination and disposal.
Information Technology (IT)	Applied computer systems - both hardware and software; often including networking and telecommunications medium, usually in the context of a business or other enterprises.
Information Technology System Owner	The official responsible for the development, procurement and maintenance of the Information System

TERM	DEFINITION
Interagency Service Agreement (ISA)	A document, generally between government departments, agencies and divisions that defines cooperative work between the different entities. The agreement will define the parties involved, work to be performed, the transfer of technologies, and funds, et cetera. The document identifies the type and amount of support each entity will provide to each other.
Internet Protocol (IP)	A telecommunications protocol enabling automated data processing systems (computers) and other similar devices to communicate using a common set of rules over telecommunications networks.
Internet Protocol version 6 (IPv6)	An updated set of IP rules. A major enhancement of IPv6 is the increase of address availability for networked devices.
Intrusion Detection System (IDS)	A system of electro-mechanical devices enabling remote sensing of the status of portals and perimeter demarcations.
Local Area Network (LAN)	A data telecommunications network which is geographically limited allowing easy interconnection of terminals, microprocessors and computers within and between adjacent buildings.
Mean Time Between Failures (MTBF)	The average time (usually expressed in hours) that a component works without failure. It is calculated by dividing the total number of failures into the total number of operating hours observed. The term can also mean the length of time a user may reasonably expect a device or system to work before an incapacitating fault occurs.
Mean Time To Recovery (MTTR)	The average time that a device will take to recover from a non-terminal failure. Examples of such devices range from self-resetting fuses (where the MTTR would be very short, probably seconds), up to whole systems which have to be replaced. The MTTR should be part of a maintenance agreement/contract. The MTTR is the timeframe the servicing organization is guaranteeing to have the system up and running again (e.g., Within 30-minutes, 24 hours, 5 working days of the failure).
Metropolitan Area Network (MAN)	A data telecommunications network intended to serve an area the size of a large city.
Office Automation (OA)	The use of computers or related data processing technology to perform work (e.g., clerical work (e.g., word processing, spreadsheets, database entry), electronic mail, filing and distributing of documents).
Physical Access Control System (PACS)	A system or collection of systems designed to provide access control to tangible and intangible assets through the use of electro-mechanical and other real devices.
Programmable Logic Controller	A device used to automate monitoring and control of industrial plant.

TERM	DEFINITION
Service Level Agreement (SLA)	An agreement where a service is formally defined. In practice, the term SLA is sometimes used to refer to the contracted delivery time (of the service or performance). As an example, internet service providers will commonly include service level agreements within the terms of their contracts with customers to define the level(s) of service being performed in plain language terms. In this case the SLA will typically have a technical definition in terms of mean time between failures (MTBF), mean time to repair or mean time to recovery (MTTR); various data rates; throughput; jitter; or similar measurable details.
Supervisory Control and Data Acquisition (SCADA)	Systems are used in industry to monitor and control plant status and provide logging facilities. SCADA systems are highly configurable, and usually interface to the physical plant via Programmable Logic Controllers.
Traditional Security	Security processes established by organizations prior to the advent of automated data processing systems. Those processes include anti-terrorism force protection, counterintelligence, counterterrorism, intelligence, resiliency, risk management & mitigation, and industrial, information, operational, personnel, and physical security.
Wide Area Network (WAN)	A data telecommunications network, usually constructed with serial lines, extending over distances greater than one mile/kilometer.

1

2

This page left intentionally blank.

Appendix A: Modernized PACS Infrastructure

Excerpted from the FICAM Roadmap dated December 2011

[**Note***: As much as possible, the formatting of this section replicates what is found in the FICAM Roadmap. Although the pagination aligns to this document, the footnote sequencing aligns to the original source material, as do the section headings and figure/table captions.*]

10. Initiative 7: Modernize PACS Infrastructure

Initiative 7, as introduced in Section 5.2.2, is an agency-level ICAM implementation initiative that includes activities associated with upgrading PACS for routine access for PIV cardholders and standardized visitor access for individuals with other acceptable credentials. As defined in the ICAM segment architecture, a PACS is an automated system that manages the passage of people or assets through an opening(s) in a secure perimeter(s) based on successful authentication and associated authorization rules. The target state calls for a modernized PACS, which includes the following characteristics:

- Electronically authenticates PIV cards and accepts multi-factor authentication as defined in NIST SP 800-116;[206]
- Supports an agency-wide approach to managing physical access services that links individual PACS via an enterprise level network wherever possible and appropriate, while maintaining local control over authorization decisions;
- Interfaces with authoritative Identity Providers and data source(s) to supply user
- attributes and credential information for automated provisioning and de-provisioning; and
- Incorporates technologies that support secure, automated processes for requesting and provisioning visitor access.

The guidance provided in this chapter is intended to help agencies achieve the target state presented in the ICAM segment architecture Use Case 8, Grant Physical Access, and the associated transition activities listed in Section 5.2.2.3.

This chapter is organized into the following five sections:

- Physical Access Implementation Planning. This section discusses the activities and processes that are necessary to properly plan for a modernized PACS implementation within an agency. It includes existing standards and guidance, PACS program governance, facility risk assessments, program funding, and schedule planning considerations that are necessary to properly plan for a physical access deployment within an agency.
- Physical Access Architecture and Design. This section describes the architecture, components, and key design characteristics common to a modernized PACS solution.
- Physical Access Technical Implementation. This section covers common technical considerations for deploying PACS solutions within federal agencies, including automated provisioning and physical access scenarios.

