Security Control Overlay of Special Publication 800-53 Revision 5

Security Controls for electronic Physical Access Control Systems (ePACS)

Version 1.0

December 24, 2020

Produced by:
PACS Modernization Working Group (PACSmod WG)

Working group chartered by the co-chairs of the:

Federal Chief Information Security Officer (CISO) Council,
Identity, Credentialing and Access Management Cubcommittee (ICAMSC)

and the

Program Director of the Department of Homeland Seucrity (DHS),
Interagency Security Committee (ISC)

Revision History

Document Version	Document Date	Revision Details
1.0	12/24/2020	Initial Publication

Table of Contents

1. INTRODUCTION

Information Technology (IT) continues to expand throughout every aspect of modern life, integrating domains that were previously thought to be unrelated. These advances have resulted in a relatively new categorization of systems termed “Cyber-Physical Systems” (CPS, [SP 1500-201]). CPSs include interacting networks of both physical and computational components.

One example of these CPSs are electronic Physical Access Control Systems (ePACS). These ePACS use a combination of IT components and physical security elements (e.g., card readers, doors/locks) to enable access to real-world resources such as secured facilities or controlled areas within facilities.

Access control systems (both Logical and Physical), leveraging authentication and authorization mechanisms, are critical aspects of security regimens. These access models require formalized system requirements, interoperability standards, audit frameworks and governance activities. This level of formality was officially applied to Logical Access Control Systems (LACS) in the Federal enterprise with the introduction of the Federal Information Security Management Act (FISMA) in 2002.

ePACS are similar to LACS in this regard; made even more concrete with the formal categorization of ePACS as IT systems initially stated in [M-10-15], requiring their reporting in support of FISMA metrics. Despite LACS having a formalized risk acceptance process through the Risk Management Framework (RMF) and FISMA, the same has yet to be done for ePACS. The National Institute for Science and Technology (NIST) has established additional guidelines related to the use of Personal Identity Verification (PIV) to facilitate physical access [SP 800-116]; however, there is no formalized ePACS operational assessment standard or methodology. As a result of this gap, non-compliant ePACS are still being procured, and Approved Product List (APL) certified ePACS are being misconfigured widely across the Federal enterprise as has been documented in the Government Accountability Office report *Federal Building Security, Actions needed to Help Achieve Vision for Security Interoperable Physical Access Control* [GAO-19-138]. In aggregate, piecemeal ePACS implementation practices represent an unmitigated risk to Federal facilities, information, and personnel.

This overlay will provide a standardized template for Chief Security Officers (CSOs) and other ePACS professionals working to secure Federal facilities in a secure and interoperable fashion. Additionally, it should help to inform those FISMA Authorizing Officials (AOs) asked to evaluate the cyber specific risks posed to the IT infrastructure comprising its ePACS. In short, this overlay will allow ePACS to benefit from FISMA in a similar fashion to its LACS counterparts.

1.1. PURPOSE & SCOPE

This document fulfills the following tasking established in [M-19-17]:

- "Develop and publish, in consultation with GSA, OPM, OMB, and DOC a Physical Access Control System (PACS) security and privacy control overlay to help agencies identify core controls for PACS."

Practically, the purpose of this document is to assist those entities responsible for physical and cyber security:

1. Provide minimum applicable IT security controls and related supplemental guidance to appropriately secure and administer ePACS
2. Establish a relationship between IT system security controls and ePACS operational configurations using a standardized risk-based approach
3. Develop an initial foundation for an ePACS operational assessment by providing supplemental guidance for the implementation of authentication mechanisms in ePACS as defined in NIST [SP 800-116]
4. Define initial responsibilities for implementation and use of this overlay

The controls, enhancements and supplemental guidance established in this document apply to the procurement, administration and operation of **ePACS** only. It does not address other aspects of building or facility security as defined by the Interagency Security Committee (ISC) such as force protection measures documented in [Countermeasures].

1.2. INTENDED AUDIENCE

The intended audience for this document is:

1. CSOs, Physical Security Specialists, Physical Security Managers, Authority Having Jurisdictions (AHJs), and similar roles with responsibilities for using electronic access control to secure Federal facilities
    - Responsible for ensuring supplemental operational guidance in this overlay are planned and implemented
2. Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), or other appointed AOs responsible for Authorizing and Accrediting ePACS within their portfolios
    - Confirm administrative controls in this overlay are implemented on ePACS and confirm operational controls are implemented as attested by CSOs or Assessors, additionally accepts any residual risk and authorizes the system
3. Assessors, Auditors (to include 3rd party evaluators)
    - Responsible for validating controls and enhancements are implemented as stated
4. ePACS integrators, system designers, and installers
    - Responsible for initial system configuration and control implementation

2. ALIGNMENT OF RISK-BASED FRAMEWORKS

In order to appropriately protect government resources from threats, owners implement risk-based approaches in the selection of security controls for a given information system or countermeasures for a facility. Risk-based approaches assist in prioritizing threats and implementing appropriate mitigations. The following table compares the high-level steps in NIST Risk Management Frameworks (RMF) and ISC Risk Management Process (RMP) for federal facilities.

NIST RMF	ISC RMP
Categorizing an information system (FIPS 199)	Determine Facility Security Level (FSL)
Selecting security controls (FIPS 200)	Identify Mitigating Countermeasures
Implementing those security controls (800-53)	Apply Countermeasures
Assessing those security controls (800-53A)	Measure Performance
Authorizing the information system (800-37)	--
Monitoring the security controls (800-137)	--

Table 1 - Framework Comparison

Provided the nature of ePACS, risks and associated impacts can be estimated given two different measurement frameworks:

- Cyber Risks Categorization (NIST, [FIPS 199]) - estimates the impact to the United States, associated with the compromise of data within an information system, resulting in a High, Moderate or Low rating; three considerations associated with the rating include impacts to:
    - Data Confidentiality
    - Data Integrity
    - Data Availability

- Physical Risks Determination (ISC, [RMP]) - incorporates 5 categories that use a points system to quantify target value and impact estimates (in the event of an attack/disruption) to determine an overall FSL rating of I (lowest) to V (highest); considerations associated with the FSL determination are:
    - Facility Mission Criticality
    - Facility Symbolism
    - Facility Population
    - Facility Size
    - Threats to Tenant Agency

Though there are notable differences between the two frameworks, the ePACS classification as an IT system necessarily facilitates the need to produce a FISMA Authority to Operate (ATO). Figure 1 represents that the CSO (or similar role) has the responsibility for the contents of this overlay in support of overarching FISMA authorization processes.