[206] SP 800-116, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS), NIST, November 2008. [SP800-116]

- Local Facility Access. This section presents guidance concerning populations that need long-term local access but are ineligible (i.e., individuals other than federal employees and contractors) for a PIV card.
- Visitor Access. This section discusses common requirements of a Visitor Management
- System (VMS) and other visitor access considerations.

10.1. Physical Access Implementation Planning

Providing reliable, robust physical security for its facilities and buildings is an important responsibility for each agency. Additionally, physical security systems and procedures affect a variety of users accessing federally-controlled facilities every day. As such, implementations of modernized PACS solutions should be planned carefully to ensure success and prevent disruptions to operations. Typically, decisions related to the selection and implementation of PACS has been determined at the individual site level. As agencies move towards achieving the target state, planning for a modernized PACS at the enterprise level offers many benefits, including cost savings achieved from enterprise software licenses, decreases in redundant collection and management of user identity data, and improved security through increased consistency. Additional advantages are discussed throughout the rest of this chapter.

This section is targeted largely at those individuals responsible for setting the direction for and planning an agency's PACS modernization effort. It will explore key aspects of implementation planning, including: program governance, facility risk assessments, program funding, and schedule planning. The OMB memorandum released on May 23, 2008[207] provides agencies with additional guidelines for consideration when planning or updating plans for the use of the PIV card in their PACS, a central aspect of the ICAM target state. In addition, the ICAM Reporting Template provides a detailed list of activities associated with implementing the ICAM segment architecture.

FAQ	
Does Physical Access Control System (PACS) infrastructure modernization require the use of an electronic PACS at every facility? No. Selection of security countermeasures, including PACS, should be based on the risk assessment of a facility. Other access control approaches, such as lock and key, might provide adequate security and be more cost effective for an exceptionally low risk facility. As agencies develop their implementation plans in accordance with ICAM, they should first focus on the highest-risk facilities for PACS modernization. Over time, this should expand to lower-risk facilities in order to leverage the PIV credential wherever possible.	

The information and guidance presented in this section is intended to assist agencies in providing answers to several common questions related to physical access implementation planning, including:

- How can my agency coordinate management of its PACS modernization efforts?
- How can my agency perform risk assessments on its facilities?

[207] Guidance for Homeland Security Presidential Directive 12 (HSPD-12) Implementation, OMB, May 23, 2008. [HSPD-12]

- What should my agency consider when funding its PACS implementation?
- What are the necessary steps required when planning and executing a PACS implementation?

10.1.1. Program Governance

Chapter 6 provides guidance concerning overarching ICAM governance at the agency level. This section is intended to supplement that guidance and highlight specific areas that agency governance bodies should seek to address at an enterprise or component/bureau level to enable successful PACS modernization efforts. For example, as part of the planning for a PACS implementation, an agency should leverage its ICAM governance structure to coordinate the PACS-related activities and investments across the bureaus/components and foster effective communication and cooperation with other efforts, such as logical access and information technology. Formalizing program governance for an agency's PACS effort within the ICAM governance structure can ensure that change is managed properly, communications are delivered effectively, and that policy is created or refined to support the target state.

Implementation Tip

To increase effectiveness, PACS governance should be made up of decision makers from each bureau/component. For example, the Change Control Board (CCB) for

USDA's enterprise PACS implementation, ePACS, includes representatives from each of its sub-agencies who are educated on PACS policies and help ensure activities and efforts at their sub-agencies meet USDA policies and common requirements.

The transition to a modernized PACS needs to incorporate an appropriate change management approach to ensure that stakeholders embrace the changes associated with the implementation. An agency should take advantage of the many tools associated with effective change management, including following a project plan, developing communication tools, and conducting training. The approach should also include steps to reinforce change such as monitoring effectiveness, building stakeholder buy-in, and celebrating successes.

Communication is important throughout the change management process and also plays a key role in the other transition activities associated with modernizing a PACS. Because physical security and access to buildings affects all government employees, contractors, and visitors, communication with and education of the end-user population can significantly impact the success of the implementation. For example, the PACS governance team should plan for and communicate any revised policy and new procedures that are created early and often. Additionally, as new ICAM services are deployed, an agency should communicate key changes to its user populations well in advance to avoid disruptions. The communication options and delivery media presented in Section 6.1.3.1 of this document can be leveraged by PACS governance to ensure appropriate and effective messages are delivered at the right time.

Lesson Learned

Some of the simplest communication tools can also be the most effective. For example, posting signs at entry points displaying important information regarding the modernization can help individuals prepare for upcoming changes. One agency learned that employees planned to arrive early on the first day PIV cards would be used at the entrance of the building because they had read the signs and were expecting delays.

10.1.1.1. Existing Policy and Requirements

The first priority of physical security is life safety, protecting the people who occupy federal buildings. In support of this paramount responsibility, there are standards, codes, and policies that individuals in the physical security field are required to follow. The PACS is one of many parts of the overarching physical security mission. Implementers must address additional standards and guidance, such as the following:

- Interagency Security Committee (ISC)[208] Compendium of Standards. The ISC was created to enhance the quality and effectiveness of physical security in, and the protection of, federal facilities in the U.S. These authoritative standards are designed to help federal security professionals implement effective security policies. Of particular relevance:
  - Facility Security Level (FSL) Determinations for Federal Facilities. Defines the criteria and process to be used in determining the FSL of a federal facility, a categorization which then serves as the basis for implementing protective measures under other ISC standards.
  - Physical Security Criteria for Federal Facilities. Establishes a baseline set of physical security criteria that provide a framework for the customization of security measures to address unique risks at a facility.
  - Interim Design-Basis Threat Report. A stand-alone threat analysis to be used in conjunction with the physical security criteria. It establishes a profile of the type, composition, and capabilities of adversaries.
- National Fire Protection Agency (NFPA) codes.[209] The NFPA is the authority on fire, electrical, and building safety and its mission is to reduce the burden of fire and other hazards on the quality of life by providing and advocating consensus codes and standards, research, training, and education. NFPA develops, publishes, and disseminates consensus codes and standards intended to minimize the possibility and effects of fire and other risks. Of specific note:
  - NFPA 101. The Code addresses those construction, protection, and occupancy features necessary to minimize danger to life from the effects of fire, including smoke, heat, and toxic gases created during a fire.
  - NFPA 72. Covers the application, installation, location, performance, inspection, testing, and maintenance of fire alarm systems, supervising station alarm systems,

[208] A description of the ISC and its ICAM authority can be found in Section 2.3.1.

[209] National Fire Protection Agency (NFPA)

public emergency alarm reporting systems, fire warning equipment and emergency communications systems, and their components.

- Underwriters Laboratories (UL). An independent product safety certification organization that tests products and writes standards for safety in an effort to promote safe living and working environments, support the production and use of products which are physically and environmentally safe and to prevent or reduce loss of life and property. UL is the trusted resource across the physical security industry for product safety certification and compliance. Standards of particular relevance:
  - UL 294. Specifies requirements for the construction, performance, and operation of systems intended to regulate or control entry into an area or access to or the use of a device(s) by electrical, electronic or mechanical means. These requirements apply to computer equipment that, when used in conjunction with the main control, is necessary for proper operation of the access control system.
  - UL 1076. Specifies requirements for the construction, performance and operation of equipment intended for use in proprietary burglar alarm units and systems used to protect against burglary.
  - UL 2050. Specifies requirements for the monitoring, signal processing, investigation, servicing and operation of alarm systems.
- Federal Information Security Management Act (FISMA). This act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for IT systems. As covered under FISMA, PACS implementers must meet all requirements associated with the RMF as defined in SP 800-37[210] and implement the appropriate security controls outlined in SP 800-53.[211] They must also comply with FISMA reporting guidelines.[212]
- Open, Systems Integration and Performance Standards (OSIPS). A family of standards developed by the Security Industry Association (SIA), an American National Standards Institute (ANSI) accredited standards organization. These standards are intended to promote interoperability between components in traditional access control systems by providing a common interface and creating levels of performance. OSIPS references architecture information for all parts of an integrated electronic security system, including the PACS, and addresses how to use the standards within a compliant ICAM implementation. Of particular note:
  - OSIPS-ACR-200x. Describes identity authentication and factors that are presented in a transaction seeking access to an Accessible Component Collection.
  - OSIPS-APC-200x. Describes the credentials presented to field devices at the access point controller.

[210] SP 800-37

[211] SP 800-53

[212] M-10-15

- OSIPS-IDM-200x. Describes claims of identity that are authenticated by comparing reference authentication factors with presented credentials.

In addition to these existing standards and regulations, the next section introduces recommended agency governance efforts that may be used to support PACS modernization. It is important to note that the recommendations in this document are not intended to replace or supersede existing life safety or physical security standards and regulations.

10.1.1.2. Agency Governance Efforts

Policy is a key enabler of success during a PACS modernization. As part of implementation planning, PACS governance should review existing agency policies to determine if they align with the ICAM segment architecture, as well as relevant laws, government-wide policies, and standards. As appropriate, the planning should address any policy gaps that are identified with revisions to existing or the creation of new policies. This section is intended to supplement the guidance around program governance found in Chapter 6 and highlight specific areas that agency governance bodies should seek to address to enable successful PACS modernization efforts.

PACS-specific policies will vary based on an agency's size, mission and business requirements, as well as the maturity of its physical access policies relative to the ICAM target state. Per M-11-11,[213] agencies must develop and issue agency implementation policy requiring the use of the PIV credential for access to the agency's facilities, networks, and information systems and alignment with the ICAM segment architecture. There are also a number of other common topics that should be incorporated in an agency's governance efforts to support the modernized PACS implementation. Figure 98 includes a list of common governance efforts and describes how agencies might consider utilizing them as a means to promote compliance and overcome implementation challenges. Many of the governance efforts listed below are expected to apply to logical access, discussed in Chapter 11, and may be combined at some agencies.

[213] M-11-11

1

Governance Effort	Description
Issue Policy Memorandum: Continued Implementation of HSPD-12	• Agency-level policy, as required by M-11-11, that includes provisions for several items related to PACS modernization, including: • Enforcing use of the PIV card for physical access and the movement away from separate (often bureau/component-specific) ID cards. • Procurement of services and products for PACS in accordance with M-06-18[214] and the Federal Acquisition Regulation (FAR).[215] • Acceptance of PIV credentials issued by other federal agencies for physical access. • Alignment with the ICAM segment architecture, including completion of an agency transition plan that includes information regarding the agency's PACS modernization.
Issue Policy/Guidance Addressing Common Physical Access Scenarios	• Policy or procedural guidance reflecting formal agency-level decisions for handling common physical access problem scenarios such as a lost/forgotten PIV card.
Issue Policy/Guidance Addressing Standardization of Local Facility Access Cards	• Policy or procedural guidance for establishing a standard local facility access card and providing guidance around when and how they are issued. This topic is discussed further in Section 10.4.
Issue Policy/Guidance Addressing Visitor Management	• Procedural guidance for establishing what types of credentials are considered acceptable for granting physical access to visitors. Direction should address additional procedures for handling individuals who are not PIV card holders (e.g., escort procedures). This topic is discussed further in Section 10.5.
Define Baseline User Privileges for Physical Access	• Effort to determine a set of baseline user privileges for physical access that can be linked into the agency's automated provisioning capability to grant new users privileges to multiple access points automatically.