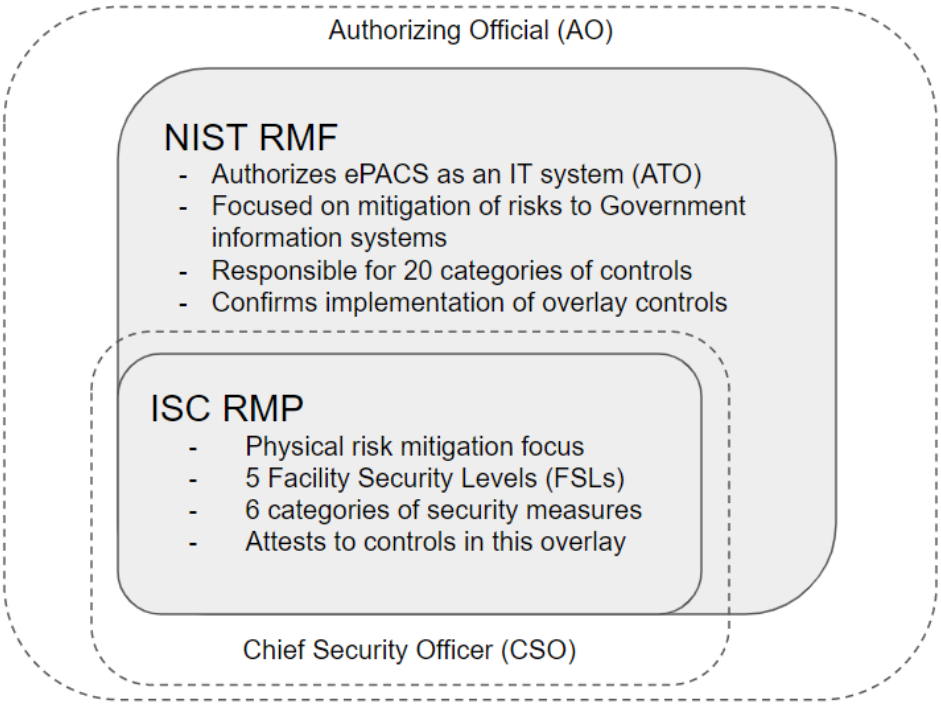

Figure 1 - Cyber - Physical Risk Relationship

The NIST and ISC risk ratings and their component factors have slightly different scope, but certain rough comparisons can be established. This overlap ensures that ePACS security and operations are enforced to prevent unauthorized or improper physical access to facilities, information and personnel.

Impacts ratings between the two risk frameworks can be modified by system or facility owners to properly reflect risk based on FSL factors. For instance, a given facility may only have an FSL-III rating, but if the mission criticality component of that area is rated higher, AOs may still want to adopt a [FIPS 199] High rating for the ePACS. This could be due to the sensitivity of the information stored in the facility or in the ePACS system or sub-systems, and its impact in the event of compromise.

To assist facility owners, [SP 800-116] provides additional recommendations on the implementation of authentication mechanisms in ePACS using PIV. These recommendations provide the following benefits:

- Leverages PIV to facilitate physical access interoperability between agencies
- Applies a 3-tiered risk model (Controlled, Limited, Exclusion) aligning additional authentication factors for higher risk areas
- Correlates general implementation guidance to areas of varying FSL ratings

For the context of Table 2, it is assumed that the area the ePACS is protecting is a uniform sensitivity; however, in reality, many buildings may have internal areas of varying sensitivity that require additional ePACS authentication mechanisms and/or components. For example, a given building may have an FSL-III rating, but may also contain a more secure area within. In this scenario, each of these protected areas should have ePACS components regulating access based on an authenticated identity; however, the FSL-III main building may only require one factor for its entry points, whereas another, more secure, internal area might require two factor authentication at its corresponding entry point(s). Additionally, Table 2 includes a NIST [SP 800-116] defined risk mapping which specifies the requirements for authentication assurance prior to an ePACS making an access determination to a physical resource.

Table 2 provides a generic equivalency between a [FIPS 199] rating applied to an ePACS and an overall FSL rating as it relates to example authentication assurance for individuals requesting access[1]. Due to the difference in risk frameworks, this table is informative and only meant for planning purposes.

FIPS 199		FSL (Example Area)		Authentication Assurance (NIST SP 800-116)
High	~	V	~	Very High Assurance (Exclusion)
Moderate	~	IV	~	High Assurance (Limited)
Low	~	III	~	Some Assurance (Controlled)
None	~	II	~	No Assurance (Public)
		I		

Table 2 - Risk Rating Comparison

Authentication requirements for administrative access to ePACS software should match the highest physical access authentication requirement covered by the ePACS. Similarly, cyber risk categorization for enterprise ePACS may increase due to the total exposure of high-risk data contained within its controlled facilities.

2.1. FISMA - PACS ACCREDITATION BOUNDARIES

For ePACS themselves, FISMA accreditation boundaries can be inclusive of any device or component that performs biometric template or image storage, crypto processing or Public Key

[1] For additional information on risk framework correlation and authentication factors see [SP 800-116] Section 4.3

Infrastructure (PKI) decision making. In the physical access world, this can be considered the software or the validation infrastructure supporting the ePACS. Though not all ePACS devices may fall directly within this overlay, if devices are TCP/IP connected they should have appropriate security around connections to components within the accreditation boundary.

2.2. RISKS TO PACS - EXPLOITATION MITIGATION

Many agencies rely on ePACS to maintain security of sensitive information, and other critical assets. Exploitation of improperly administered ePACS can lead to unauthorized and/or unaudited access to such information or other sensitive resources. These risks stress the need to ensure alignment of facility security and IT security plans.

The IT security plan should take into consideration authentication to the ePACS applications in support of software administration or configuration management. This access must not be of lower assurance/security than what is required to access a physical resource the ePACS protects. For instance, if an ePACS is used to manage access to a [SP 800-116] defined Limited area, it would require two factor authentications in support of physical access, thus ePACS privileged system administration would require no less than two authentication factors.

Facility security plans should similarly consider authentication mechanisms applied to physical access to spaces containing data centers and IT resources. Having a lower level of physical authentication to spaces housing critical IT resources could lead to breach of data or networks through physical access to such equipment.

3. How to Read This Overlay

This overlay addresses [SP 800-53] control applicability to ePACS and provides supplemental guidance to specific controls and enhancements. The aim is to assist AOs in reducing cyber related risk to the ePACS IT systems themselves, and also to provide CSOs, or similar roles, operational guidance that fulfills the intents of [SP 800-116] and [M-19-17]. Supplemental guidance is primarily aligned to the Identification and Authentication (IA) and Access Control (AC) control families as these are the primary constituent categories of the *Authentication* + *Authorization* = *Access* model; however, some operational guidance is aligned to other [SP 800-53] control families to ensure operational elements meet policy requirements.

An overarching set of reference tables is provided encompassing controls from each family to indicate those controls that are minimally applicable to ePACS, which includes relevant [SP 800-53B] LOW baselines. Applicability tables in Section 5 identify if supplemental guidance exists. AOs may determine that other controls that are not applicable in this overlay need to be addressed to support the NIST RMF.

A → Control Family		
Base Control	Relevant Guidance	Relevant Enhancements
B → AC-2	**C** → ✓*	**D** → 1, 2*, 3, 4*, 5

Table 3 - Control Applicability Reference

All base controls from [SP 800-53] are listed in this table; elements of the table are outline to include:

A → Lists the control family
B → Identifies the base control
C → Indicates if the control is applicable to an ePACS system with a checkmark; asterisks denote supplemental guidance on the base control
D → Lists the enhancements that are applicable to an ePACS system with a number; asterisks denote supplemental guidance on the enhancement

Each control or enhancement with supplemental guidance are contained within two tables given the following format. Table are outlined below.