[214] M-06-18

[215] FAR Subpart 4.13

Governance Effort	Description
Bureaus/Component Modernization Plans	• Effort by agency leadership and management to review and provide guidance related to bureau/subcomponent implementation plans for modernizing PACS. The review should take into consideration whether the proposed approach meets relevant requirements and is the most cost effective (e.g., upgrading an existing PACS rather than purchasing a new system).
Incorporate the PIV Card Implementation Maturity Model (PIMM)	• Effort to incorporate the PIMM into PACS project performance measurement. The PIMM describes various levels of PIV card use to help agency leadership and PACS implementers determine the maturity of the PACS program and make decisions accordingly.

Figure 98: Sample PACS Governance Efforts

An important aspect of governance is the ability to measure project performance and maturity; however, measuring the progress of a modernized PACS implementation can be complex due to variations in the requirements, facility size, and amount of existing electronic PACS. SP 800-116 presents the PIV card Implementation Maturity Model (PIMM),[216] which should be used by agencies to measure progress while working towards achieving the target state. The levels are progressive and range from, "Ad Hoc PIV card Verification," to "Access to Exclusion, Limited, or Controlled Areas by PIV card or Exception Only." The lowest level describes a site that has the ability to authenticate PIV cards by performing required authentication mechanisms on an ad hoc basis. The most mature level describes a site in which only the PIV card is an acceptable credential for federal employees and contractors covered under HSPD-12. The PIMM can be integrated into agency's ICAM performance management reviews to determine the success of the modernized PACS implementation effort and set completion goals.

10.1.2. Facility Risk Assessments

Government facilities are a part of the nation's critical infrastructure, and as such, have certain protection requirements. The following mandates and requirements underscore an agency's responsibility for protecting federal facilities:

- HSPD-7 Critical Infrastructure Protection Mandates. Establishes a national policy for federal departments and agencies to identify and prioritize U.S. critical infrastructure and key resources and to protect them from terrorist attack. HSPD-7 identifies 17 sectors that require protective actions to prepare for, protect, or militate against a terrorist attack or other hazards.
- National Infrastructure Protection Plan (NIPP). Outlines the parameters for infrastructure protection. The use of the NIPP risk management framework is a part of the overall effort to ensure the protection and resiliency of our Nation's Critical Infrastructure/Key Resources. The NIPP includes the Government Facilities Sector Plan, which provides an approach to enhancing protection of government facilities.

[216] SP 800-116

Facilities and access points should be protected based on risk. The ISC Compendium of Standards, discussed in Section 10.1.1.1, provides agencies with guidance on how to perform facility risk assessments, define the appropriate FSL, and analyze the required level of protection to determine and implement the appropriate security countermeasures. As described in M-11-11,[217] the Department of Homeland Security (DHS) has also partnered with the GSA Public Building Service (PBS) to ensure that risk assessments and implementation of physical access measures for buildings under PBS' purview are executed in accordance with the ISC and NIST guidelines. There are a variety of risk assessment processes available for agency use. Figure 99 provides a summary of the main steps that are commonly conducted as part of a facility risk assessment, as defined in the ISC guidance and based upon industry best practices.

Process Integration Step	Description	Key Considerations
Step 1: Set Security Goals	Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture or baseline.	• Agency's security control posture and risk tolerance. • Security requirements, including FICAM security targets for PACS.
Step 2: Identify	Develop an inventory of the assets, systems, and access points that exist within a facility.	• Range of systems and assets within a given facility. • Calculated value of assets within a given facility.
Step 3: Assess	Determine risk by identifying potential consequences of vulnerabilities.	• Likelihood of occurrence. • Impact if vulnerabilities are exploited. • Local conditions and the area surrounding a facility.
Step 4: Analyze	Categorize and analyze risk assessment results to develop a comprehensive picture of facility risk.	• Relevant legislation, policies, and standards. • Protection priorities and adequate countermeasures.

Figure 99: Common Risk Management Steps

The end result of the risk assessment is a complete risk profile of the facility. This information helps physical security implementers make decisions regarding appropriate security countermeasures to employ, including electronic (e.g., video surveillance, intrusion detection, PACS, etc.), physical (e.g., bollards, gates), and guard force. The scope of this guidance is limited to authentication-based access control and thus focuses on the electronic PACS as a

[217] M-11-11

countermeasure;[218] however, agencies can find additional guidance on selecting a full range of alternative countermeasures in the ISC's Compendium of Standards.[219]

When applying the results of the facility risk assessment to the design of its PACS, an agency needs to determine the risk level of a particular facility and individual areas within the facility that will be protected by a controlled access point. The agency should then determine the appropriate authentication mechanism(s) that should be deployed at each access point, as defined in SP 800-116. SP 800-116 uses the restricted area concept of "Controlled, Limited, Exclusion" areas to address individual areas nested within a facility that may have specific security requirements. They are defined as follows:

- Exclusion Area. An Exclusion area is a restricted area containing a security interest or other matter of such nature that access to the area, or proximity resulting from access to the area, constitutes access to the security interest or matter.
- Limited Area. A Limited area is a restricted area containing a security interest or other matter of such nature that uncontrolled movement will permit access to the security interest or matter. Access in Limited areas may be controlled by requiring escorts or by other internal restrictions and controls.
- Controlled Area. A Controlled area is that portion of a restricted area usually near or surrounding an Exclusion or Limited area. Entry to the controlled area is restricted to authorized personnel.