V → Base Control
Applicable Control from [SP 800-53]
W → Base Control Description

Table 4 - Base Control Summary

Control Enhancements		
Applicable Enhancement	Administration	Operations
X → Enhancement Description	**Y** → Additional guidance on applying security controls aimed at mitigating ePACS cyber risks.	**Z** → Additional guidance on applying ePACS configurations to support physical access controls in alignment with [800-116].

Table 5 - Supplemental Guidance

V → Expresses the control Family, specific control number and title of each applicable base control (e.g., AC-2 Account Management)
W → Includes the applicable portions of the control description as stated in [SP 800-53] for reference
X → Defines any applicable enhancements in addition to the existing base control (e.g., AC-2(3) Disable Accounts)
Y → Provides supplemental guidance for the administration of the host system and IT infrastructure supporting ePACS software related to the enhancement (e.g., ePACS administrator accounts expire after X days of inactivity)[2]
Z → Provides supplemental guidance for the operations of an ePACS sub-system related to the enhancement (e.g., ePACS user accounts are disabled after X weeks of inactivity, or other specific controls related to reader or lock configurations)

[2] Examples of supplemental guidance in this section are illustrative only.

4. CONTROL FAMILIES NAVIGATION

The following table lists all control families from [SP 800-53]; however, hyperlinks are provided to those families that have supplemental guidance in this overlay.

ID	Family Name	ID	Family Name
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

5. APPLICABILITY SUMMARY

The following tables, organized by control family, include all applicable base controls and control enhancements that an ePACS with a FIPS 199 LOW baseline should consider. Controls and control enhancements that contain supplemental guidance are denoted with an asterisk (*).

Access Control		
Control	*Relevant Guidance*	*Relevant Enhancements*
AC-1	✓*	
AC-2	✓*	1*, 3*, 4, 5, 7
AC-3	✓*	3*, 7, 8*, 10*
AC-5	✓	
AC-6	✓	1, 2, 5, 7, 9, 10
AC-7	✓	3
AC-8	✓	
AC-9	✓	1
AC-12	✓	3
AC-14	✓	
AC-17	✓	1
AC-18	✓	
AC-19	✓	
AC-20	✓	
AC-22	✓	

Awareness and Training		
Control	*Relevant Guidance*	*Relevant Enhancements*
AT-1	✓	
AT-2	✓	1, 2, 3, 4, 5, 6
AT-3	✓	1, 2*, 3
AT-4	✓	

Audit and Accountability		
Control	*Relevant Guidance*	*Relevant Enhancements*

Audit and Accountability		
AU-1	✓*	
AU-2	✓*	
AU-3	✓*	
AU-4	✓	
AU-5	✓	1, 2
AU-6	✓*	3*, 6, 9
AU-7	✓	
AU-8	✓	1, 2
AU-9	✓	6
AU-10	✓	1
AU-11	✓	1
AU-12	✓	1, 2, 4

Assessment, Authorization, and Monitoring		
Control	*Relevant Guidance*	*Relevant Enhancements*
CA-1	✓	
CA-2	✓*	1, 2
CA-3	✓	
CA-5	✓	
CA-6	✓*	2
CA-7	✓	4
CA-9	✓	

Configuration Management		
Control	*Relevant Guidance*	*Relevant Enhancements*
CM-1	✓	
CM-2	✓*	3, 6, 7
CM-3	✓	2, 7, 8
CM-4	✓	1, 2

Configuration Management		
CM-5	✓	5*
CM-6	✓*	2
CM-7	✓	1
CM-8	✓	1, 6, 7, 9
CM-9	✓	
CM-10	✓	
CM-11	✓	

Contingency Planning		
Control	*Relevant Guidance*	*Relevant Enhancements*
CP-1	✓	
CP-2	✓	1, 2, 3, 5, 6, 7, 8
CP-3	✓	1
CP-4	✓*	1
CP-6	✓	1, 2, 3
CP-9	✓*	1, 2, 5, 6
CP-10	✓	2*,4*, 6

Identification and Authentication		
Control	*Relevant Guidance*	*Relevant Enhancements*
IA-1	✓	
IA-2	✓*	1, 2*, 8*, 10, 12*
IA-3	✓	3
IA-4	✓	
IA-5	✓	2*, 6*, 12*, 13, 14*, 15*
IA-6	✓	
IA-7	✓*	
IA-8	✓	1*, 2, 4, 5*
IA-11	✓	

Identification and Authentication		
IA-12	✓	

Incident Response		
Control	*Relevant Guidance*	*Relevant Enhancements*
IR-1	✓	
IR-2	✓	1
IR-3	✓	2, 3
IR-4	✓	3, 4, 6, 7, 8, 11, 14, 15
IR-5	✓	
IR-6	✓	
IR-7	✓	2
IR-8	✓	

Maintenance		
Control	*Relevant Guidance*	*Relevant Enhancements*
MA-1	✓	
MA-2	✓	
MA-4	✓	1, 4, 5, 7
MA-5	✓	1, 2, 3, 4, 5
MA-6	✓	1
MA-7	✓	

Media Protection		
Control	*Relevant Guidance*	*Relevant Enhancements*
MP-1	✓	
MP-2	✓	
MP-3	✓	
MP-4	✓	

Media Protection		
MP-6	✓	
MP-7	✓	

Physical and Environmental Protection		
Control	*Relevant Guidance*	*Relevant Enhancements*
PE-1	✓*	
PE-2	✓*	1, 3
PE-3	✓*	1, 2, 3, 4, 5, 7, 8
PE-4	✓	
PE-6	✓	1, 2, 3, 4
PE-8	✓	
PE-9	✓	
PE-11	✓	1, 2
PE-12	✓	
PE-13	✓	
PE-14	✓	
PE-15	✓	
PE-16	✓	
PE-18	✓*	
PE-23	✓	

Planning		
Control	*Relevant Guidance*	*Relevant Enhancements*
PL-1	✓*	
PL-2	✓*	
PL-4	✓	1
PL-7	✓*	
PL-8	✓	1
PL-9	✓*	

Planning		
PL-10	✓*	
PL-11	✓*	

Program Management		
Control	*Relevant Guidance*	*Relevant Enhancements*
PM-1	✓	
PM-2	✓	
PM-8	✓	
PM-9	✓	
PM-10	✓	
PM-11	✓	
PM-12	✓	
PM-14	✓	
PM-15	✓	
PM-16	✓	
PM-22	✓	
PM-25	✓	
PM-26	✓	
PM-28	✓	
PM-30	✓	

Personnel Security		
Control	*Relevant Guidance*	*Relevant Enhancements*
PS-1	✓	
PS-2	✓	
PS-3	✓	
PS-4	✓*	
PS-5	✓	
PS-6	✓	

Personnel Security		
PS-7	✓	
PS-8	✓	
PS-9	✓	

Personally Identifiable Information Processing and Transparency
No applicable controls

Risk Assessment		
Control	*Relevant Guidance*	*Relevant Enhancements*
RA-1	✓	
RA-2	✓	
RA-3	✓	1
RA-5	✓	2, 11
RA-7	✓	