Lesson Learned

It can be difficult to analyze a site for its risks and know how to apply the appropriate guidance while keeping cost savings in mind. An agency might find value in assembling a small team of cross functional resources (including physical security, IT, etc.) from its ICAM program to help bureaus/components or individual sites conduct facility risk assessments and make decisions regarding the best way to achieve a compliant, modernized PACS.	

Once an agency has determined the appropriate authentication mechanisms based on a facility's risk, it should make decisions around the best PACS solution and how to fund its implementation. The following section provides additional considerations and guidance on these topics.

Implementation Tip

Focus on what you can control. Agencies frequently occupy leased space where the landlord controls the exterior physical security. If the existing system cannot process the PIV card for physical access, establish an access point at the entry to the agency- controlled space. This arrangement allows the agency to meet its requirements for PIV card authentication while still adhering to the leasing agreement.	

[218] For more information on the security controls that can be implemented by a PACS, see Federated Physical Access Control System (PACS) Guidance, Federal CIO Council.

[219] Government users with a need to know may access the ISC standards that are For Official Use Only (FOUO) by requesting access at ISC@DHS.gov.

10.1.3. Program Funding

A key aspect of physical access implementation planning is making decisions around the funding and acquisition of a modernized PACS solution. This includes estimating solution costs, determining the proper funding method, and planning for and completing acquisition of the required products and services. This section discusses key considerations for estimating program funding needs and potential funding models for an agency's PACS modernization. Additional information on acquisition planning and the budget request process can be found in Section 6.1.3.3.

ROI	
One large agency was able to save tens of thousands of dollars per site on costs associated with server hosting, hardware and software, and executing IT security requirements when their individual PACS were rolled into the enterprise service offering.	

Selecting an appropriate PACS modernization approach and corresponding technology solution is one of the first steps in determining how a PACS program will be funded. Agencies should chose a solution that aligns with the ICAM segment architecture, supports their access control processes and requirements, leverages existing infrastructure wherever possible, and provides the best value for their investment. Once a solution has been determined, an agency should evaluate a number of factors in order to estimate the costs that will be incurred. The items provided in Figure 100 are examples of common factors and considerations that agencies should examine not only to determine costs, but also determine the potential cost savings that various PACS solutions are capable of providing.

Evaluation Factor	Description
Facility Size	The number of users requiring access to a facility significantly impacts the level of administrative effort required to provision user accounts and manage access privileges. In addition, there may be potential cost breaks for certain volumes.
Level of PACS Services Provided	Agencies should determine at which level PACS services should be provided. There are cost savings and efficiencies that can be achieved by providing services at the enterprise-level. For example, an agency hosting a server for the bureaus/components.
Analysis of Population	Organizations should examine populations (employees, contractors, short term, etc.) and facility tenants (federal, non-federal) to determine the types of groups requiring access. Complex user populations should be considered when making a decision on the type of PACS solution to implement. In addition, there should be capability to handle increased capacity as the modernization progresses and the amount/type of users change over time.

Evaluation Factor	Description
Number of PACS	The number of PACS within an agency often dictates implementation time and can significantly affect implementation cost, depending on the resources' connection requirements.
Type of PACS	The type of PACS varies based on the vendors, platforms, operating systems, products, databases, etc. that are in use across the organization. These variances impact the complexity of integrating resources with the PACS infrastructure and require different integration processes.
Existing PACS Investments	Agencies may have existing investments in place that are capable of providing physical access services in a manner consistent with the target state ICAM segment architecture. These investments should be leveraged wherever possible and offer the potential to achieve a modernized PACS state without requiring significant investment from the organization.
Credentials Supported	Agencies should examine the types of credentials that the PACS must support (including PIV-I) and incorporate any costs associated with validating acceptable credentials.
Protection Areas[220] 220	Agencies should consider the number or combination of protection areas (Limited, Exclusion, Controlled) when determining program costs. For example, a high number of exclusion protection areas may increase costs due to the added level of access control required to protect those areas.

Figure 100: Common PACS Acquisition Considerations

Once a solution has been identified and the potential costs and cost savings have been estimated, agencies should make decisions around how to fund the PACS solution. Typically, PACS have been selected and funded at the site level. As agencies look to move towards an enterprise model, this can introduce challenges for funding and implementing enterprise PACS services, where equipment and services will likely be purchased centrally. To date, agencies have taken several different approaches to funding their PACS modernization efforts. These include:

- Incorporate Costs into Existing Investment. Rather than having a separate PACS investment, costs for PACS modernization can be included in an existing business case.
- Investment Business Case. A new investment request to fund PACS modernization at the enterprise level. The business case includes details of how the proposed investment would support the agency's mission.
- Working Capital Fund. A fund that is able to provide financing to agencies without annual appropriation by Congress for operations that generate receipts. This funding method works well for an agency that is providing the enterprise PACS as a centralized service and has a fee structure for the users across the bureaus/components.

[220] More detailed information can be found in Section 10.1.1.2.

Implementation Tip

The products implementing and executing the cryptographic processes with the PIV card must comply with FIPS 140 and be approved by NIST validated laboratory. Agencies should procure products and services from manufacturers who provide architectures that minimize the cost of FIPS 140 by producing components in very high volume, or by amortizing the cost into common components, such as a multi-door controller.

In addition to determining funding needs and obtaining funding, a key aspect of PACS implementation planning is outlining the life cycle activities associated with the modernization effort and determining the project schedule. This is addressed further in the following section.

10.1.4. Schedule Planning

Modernizing PACS projects requires close coordination across multiple workstreams within an agency and may, in some cases, represent a multi-year effort. During this period, it is critical to develop a transition plan that keeps the current PACS and physical security infrastructure in place while reducing security system downtime. Because of this complexity, program/project managers should consider following a system development life cycle (SDLC) that addresses key activities and timing considerations. There are a variety of SDLCs that are commonly accepted and used within the Federal Government. Each agency should have a defined and repeatable SDLC that meets the agency's business needs and supports IT investments; these same concepts can be applied to physical security investments. While individual agency SDLCs may be more granular in detail and contain additional steps/phases, the activities and considerations presented in this section can be adapted into any SDLC model.

Implementation Tip

An important aspect of developing a phased implementation approach is accurately documenting the activities that must occur during each phase and defining measurable exit criteria. This ensures that the implementation proceeds along a predictable path, which can help mitigate many common implementation risks.

The guidance presented in this document has been organized into a traditional, sequential five-phase SDLC (waterfall) process, as it is the simplest and most commonly used model. The phases discussed have been abstracted from a variety of individual agency SDLC models to suit the needs of this document and create an appropriate basis for discussion. The five phases are: Planning, Requirements and Design, Build, Implement, and Operate and Maintain. This section examines each of the SDLC phases in greater detail and discusses the PACS-specific events that should occur as part of each phase.

Implementation Tip

One large agency created a working group to gather information around its deployed PACS infrastructure, such as vendor product, version and architecture. Collecting this data can help agency leadership determine how to leverage existing investments when planning and designing its target state PACS solution.

10.1.4.1. Planning Phase

Section 10.1 of this chapter discusses the overall planning considerations when implementing a modernized PACS. This section describes planning as the first phase of the structured SDLC process commonly used when executing complex solutions. Completing the Planning Phase is critical for modernizing PACS solutions, as many of the common problems encountered can be avoided through careful planning.

Lesson Learned

Investing in and installing multi-technology PIV card readers gives program implementers' access control during the transition from agency-specific proximity cards to PIV cards. It also allows proximity cards to be issued to resolve temporary physical access challenges such as lost, stolen, or damaged PIV

Figure 101 provides a list of common activities that should occur during the Planning Phase and notes estimated completion times for each; however, activities may occur in parallel, and actual times can vary widely based on organizational size and project complexity.

Activity	Description	Completion
Develop Communications Plan	Develop the approach and plan to communicate (using a variety of mediums) the changes that a PACS modernization effort will bring to internal users, resource owners, and stakeholders. It should include some form of agency cultural education plan if changes will be significant.	2 – 4 weeks
Conduct Gap Analysis	Determine the desired operation and use cases for the target state system and then compare against capabilities of the current equipment. This should be followed by an objective assessment of capabilities of the current PACS to determine what solution is required to achieve the desired target state.	2 – 4 weeks
Conduct Cost/Benefit Analysis	Evaluate organizational factors and conduct a cost/benefit analysis to determine an appropriate PACS solution.	3 – 6 weeks
Develop PACS Modernization Business Plan	Develop a business plan to support modernization of the existing PACS infrastructure or a new infrastructure. This should lay out the selected approach, timeline, resource requirements, and estimated costs.	4 – 6 weeks

Activity	Description	Completion
Develop Implementation Plan/Schedule	Develop a phased implementation approach and schedule based on available information using standardized agency resources.	2 – 4 weeks
Categorize the PACS	Conduct Step 1 of the Risk Management Framework (RMF):[221] Categorize Information Systems based on mission/business objectives. Register the PACS in the IT system inventory.	4 – 12 weeks
Develop Risk Management Plan	Utilize existing risk management sources to develop a Risk Management Plan, as discussed in Chapter 6, for handling risks related to modernizing the PACS infrastructure.	2 – 4 weeks
Begin Field Prioritization	Begin examining agency PACS and developing field assessment criteria in order to prioritize/organize deployment of modernized PACS services to agency facilities.	1 – 2 weeks
Develop Field Integration Guide	Develop a Field Integration Guide, a formal document used to outline the process that an agency's physical security resources will go through to become integrated with the PACS solution.	6 – 8 weeks
Develop PACS Migration Plan	Develop a migration plan that outlines how the agency plans to transition its physical resources to use the modernized access control system.	1 – 3 weeks
Develop Pilot Implementation Plan	Develop a plan and schedule for piloting the modernized PACS solution on a small subset of the user population with well- defined resource requirements.	4 – 12 weeks

Figure 101: Planning Phase Sample Activities

10.1.4.2. Requirements and Design Phase

The Requirements and Design Phase follows the Planning Phase in the SDLC. In this phase, an agency thoroughly documents the requirements for the PACS solution and defines how the solution should operate within the existing infrastructure. Figure 102 provides a list of common activities that should occur during the Requirements and Design Phase and notes estimated completion times for each; however, activities may occur in parallel, and actual times can vary widely based on organizational size and project complexity.

[221] A more detailed discussion of the Risk Management Framework can be found in Section 6.2.4.1.