System and Service Acquisition		
Control	*Relevant Guidance*	*Relevant Enhancements*
SA-1	✓	
SA-2	✓	
SA-3	✓	1, 2, 3
SA-4	✓*	9, 10
SA-5	✓	
SA-8	✓	
SA-9	✓*	1, 2, 3, 4, 5, 8
SA-22	✓	

System and Communications Protection		
Control	*Relevant Guidance*	*Relevant Enhancements*
SC-1	✓	

System and Communications Protection		
SC-5	✓	
SC-7	✓	
SC-8	✓	1
SC-12	✓*	
SC-13	✓	1, 2
SC-15	✓	
SC-16	✓*	2
SC-17	✓*	
SC-20	✓	
SC-21	✓	
SC-22	✓	
SC-28	✓*	1
SC-39	✓	

System and Information Integrity		
Control	*Relevant Guidance*	*Relevant Enhancements*
SI-1	✓	
SI-2	✓	
SI-3	✓	
SI-4	✓	
SI-5	✓	
SI-12	✓	

Supply Chain Risk Management		
Control	*Relevant Guidance*	*Relevant Enhancements*
SR-1	✓	
SR-2	✓	1
SR-3	✓	
SR-5	✓	

Supply Chain Risk Management		
SR-6	✓	
SR-8	✓	
SR-10	✓	
SR-11	✓	1, 2, 3
SR-12	✓	

6. SUPPLEMENTAL GUIDANCE TO CONTROLS AND ENHANCEMENTS

6.1. ACCESS CONTROL (AC)

AC-1 Policy and Procedures
Applicable Control from 800-53
a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] access control policy that a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the access control policy and the associated access controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and c. Review and update the current access control: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency]

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
AC-1	Access policies and procedures should be documented in Access Control Policy or codified standard operating procedures.	Implementation of ePACS should take into consideration authentication factors supported by PIV and defined in [SP 800-116] in conjunction with

	ePACS should be designed and procured (SA-4) in accordance with mandatory requirements placed on physical access control systems ([M-19-17], [OMB A-11]).	Table 6 - Recommended Authentication Factors below. While not all Common Access Cards [CAC] currently support PKI-CAK, there is no restriction on using more factors than recommended.

Required Authentication Factors	Authentication Mechanism(s)	Interface
One	PKI-CAK	Contactless
Two	PKI-Auth	Contact or Virtual Contact
Three	PKI-Auth + BIO	Contact or Virtual Contact

Table 6 - Recommended Authentication Factors

Navigation to Associated Controls*:* IA-5 (2) PL-7

AC-2 Account Management
Applicable Control from 800-53
a. Define and document the types of accounts allowed for use within the system; b. Assign account managers; c. Establish conditions for group and role membership; d. Specify:

1. Authorized users of the system;
2. Group and role membership; and
3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;

e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;
f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, and conditions];
g. Monitor the use of accounts;
h. Notify account managers and [Assignment: organization-defined personnel or roles] within:
   1. [Assignment: organization-defined time-period] when accounts are no longer required;
   2. [Assignment: organization-defined time-period] when users are terminated or transferred; and
   3. [Assignment: organization-defined time-period] when system usage or need-to-know changes for an individual;
i. Authorize access to the system based on:
   1. A valid access authorization;
   2. Intended system usage; and
   3. [Assignment: organization-defined attributes (as required)];
j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency];
k. Establish and implement a process for changing shared or group account credentials (if deployed) when individuals are removed from the group; and
l. Align account management processes with personnel termination and transfer processes

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
AC-2;a/f	ePACS can be split into two families of users. One being ePACS application users who interact with the software and the second being cardholders who are authorized to access a physical resource. ePACS systems access rights should be documented defining categories of users.	Entities having authority over the operations of ePACS and authority of physical security of facilities should define and document authorized populations that interact with ePACS system.

	Access to ePACS software should also follow this guidance for ePACS application users.	Access to spaces controlled by ePACS should follow this guidance. In-person registration includes a biometric verification of the cardholder. The Access Control Policy may require gathering attributes beyond those available from the card (e.g., data from personnel security systems of record). It is recommended that the ePACS always record the following from a PIV or PIV-Interoperable (PIV-I) Card: ● CHUID ● PIV Authentication Certificate; and ● Card Authentication Certificate (if available) [Removal of accounts should follow guidance outline in PS-4]
AC-2 (1) Support the management of system accounts using [Assignment: organization-defined automated mechanisms.]	Access to ePACS software should also follow this guidance for application users.	ePACS accepts import and modifications of records from a source it trusts and that complies with the security requirements.
AC-2 (3) Disable accounts when the accounts: (a) Have Expired; (b) Are no longer associated with a user or individual; (c) Are in violation of organizational	Access to ePACS software should also follow this guidance for both application users and cardholders.	ePACS system for card holders should follow this guidance Special consideration should be taken for persons who do not qualify for PIV credentials as defined in [SP 800-

policy; or (d) Have been inactive for [Assignment: organization-defined time-period]		116], and temporary credentials issued to employees or visitors.

AC-3 ACCESS ENFORCEMENT
Applicable Control from 800-53
Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
AC-3	ePACS is configured to follow documented access rules specified in the Access Control Policy or documented standard operating procedures. Example include: ● Work Time and schedule; ● Role/group access; ● Escalation of authentication factors based on time/schedule. ● Usage of Authentication Factors as determined by [SP 800-116]	Operations follow guidelines established in AC-1 and PL-7.
AC-3 (3) Mandatory Access Control Enforce [Assignment: organization-defined mandatory access control policy] over the set	ePACS application users should be prevented from remotely actuating physical devices higher than their security	Physical access to facilities or areas, should follow rules established in Facility Access Control Policies and

of covered subjects and objects specified in the policy, and where the policy: a. Is uniformly enforced across the covered subjects and objects within the system; b. Specifies that a subject that has been granted access to information is constrained from doing any of the following; 1. Passing the information to unauthorized subjects or objects; 2. Granting its privileges to other subjects; 3. Changing one or more security attributes (specified by the policy) on subjects, objects, the system, or system components; 4. Choosing the security attributes and attribute values (specified by the policy) to be associated with newly created or modified objects; and 5. Changing the rules governing access control; and c. Specifies that [Assignment: organization-defined subjects] may explicitly be granted [Assignment: organization-defined privileges] such that they are not limited by any defined subset (or all) of the above constraints.	assignment allows, as this would potentially allow improper access to resources. Additionally, ePACS application users should not be able to elevate other user privileges higher than what their authorization allows within the application.	should be granted on an individual basis following established IA Family Policies in conjunction with agency defined account management practices.

AC-3 (8) Revocation of Access Authorization Enforce the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on [Assignment: organization-defined rules governing the timing of revocations of access authorizations].		The ePACS verifies that the PIV or PIV-I subject has not been excluded by an ePACS software user or administrator. Revocation of access to physical spaces should occur within [Assignment: organization-defined time frame] depending on reason for revocation of access.
AC-3 (10) Employ an audited override of automated access control mechanisms under [Assignment: organization-defined conditions] by [Assignment: organization-defined roles].		Any override of normal documented operations must be audited per AU-2.

6.2. AWARENESS AND TRAINING (AT)

AT-3 Role-Based Training
Applicable Control from 800-53
a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined roles and responsibilities]: 1. Before authorizing access to the system, information, or performing assigned duties, and [Assignment: organization-defined frequency] thereafter; and 2. When required by system changes; and b. Update role-based training [Assignment: organization-defined frequency].

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
AT-3 (2) Physical Security Controls Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of physical security controls.		An organization establishes, conducts, and complies with PACS-related training policies and procedures, especially as it relates to those roles responsible for on-premises security (e.g., guards).

6.3. AUDIT AND ACCOUNTABILITY (AU)

AU-1 Policy and Procedures
Applicable Control from 800-53
a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] audit and accountability policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and c. Review and update the current audit and accountability: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency].

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
AU-1	Auditing of ePACS software should also follow this guidance.	The ePACS logs auditable events as documented in the Access Control Policy and information security assessment. Ensure Audit controls are in line with physical security requirements around IT risk classification.

AU-2 Audit Events
Applicable Control from 800-53
a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2 a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
AU-2 (c)	The ePACS logs the following software events: ● Verification of Trusted Origin at registration (in person or automated) ● Automated registration and modification of ePACS records ● Path Validation Periodic re-validation of registered cards or time of registration ● Mappings, transforms, or translation of numbers or identifiers used by	The ePACS logs the following physical events: ● AC-3 Access Enforcement (e.g., Authorization decisions) ● Access Granted ● Access Denied, specific reason for denial also logged ● Individual and group reporting of alarms (e.g., door force, door prop); In accordance with physical security requirements around IT risk classification

	different parts of the system. (This is often called credential number processing and transmission) ● Time updates of system components, system time ● Software or firmware updates ● Configuration changes ● Administrator actions	● Authentication Factor(s) verified (e.g., PIV Authentication Key, PIN, and/or biometric) at registration (in person) ● Modification to ePACS system components (e.g., verification of software driven configuration changes) ● Any modification of the operating condition of condition status of the ePACS system components (e.g., authentication factor change at readers, access granted through the door by a non-cardholder through software, any override of normal operations)

AU-3 Content of Audit Records
Applicable Control from 800-53
Ensure that audit records contain information that establishes the following: a. What type of event occurred; b. When the event occurred; c. Where the event occurred; d. Source of the event; e. Outcome of the event; and f. Identity of any individuals, subjects, or objects/entities associated with the event

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
AU-3	ePACS software should also follow this guidance.	Field component time should be synchronized with ePACS software time to ensure proper audit accountability. Time zones should also be taken into consideration when devices in different time zones from ePACS servers. Events as defined in AU-2 should contain unique device identifiers able to identify source of the generating event, condition generating event, and time of event generation.

AU-6 Content of Audit Records

Applicable Control from 800-53
a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; b. Report findings to [Assignment: organization-defined personnel or roles]; and c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
AU-6	ePACS software should adequately meet the audit requirements for spaces with high security requirements, as defined in PL-7.	
AU-6 (3) Organization-wide situational awareness includes awareness across all three levels of risk management (i.e., organizational level, mission/business process level, and information system level) and supports cross-organization awareness.		ePACS provides capability to analyze and correlate audit logs from various components, devices, cardholder interactions, or archived sources. Practice Note: ePACS logs can be provided to additional teams within an organization (e.g., Continuous Diagnostics and Mitigation (CDM), Insider Threat, and traditional network/IT security operations monitoring).

6.4. ASSESSMENT, AUTHORIZATION, AND MONITORING (CA)

CA-2 Control Assessments
Applicable Control from 800-53
a. Develop a control assessment plan that describes the scope of the assessment including: 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities;

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
CA-2	An assessment plan should be created and implemented pertaining to the facilities falling under operation of ePACS system. Assessment should cover, at a minimum: ● Facility architecture ● ePACS system configuration ● PKI validation components	Entities having responsibility for the security of the facilities should be included in the creation of assessment criteria. Plan should incorporate existing physical security operational considerations.

CA-6 Authorization
Applicable Control from 800-53
a. Assign a senior official as the authorizing official for the system; b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;

c. Ensure that the authorizing official for the system, before commencing operations:
  1. Accepts the use of common controls inherited by the system; and
  2. Authorizes the system to operate;
d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;
e. Update the authorizations [Assignment: organization-defined frequency]

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
CA-6	The ePACS meets security authorization requirements of FISMA. The security controls been approved and the applicable assessments have been performed (e.g., [SP 800-116]) on the ePACS and approved by the authority(ies) having jurisdiction over the operations and maintenance of the system and its components.	

6.5. CONFIGURATION MANAGEMENT (CM)

CM-2 Baseline Configuration
Applicable Control from 800-53
a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and b. Review and update the baseline configuration of the system: 1. [Assignment: organization-defined frequency]; 2. When required due to [Assignment organization-defined circumstances]; and 3. When system components are installed or upgraded

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
CM-2:b.1, b.3	Periodic review of system configuration against documented baseline configuration should occur. Components should include software versions of installed ePACS software, versions of all internet protocol (IP) connected field devices (e.g., firmware, revisions) and physical location of field devices. ePACS deployment and baseline should align when performing a system update. All software and IP connected components should meet new baseline standards when updates occur.	Periodic review of operational status of ePACS components should occur. All IP connected field devices should have operational configurations reviewed according to Access Control Policy baselines.

CM-5 Access Restrictions for Change
Applicable Control from 800-53
Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
CM-5 (5) Privilege Limitation for Production and Operation (a) Limit privileges to change system components and system-related information within a production or operational environment; and (b) Review and reevaluate privileges [Assignment: organization-defined frequency].	The ePACS has the ability to enforce administrative privilege for configuration management operations. Standard IT administrative operations are separate from administrative rights within the ePACS software. Baseline configurations should follow agency specific guidelines (e.g. US Government Configuration Baseline (USGCB), Security Technical Implementation Guides (STIGs)). Periodic review of ePACS application users and application privileges should be established to ensure compliance with AC-2.	The ePACS has the ability to enforce administrative privilege for configuration management operations within the ePACS software, separate from administrative privileges within the IT operational environment. Authentication to ePACS software corresponds to the highest level of authentication mechanisms enforced at physical spaces controlled by ePACS software. A process to periodically review cardholder groups, definitions, and privileges according to policy (AC-2 (a) and PL-7) should be established.

CM-6 Configuration Settings
Applicable Control from 800-53
a. Establish and document configuration settings for components employed within the system using [Assignment: organization-defined common secure configurations] that reflect the most restrictive mode consistent with operational requirements; b. Implement the configuration settings; c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization- defined operational requirements]; and d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
CM-6	Nominal operations should be established and documented (CM-2). Baseline configurations should follow agency specific guidelines (e.g., USGCB, STIGs).	Deviation from baseline operations must be an auditable event (AU-2).

6.6. CONTINGENCY PLANNING (CP)

CP-4 Contingency Plan Testing
Applicable Control from 800-53
a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests]. b. Review the contingency plan test results; and c. Initiate corrective actions, if needed.