Activity	Description	Completion
Gather PACS Solution Requirements	Conduct a requirements gathering exercise with stakeholders and impacted parties at all organizational levels to document requirements of the PACS solution. These requirements are critical as they will be used to drive the design, build, and configuration of the PACS capability.	4 – 6 weeks
Validate PACS Solution Requirements	Validate the documented requirements with the appropriate stakeholders in order to ensure that the PACS solution is properly designed and configured to meet the agency's needs.	1 – 2 weeks
Secure Funding Sources	Utilize the PACS business plan to secure funding sources for the modernization effort. This should include determining if existing investments exist and how to leverage them.	6 – 10 weeks
Select Security Controls	Conduct Step 2 of the Risk Management Framework (RMF): Select Security Controls by choosing the appropriate security controls and documenting the selected controls in the security plan.[222]	2 – 4 weeks
Document System Design	Draft an initial system design document that clearly states how the system should function within the agency's environment. The design document and associated requirements are then used during the build phase as a reference for how the PACS system should operate.	2 – 4 weeks
Define and Configure Provisioning Workflows	Define provisioning workflows, which are used to determine how users are granted rights to access points and what approvals or additional steps are required. This process often involves configuring automated workflows based on existing manual processes.	2 – 4 weeks
Develop Solution Architecture	Develop an initial solution architecture for the PACS implementation. This architecture defines the solution components and describes their interactions.	2 – 4 weeks
Conduct Resource Acquisition	With funding sources secured, conduct the process of purchasing any required hardware or software and services.	4 – 12 weeks

Figure 102: Requirements and Design Phase Sample Activities

[222] For more information on the security controls that can be implemented by a PACS, see Federated Physical Access Control System (PACS) Guidance, Federal CIO Council.

Implementation Tip

Be sure to include ICAM requirements for modernized PACS in facility arrangements, negotiations, and the procurement process for leased space. When these requirements are introduced during the Requirements and Design Phase, an agency can more easily ensure the proper requirements are incorporated into lease agreements.	

10.1.4.3. Build Phase

Following the Design Phase, agencies enter the Build Phase, where the majority of the technical solution development, configuration, and testing occurs. Figure 103 provides a list of common activities that should occur during the Build Phase and notes estimated completion times for each; however, activities may occur in parallel, and actual times can vary widely based on organizational size and project complexity.

Activity	Description	Completion
Stand Up Development and Test Environments	Establish development and testing environments so that PACS developers and testers can conduct build activities in an environment that does not impact the agency's production systems.	4 – 6 weeks
Build/Configure Servers	Build and/or configure servers to properly operate the PACS solution, as needed based upon the chosen implementation path.	1 – 2 weeks
Install Supporting Software	Install supporting software (i.e., Commercial Off-The-Shelf [COTS] Identity Access Management [IAM] Suite) on PACS servers, as needed based upon the chosen implementation path.	1 – 2 weeks
Configure Supporting Software	Configure PACS software to specifically meet the agency's unique needs and/or perform certain functions, as needed based upon the chosen implementation path.	1 – 2 weeks
Implement and Assess Security Controls	Conduct Steps 3 and 4 of the Risk Management Framework (RMF) by applying the controls identified in the requirements and design phase and by assessing the adequacy and effectiveness of the security controls and documenting the findings in an assessment report.	12 – 20 weeks
Conduct Testing on Initial Build	Perform testing on the PACS solution in a development and/or test environment to ensure that system errors are found and corrected before the solution is deployed on the agency's network.	2 – 4 weeks
Conduct Pilot Implementation Deployment	Conduct a pilot implementation to expose a small subset of the agency's user base to the PACS solution for the purpose of evaluating the solution's operations against real-world requirements.	Varies on size of deployment (number of facilities and

Figure 103: Build Phase Sample Activities

10.1.4.4. Implement Phase

Once an agency has configured its PACS solution and tested to ensure that it meets agency and government-wide requirements and performs appropriately, the program enters the Implementation Phase. This phase consists of activities for migration of the PACS solution from a development and test environment into the agency's production infrastructure. There may be an overlap in access control services provided by the old and new PACS for a period of time until the cardholder population is fully transitioned to the new PACS. Figure 104 provides a list of common activities that should occur during the Implement Phase and notes estimated completion times for each; however, activities may occur in parallel, and actual times can vary widely based on organizational size and project complexity.

Activity	Description	Completion
Authorize the PACS	Conduct Step 5 of the Risk Management Framework (RMF):[223] Authorize Information System by preparing and submitting the security authorization package to the authorizing official. The authorizing official chooses to accept the risk and authorize the system if the risk associated with operating the PACS is deemed acceptable.	1 – 2 weeks
Conduct User Acceptance Testing	Conduct user acceptance testing to ensure that the PACS solution is acceptable to stakeholders and end users and performs the required functions in an appropriate manner.	2 – 4 weeks
Conduct User Training	Develop training materials and conduct user training prior to PACS deployment to ensure that users are capable of accessing their worksites without disruption.	2 – 4 weeks
Deploy PACS Solution to Live Production Environment	Deploy the PACS solution on the agency's network infrastructure and begin controlling access to facilities.	Varies according to deployment size (number of facilities and access points)
Perform Awareness and Outreach	Conduct awareness and outreach activities in accordance with the Communications Plan developed as part of the Planning Phase. This involves actively communicating to users that a new access control system is being deployed, the benefits and efficiencies that users can expect, and any steps necessary to begin using the new system.	This will occur as needed throughout the deployment process

Figure 104: Implement Phase Sample Activities

[223] A detailed discussion of the RMF can be found in Section 6.2.4.1.

10.1.4.5. Operate and Maintain Phase

After an agency has successfully deployed its modernized PACS solution to a live production level, the program enters the Operate and Maintain Phase. This phase lasts for the remainder of the time that the PACS solution is in use and consists of ongoing management and system maintenance activities such as: conducting training, operating the PACS solution, and protecting new resources as they come online.

Implementation Tip

Enterprise development often includes connection of multiple local PACS servers that may contain local user records. This process may involve removal of redundant accounts in instances where one person has access to multiple sites. Additionally, agencies should have a plan for handling duplicate user records.	

Figure 105 provides a list of common activities that should occur during the Operate and Maintain Phase and notes estimated completion times for each; however, activities may occur in parallel, and actual times can vary widely based on organizational size and project complexity.