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
CP-4		All ePACS system components should be periodically tested to meet the documented continued operations policies and procedures. This includes, but is not limited to software, servers, and field components.

CP-9 System Backup
Applicable Control from 800-53
a. Conduct backups of user-level information contained in [Assignment: organization-defined system components] [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];

b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];
c. Conduct backups of system documentation, including security and privacy-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and
d. Protect the confidentiality, integrity, and availability of backup information

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
CP-9		ePACS system components should follow this guidance. Any components unable to be backed up (e.g., field devices, card readers) should fall under the guidance defined in CP-10.

CP-10 System Recovery and Reconstitution
Applicable Control from 800-53
Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time-period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
CP-10 (2) Transaction Recovery	ePACS systems should be capable of	Field components should be capable

Implement transaction recovery for systems that are transaction-based.	recovering transactions generated when field components are operating in a disconnected mode from the ePACS software.	of operating in a disconnected mode without loss of transaction records for [Assignment: organization-defined time-period].
CP-10 (4) Restore within Time period Provide the capability to restore system components within [Assignment: organization-defined restoration time-periods] from configuration-controlled and integrity-protected information representing a known, operational state for the components.	ePACS should support replacement or restoration of the ePACS infrastructure and software within [Assignment: Organization-defined restoration time-period] ePACS application should continue operation until restoration of service according to IA-5. Practice note: PKI components are outside the scope of this overlay; however, special consideration should be taken to ensure PKI has redundancies compatible with ePACS application.	ePACS components should support field component restoration from stored configuration and any associated trust stores through configuration download.

6.7. IDENTIFICATION AND AUTHENTICATION (IA)

IA-2 Identification and Authentication (Organizational Users)
Applicable Control from 800-53
Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
IA-2	ePACS is configured to utilize PKI (SC-12) to allow PIV credentials issued from [Assignment: Organization-defined] to uniquely identify application users within ePACS. ePACS system must be able to map unique identifiers from administrator PIV (e.g., FASC-N, UUID, altSecID).	Physical access privileges assigned to users follow [SP 800-116] authentication mechanisms and enforced by policies in AC-3, PL-1, PL-7. Unique identifiers registered to each user (e.g., FASC-N, UUID, altSecID mapping, or concatenation of other fields from acceptable X.509 certificates).
IA-2 (2) Multifactor Authentication to Non-Privileged Accounts		Physical access privileges assigned to users follow [SP 800-116] authentication mechanisms and

		enforced by policies in AC-3, PL-1, PL-7.
IA-2 (8) Access to Accounts - Replay Resistant Implement replay-resistant authentication mechanisms for access to [Selection (one or more): privileged accounts; non-privileged accounts]	ePACS applications should be configured to allow [FIPS 201] certified credentials (e.g., PIV, PIV-I) and associated PKI (IA-5 (2)) authentication mechanisms which prevent private key replay. Additional secure authenticators are also allowed, such as One-Time Passwords (OTP).	Systems should be configured to only allow [FIPS 201] certified credentials (e.g. PIV, PIV-I) and their associated PKI (IA-5 (2)) or biometric functionalities based on access control policies.
IA-2 (12) Acceptance of PIV Credentials Accept and electronically verify Personal Identity Verification-compliant credentials	ePACS to be configured to allow [FIPS 201] defined PIV credentials in support of administrative use.	Systems should be configured to allow [FIPS 201] defined PIV credentials.

IA-5 Authenticator Management
Applicable Control from 800-53
Manage system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator; b. Establishing initial authenticator content for any authenticators issued by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators; e. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; f. Changing default authenticators prior to first use;

g. Changing or refreshing authenticators [Assignment: organization-defined time-period by authenticator type];
h. Protecting authenticator content from unauthorized disclosure and modification;
i. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and
j. Changing authenticators for group or role accounts when membership to those accounts changes.

Control Enhancements

Applicable Enhancement	Administration	Operations
IA-5 (2) Public Key-Based Authentication a. For public key-based authentication: 1. Enforce authorized access to the corresponding private key; and 2. Map the authenticated identity to the account of the individual or group; and b. When public key infrastructure (PKI) is used: 1. Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and 2. Implement a local cache of revocation data to support path discovery and validation.	The ePACS utilizes PKI and verifies: ● the issuer, ● that the reference authenticator is created by the issuer and ● that the reference authenticator is not altered and is still valid ● Full path validation occurs at time of registration and re-validation of certificate at time of access. ● presents proof of holder of key (PKI + PIN) The ePACS verifies the signatures of any signed objects and uses PDVal for signed objects involved in authentication (e.g., authenticating acceptance devices, the card or the card holder). Appropriate RFC5280 certificate proccing to include: ● Name constraints; ● Policy Mapping; ● Basic Constraint Checking; ● Name Chaining;	ePACS is configured to grant access to PIV or PIV-I like (or other locally trusted certificate based) credentials that meet the validation criteria configured (See Table 6 - Recommended Authentication Factors). Minimally, the ePACS utilizes PKI and verifies: ● the issuer, ● that the reference authenticator is created by the issuer and ● that the reference authenticator is not altered and is still valid ePACS is configured to only grant access to credentials that meet the validation criteria configured

	• Signature Chaining; • Certificate Validity; • Key usage, basic constraints, and certificate policies certificate extensions; • Full CRLs; and • CRLs segmented on names. ePACS periodically re-validated stored certificates to ensure updated status and validity of enrolled certificates.	
IA-5 (6) Protection of Authenticators Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access		Category of systems being protected by ePACS needs to be secured to the related security level. Authentication factors required to access those systems as outlined in [SP 800-116] should be consistent with system classification.
IA-5 (12) Biometric Authentication Performance: For biometric-based authentication, employ mechanisms that satisfy the following biometric quality requirements [Assignment: organization-defined biometric quality requirements]		ePACS deployment of biometric devices meets the criteria [Assignment: organization-defined biometric quality requirements] and meets the authentication mechanisms for biometrics outline in [SP 800-76]. Other biometric devices or associated quality settings per individual can be employed if exceptions are documented.
IA-5 (14) Managing content of PKI Trust Stores	Systems operating ePACS should be included in the distribution and	

For PKI-based authentication, employ an organization-wide methodology for managing the content of PKI trust stores installed across all platforms, including networks, operating systems, browsers, and applications.	management of PKI trust stores. External trust stores may need to be included as part of the PKI management plan IA-5 (9) to allow proper usage and management of external federal entities and approved PIV-I cardholders.	
IA-5 (15) GSA-Approved Products and Services: Use only General Services Administration-approved and validated products and services for identity, credential, and access management.	ePACS products (hardware and software) are to be acquired from GSA's FIPS 201 Approved Product List with versions consistent with tested version (SA-4).	Deployed card readers, card reader interface modules, and/or card reader control modules, and other associated software should meet Approved Product List Architecture and versions listed on GSA's FIPS 201 Approved Product List approval letter.

IA-7 Cryptographic Module Authentication

Applicable Control from 800-53

Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

Control Enhancements

Applicable Enhancement	Administration	Operations
IA-7		Devices purchased in accordance with IA-5 (15) and SA-4 meet this requirement.

IA-8 Identification and Authentication (non-organizational users)
Applicable Control from 800-53
Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
IA-8 (1) Acceptance of PIV Credentials from other Agencies. Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.	ePACS accepts certificate-based credentials (PIV/CAC) from other agencies as allowable by [Assignment: organization- defined policy] (SC-12).	Usage limitations on credentials from other agencies as defined by [Assignment: organization- defined policy]. While not all CAC currently support PKI-CAK, there is no restriction on using more factors than recommended.
IA-8 (5) Acceptance of PIV-I Credentials Accept and verify federated or PKI credentials that meet [Assignment: organization- defined policy]	ePACS accepts certificate-based credentials PIV-I from other organizations as allowable by [Assignment: organization- defined policy] (SC-12, [SP 800-116]).	Usage limitations on credentials from other organizations as defined by [Assignment: organization- defined policy].

6.8. PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

PE-1 Policy and Procedures
Applicable Control from 800-53
a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles] 1. [Selection (one or more): organization-level; mission/business process-level; system-physical and environmental protection policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and c. Review and update the current physical and environmental protection: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency].

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
PE-1	Physical and environmental protection policy should be created in coordination with entities responsible for physical security of facilities.	Physical and environmental protection policy should take into account security categorization of resources (electronic or physical), personnel, or data, being protected.

PE-2 Physical Access Authorizations
Applicable Control from 800-53
a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides; b. Issue authorization credentials for facility access; c. Review the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and d. Remove individuals from the facility access list when access is no longer required

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
PE-2 (x)	Access policies and procedures should be documented in Access Control Policy or codified standard operating procedures (AC-1). Policies should be maintained to determine which individuals or groups of individuals (AC-2) have access to the facilities (e.g., employees, contractors, visitors)	Facility Access Control Policy or codified standard operating procedures should determine what spaces individuals or groups of individuals (AC-2) can access, and any limitations of those spaces (AC-3 PL-7).

PE-3 Physical Access Control

Applicable Control from 800-53

a. Enforce physical access authorizations at [Assignment: organization-defined entry and exit points to the facility where the system resides] by:
    1. Verifying individual access authorizations before granting access to the facility; and
    2. Controlling ingress and egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems or devices]; guards];
b. Maintain physical access audit logs for [Assignment: organization-defined entry or exit points];
c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [Assignment: organization-defined controls];
d. Escort visitors and monitor visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and monitoring];
e. Secure keys, combinations, and other physical access devices;
f. inventory [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and
g. Change combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated

Control Enhancements

Applicable Enhancement	Administration	Operations
PE-3:a		ePACS system should be configured to ensure installation and configuration conform to system planning in PL-2.
PE-3:a.1		Authorization of access rights should conform to security requirements developed in PL-1.

PE-3:a.2		ePACS systems should conform to [SP 800-116] authentication mechanisms, and implemented in accordance with site security requirements as created in PL-1.
PE-3:b	ePACS should be able to maintain audit logs as required in AU-2 and AU-3.	ePACS should be configured to maintain audit logs as required in AU-2 and AU-3.
PE-3:c		ePACS systems should conform to [SP 800-116] authentication mechanisms, and implemented in accordance with site security requirements as specified by PL-1.

PE-18 Location of System Components
Applicable Control from 800-53
Position system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
PE-18	The ePACS performs all automated system security relevant processing (IA-	The ePACS performs all individual security relevant processing (IA-2,

	2, IA-5) on the secure side of the physical security boundary: ● PKI PDVal ● Biometric matching for 1:1 verification ● Certificate revocation and status checking ● Credential identifier processing	IA-5) on the secure side of the physical security boundary: ● PKI PDVal ● Nonce generation ● Challenge/response ● Biometric matching for 1:1 verification ● Certificate revocation and status checking ● Credential identifier processing ● Authorization decisions

6.9. PLANNING (PL)

PL-1 Policy and Procedures
Applicable Control from 800-53
a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] planning policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the planning policy and the associated planning controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; and c. Review and update the current planning: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency].

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
PL-1	System owners should create Access Control Policy or formalize standard operating procedures to meet this control.	System operators should create Access Control Policy or formalize standard operating procedures to meet this control, taking into consideration authentication modes, assurance levels, population definitions, accessing populations, rules of access, time of day restrictions, and threat level restrictions and exceptions. Access

		Control policy should also address events which are recorded in the audit logs (AU-2).

PL-2 System Security and Privacy Plans

Applicable Control from 800-53

a. Develop security and privacy plans for the system that:
   1. Are consistent with the organization's enterprise architecture;
   2. Explicitly define the constituent system components;
   3. Describe the operational context of the system in terms of missions and business processes;
   4. Provide the security categorization of the system, including supporting rationale;
   5. Describe any specific threats to the system that are of concern to the organization;
   6. Provide the results of a privacy risk assessment for systems processing personally identifiable information;
   7. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;
   8. Provide an overview of the security and privacy requirements for the system;
   9. Identify any relevant control baselines or overlays, if applicable;
   10. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;
   11. Include risk determinations for security and privacy architecture and design decisions;
   12. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]; and
   13. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

b. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles];

c. Review the plans [Assignment: organization-defined frequency];

d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and

e. Protect the plans from unauthorized disclosure and modification.

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
PL-2	The ePACS Access Control Policy or formalized security operations specifies the PACS Assurance Level required for protecting this facility in accordance with authentication mechanisms defined in [SP 800-116]. Security and privacy plans around Administration of ePACS (PL-2) should be approved by authorizing officials which have authority over IT systems.	The ePACS Access Control Policy or formalized security operations specifies the PACS Assurance Level required for protecting this facility in accordance with authentication mechanisms defined in [SP 800-116]. Security and privacy plans around operations of ePACS (PL-2) should be approved by authorizing officials which have authority over physical access.

PL-7 Concept of Operations
Applicable Control from 800-53
a. Develop a Concept of Operations (CONOPS) for the system describing how the organization intends to operate the system from the perspective of information security and privacy; and b. Review and update the CONOPS [Assignment: organization-defined frequency].

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
PL-7		Concept of operations for the facility

		access should take into consideration the following ● ePACS authentication factors and mechanisms listed in Table 6 - Recommended Authentication Factors, should be selected for protecting the facility based on the FSL determination ● Authentication Mechanisms required and permitted for each security area as defined in [SP 800-116] ● Various populations of individuals for whom access to the facility is controlled. (AC-3) ● Rules of access for each population of individuals for whom access to the facility is controlled ● Time of Day restrictions for access ● Exceptions for access that are based on threat level ● Events recorded in the audit log (AU-2)

PL-9 Central Management
Applicable Control from 800-53
Centrally manage [Assignment: organization-defined controls and related processes]

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
PL-9	The ePACS centrally implements the identification and authentication measures specified in the Access Control Policy, including: authentication modes, accessing populations, time of day restrictions, and threat level restrictions and exceptions. (PL-1) documents the policy that the ePACS enforces during identification and authentication.	The ePACS centrally implements the identification and authentication measures specified in the Access Control Policy or documented security procedures, including authentication modes, accessing populations, time of day restrictions, and threat level restrictions and exceptions. (PL-1) documents the policy that the ePACS enforces during identification and authentication policies.