Activity	Description	Completion
Monitor Security Controls	Conduct Step 6 of the Risk Management Framework (RMF): Monitor Security Controls by monitoring changes to the information system and its environment of operation and conducting ongoing assessments of security controls in accordance with the monitoring strategy.	On-going
Ongoing User Training	Continue to update and modify user training curriculums as the PACS solution matures and new technology is implemented. Conduct additional training as necessary.	This will occur as needed throughout the deployment
Modify Provisioning Workflows	Update provisioning workflows as business needs and access rules change over time. Changes may also be required as resource owners experience the benefits that can be provided by modernized PACS services and provisioning workflows can be streamlined.	2 – 4 weeks per occurrence
Conduct Hardware/ Technology Refresh	Conduct periodic updates and/or upgrades to solution hardware and other technology over the lifespan of a PACS solution as a means of extending the usable life of the solution or adding new capabilities.	12 – 36 weeks
Software/Firmware Refresh	Update software and firmware to accommodate manufacturer improvements, bug fixes, or to remain compliant with the latest policies and standards.	15 minutes per device (reader or controller)

Figure 105: Operate and Maintain Phase Sample Activities

This page left intentionally blank.

Appendix B: Life Cycle Management Tailoring Agreement Checklist

LIFE CYCLE MANAGEMENT TAILORING AGREEMENT CHECKLIST		
Project Name/Acronym:	**Date:**	
Unit Mission/Business Sponsor:	**Unit**:	
Project Investment Tracking No.: [OMB 300 UPI Code, Grant ID, Unit Funds, etc.]		
Project Contact Information: [Name, Email, Phone, Role]		
System Purpose:		
Project Scope:		
Project Questions	**Yes**	**No**
1. Number of existing/planned internal interfaces? _____ External Interfaces? _____ 1a. If applicable, do you have approval to interface with these systems?	[ ]	[ ]
2. Is the System/Application being targeted to be supported internally in the Agency's Data Center and/or on the IT Infrastructure?	[ ]	[ ]
3. Will the System be hosted outside of the Agency's Data Center? 3a. If Yes, where? _____	[ ]	[ ]
4. Is the System or application being associated with an existing Agency Certification and Accreditation package? 4a. If yes, which package? _____	[ ]	[ ]
5. Will Agency Users be required to log-in and authenticate? 5a. If yes, will the system use Active Directory?	[ ] [ ]	[ ] [ ]
6. Will the system require 24x7 availability?	[ ]	[ ]
7. Will the system be mission or business critical? 7a. If Yes, will a Disaster Recovery Site/Alternative processing site be required?	[ ] [ ]	[ ] [ ]

8. Will the system process and/or store sensitive Agency information or Personally Identifiable Information (PII)? PII refers to information about individuals maintained by the Agency, including information which can be used to distinguish or trace an individual's identity and any other information that is linked or linkable to an individual, such as medical, educational, financial, or employment information. Examples include, but are not limited to: • General Personal Data: full name, maiden name, full date of birth; • Address Information: street address or email address; and • Personal Identification Number: Social Security Number, passport.	[ ]	[ ]
9. Will there be an acquisition of new hardware and/or COTS software?	[ ]	[ ]
10. Will the system support public or collaborator usage from the internet?	[ ]	[ ]
11. Will Public Users be required to log-in and authenticate to the System? If yes, what is the estimated number of external users? _____	[ ]	[ ]
12. When do you expect the system to be available for production use? _____	[ ]	[ ]

Type of Project: (Check all that apply)

[ ] New COTS HW/SW Implementation
[ ] Existing COTS HW/SW Upgrade/Enhancement
[ ] Common Enterprise Application Development
[ ] Custom Unit Portfolio Application Development
[ ] Public Website Development
[ ] New IT Infrastructure requirement

Deliverables, Reviews & Events	**Required Yes**	**No**	**Update Only**	**Comments** (e.g. when updates are required)
Initiation Phase				
Informational Brief				
Project Management Plan				
Security Requirement Workbook to include: • System Categorization • E-Authentication questionnaire • Privacy Threshold Analysis				
System Categorization / Data Types (NIST SP 800-60)				
FEMA Mapping				

1

1

Deliverables, Reviews & Events	Required Yes	Required No	Update Only	Comments (e.g. when updates are required)
Requirements Definition Phase				
Requirements Review Brief				
Requirements Statement				
Configuration Management (CM) Plan				
Detailed Analysis and Design Phase				
System Design Review Brief				
Requirements Specification				
Product Evaluation				
Concept of Operations				
Preliminary Risk Assessment (RA)				
Detailed Design Document				
Privacy Impact Analysis				
Detailed Analysis and Design Phase				
System Security Plan (SSP)				
Training Plain				
Test Plan				
System Test & Evaluation (ST&E) Plan for Security				
Development and Testing				
Production Readiness Review				
Contingency/Disaster Recovery Plan				
Test Results Summary				
Data Conversion Plan				
Operational Support Plan				

2

1

Deliverables, Reviews & Events	Required Yes	Required No	Update Only	Comments (e.g. when updates are required)
ST&E Result – Security Assessment Report (SAR)				
Contingency Plan/Disaster Recovery Results				
Risk Assessment – Final with Vulnerability Scan Results				
IT Security Plans of Actions and Milestones (POA&M)				
Deployment				
Certification and Accreditation Package - SSP Final				
Production Authority to Operate (ATO)				
Operations				
Post Implementation				

Signatures Required:

UNIT IT Manager: _____ Date: _____

PROJECT Manager: _____ Date: _____

Director, IT Computer Security: _____ Date: _____

2

3