PL-10 Baseline Selection
Applicable Control from 800-53
Select a control baseline for the system

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
PL-10	Control Baselines are pre-defined sets of controls (including authentication mechanisms defined in [SP 800-116]) specifically assembled to address the protection needs of a group, organization, or community of interest. The Access Control Policy or formalized security operations contains criteria for categorizing areas, authentication mechanisms associated with areas should align with requirements detailed in [SP 800-116].	Control Baselines are pre-defined sets of controls (including authentication mechanisms defined in [SP 800-116]) specifically assembled to address the protection needs of a group, organization, or community of interest. The Access Control Policy or formalized security operations contains criteria for categorizing areas, authentication mechanisms associated with areas should align with requirements detailed in [SP 800-116].

PL-11 Baseline Tailoring
Applicable Control from 800-53
Tailor the selected control baseline by applying specified tailoring actions

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
PL-11	Systems protected by ePACS should have their [FIPS 199] categorization taken into consideration when applying [SP 800-	Authentication mechanisms defined by [SP 800-116] should take into consideration the [FIPS 199]

	53B] tailoring guidance.	categorization of the areas or facility FSL

6.10. PERSONNEL SECURITY (PS)

PS-4 Personnel Termination
Applicable Control from 800-53
Upon termination of individual employment: a. Disable system access within [Assignment: organization-defined time-period]; b. Terminate or revoke any authenticators and credentials associated with the individual; c. Conduct exit interviews that include a discussion of [Assignment: organization-defined information security topics]; d. Retrieve all security-related organizational system-related property; and e. Retain access to organizational information and systems formerly controlled by terminated individual.

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
PS-4 (a)	Removal of access to ePACS application should be defined in operational policy for account removal in AC-2.	Removal of access to physical spaces as defined in AC-2.

6.11. SYSTEM AND SERVICES ACQUISITION (SA)

SA-4 Acquisition Process
Applicable Control from 800-53
Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service: a. Security and privacy functional requirements; b. Strength of mechanism requirements; c. Security and privacy assurance requirements; d. Controls needed to satisfy the security and privacy requirements e. Security and privacy documentation requirements; f. Requirements for protecting security and privacy documentation; g. Description of the system development environment and environment in which the system is intended to operate; h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and i. Acceptance criteria

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
SA-4	The ePACS incorporates components listed on the GSA FIPS 201 APL at all points in the system where products from an APL category are appropriate.	

SA-9 External System Services
Applicable Control from 800-53
a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls]; b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques].

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
SA-9	ePACS systems used for internal alarm monitoring must have UL1076 certification. System used for monitoring external alarms must have UL1610 certification and ensure communications to external alarm monitoring service providers are appropriately protected. ePACS systems using external ePACS system hosting are FedRAMP certified [OMB 10-28].	ePACS systems used for internal alarm monitoring must have UL1076 certification. System used for monitoring external alarms must have UL1610 certification and ensure communications to external alarm monitoring service providers are appropriately protected. ePACS systems using external ePACS system hosting are FedRAMP certified [OMB 10-28].

6.12. SYSTEM AND COMMUNICATIONS PROTECTION (SC)

SC-12 Cryptographic Key Establishment and Management
Applicable Control from 800-53
Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
SC-12	The ePACS provides or relies on a trust store for Root and Issuing Certification Authorities as authorized for the ePACS per IA-5(9) and IA-5(14). The ePACS allows for Create, Read, Update, and Delete (CRUD) management of trust store. This mechanism is used to provide management of the minimum set of trust anchors necessary to operate the ePACS.	

SC-16 Transmission of Security and Privacy Attributes
Applicable Control from 800-53
Associate [Assignment: organization-defined security and privacy attributes] with information exchanged between systems and between system components.

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
SC-16		ePACS system components utilizing default passwords or certificates for communication and transmission of cardholder data should have the capability to generate new passwords or certificates and not rely on system defaults to protect data transmission.

SC-17 Public Key Infrastructure Certificates
Applicable Control from 800-53
a. Issue public key certificates under an [Assignment: organization-defined certificate policy] or obtain public key certificates from an approved service provider; and b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
SC-17		Entities that have authority over physical security of facilities should define lists of external certificate authorities to be trusted by ePACS. Trust of external certificate authorities should be managed per the organization's certificate management statement or identification and authentication policy (see SC-12 IA-5(9) IA-5(14)).

SC-28 Protection of Information at Rest
Applicable Control from 800-53
Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].

Control Enhancements		
Applicable Enhancement	**Administration**	**Operations**
SC-28	Systems containing ePACS data need to have security controls in place that appropriately reflect the usage of the ePACS. The areas being physically protected, and audit records of those areas need to be considered. Additionally, any classification of individual cardholder PII should be in consideration.	

APPENDIX A: REFERENCES

[Countermeasures] The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, Appendix B: Countermeasures, 2019 FOUO, available upon request from ISCAccess@hq.dhs.gov

[FIPS 199] Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004 (as amended) https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

[FIPS 201] Federal Information Processing Standards Publication 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013 (as amended) https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

[GAO-19-138] Federal Building Security; Actions Needed to Help Achieve Vision for Secure, Interoperable Physical Access Control, December 2018 https://www.gao.gov/assets/700/696229.pdf

[M-10-15] Office of Management and Budget Memorandum 10-15, FY2010 Reporting Instructions for Federal Information Security Management Act and Agency Privacy Management, April 2010 https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2010/m10-15.pdf

[M-10-28] Office of Management and Budget Memorandum 10-28, Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and Department of Homeland Security, July 2010 https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2010/m10-28.pdf

[M-19-17] Office of Management and Budget Memorandum 19-17, Enabling Mission Delivery through Improved Identity, Credential and Access Management, May 2019 https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

[OMB A-11] Office of Management and Budget Circular Number A-11, Preparation, Submission, and Execution of the Budget, July 2020 https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

[RMP] The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, 2nd Edition, November 2016 https://www.cisa.gov/publication/isc-risk-management-process

[SP 800-53] National Institute of Standards and Technology, Security and Privacy Controls for Federal Information Systems and Organizations; Special

Publication 800-53, September 2020 (as amended)
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[SP 800-53B] National Institute of Standards and Technology, Control Baselines for Information Systems and Organizations, Special Publication 800-53B, October 2020
https://csrc.nist.gov/publications/detail/sp/800-53b/final

[SP 800-76] National Institute of Standards and Technology, Biometric Specifications for Personal Identity Verification, Special Publication 800-76, July 2013 (as amended)
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[SP 800-116] National Institute of Standards and Technology, Guidelines for the Use of PIV Credentials in Facility Access, Special Publication 800-116, June 2018 (as amended)
https://csrc.nist.gov/publications/detail/sp/800-116/rev-1/final

[SP 1500-201] National Institute of Standards and Technology, Framework for Cyber-Physical Systems: Volume 1, Overview, Special Publication 1500-201, June 2017 (as amended)
https://www.nist.gov/publications/framework-cyber-physical-systems-volume-1-overview