



**INTERAGENCY
SECURITY
COMMITTEE**



FACILITY ACCESS CONTROL

An Interagency Security Committee Best Practice

2020 Edition

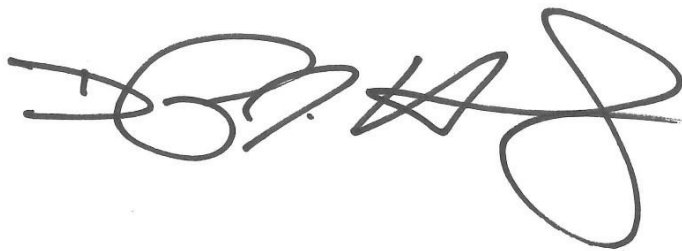
U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Interagency Security Committee

Message from the Chief

One of the priorities of the Department of Homeland Security (DHS) is the protection of federal employees and private citizens who work within and visit federally owned or leased facilities. The Interagency Security Committee (ISC), chaired by DHS, consists of 64 executive-level departments and agencies and has a mission to develop security policies, standards, and recommendations for nonmilitary federal facilities in the United States.

As Chief of the ISC, I am pleased to introduce the ISC document titled *Facility Access Control: An Interagency Security Committee Best Practice*. At a recent ISC Strategic Summit, members identified facility access control as their number-one subject area. Based on their request, the ISC formed a working group on facility access control, resulting in the development of this document. This ISC document provides guidance on addressing facility access control throughout the full access control process, from employee and visitor entry, through security screening, to the first point of authentication into nonpublic space.

This guide represents exemplary collaboration within the ISC Facility Access Control Working Group and across the entire ISC.

A handwritten signature in black ink, appearing to read 'Daryle Hernandez', with a large, stylized flourish at the end.

Daryle Hernandez
Chief, Interagency Security Committee

Table of Contents

- Message from the Chief..... 1**
- Table of Contents 2**
- 1.0 Purpose..... 4**
- 2.0 Background 4**
- 3.0 Applicability 5**
- 4.0 Access Control 5**
 - 4.1 Developing Access Control Procedures5
 - 4.1.1 Checking Identity Documents6
 - 4.1.2 Forms of Identity Documents Accepted6
 - 4.2 Communicating Access Control Procedures6
 - 4.2.1 Standardized Language7
 - 4.2.2 Communication Materials7
 - 4.2.3 Web-based Information7
 - 4.3 Entry Eligibility7
 - 4.3.1 PIV Cardholders8
 - 4.3.2 PIV-Interoperable Cardholders8
 - 4.3.3 Non-PIV Cardholders9
 - 4.4 REAL ID9
 - 4.4.1 Alternate Access Control Options 10
 - 4.5 Suspension, Removal, and Revocation 10
 - 4.6 Foreign Access Management..... 10
- 5.0 Screening..... 11**
 - 5.1 Security Screening Station..... 11
 - 5.2 Random Security Screening 12
 - 5.2.1 Methodology 12

5.2.2 Implementation	14
6.0 Escort Procedures	14
7.0 Physical Access Control Systems	15
7.1 PIV Assurance Level.....	16
8.0 FSL and PACS Considerations.....	17
8.1 Perimeter Considerations.....	18
8.2 Internal Agency Space Considerations	19
Appendix A: Foreign Access Management	20
A.1 Foreign National Vetting.....	22
Appendix B: List of Acceptable Forms of Identification.....	23
Appendix C: Flow Chart for Access Control	25
Appendix D: Resources.....	26
Glossary.....	26
List of Abbreviations, Acronyms, and Initializations.....	28
References: General.....	29
References: Foreign Access Management.....	31
Acknowledgements	33

1.0 Purpose

This document provides guidance for federal Executive Branch departments and agencies regarding access control requirements and options for individuals entering federally occupied space.

2.0 Background

The Interagency Security Committee (ISC) was formed by Executive Order (EO) 12977 following the Oklahoma City, OK bombing. This devastating event prompted the White House to establish a permanent body to address continuing government-wide physical security needs for federal facilities. Today, the ISC is chaired by the Department of Homeland Security (DHS) and consists of a permanent body with representatives from 64 federal departments and agencies.

The ISC is the authority on policies, standards, and recommendations related to the security and protection of federal facilities. After identifying the need for a single source of guidance on facility access control across Executive Branch departments and agencies, the ISC formed the Facility Access Control (FAC) Working Group to develop an authoritative guide to help federal departments and agencies better understand their obligations and requirements relating to common access to facilities. Given the ISC's diverse membership, the working group was able to draw upon a variety of subject matter experts to distill this information into a single best practices guide.

Facility access control has been an area of concern not only for ISC members, but also for government oversight entities. On December 20, 2018, the Government Accountability Office (GAO) issued a report titled *GAO-19-138, Federal Building Security Actions Needed to Help Achieve Vision for Secure, Interoperable Physical Access Control*. GAO was asked to examine physical access control systems (PACS) implementation efforts. Their recommendations included:

- The Office of Management and Budget (OMB) should determine and regularly monitor a baseline level of progress on PACS implementation.
- The ISC should assess the extent of, and develop strategies to address, government-wide challenges to implementing PACS.

When creating *Facility Access Control: An ISC Best Practice* (hereafter "this document"), the FAC Working Group was careful to recommend best practices that will assist agencies in implementing PACS and which are compliant with OMB policies and the Identity, Credential, and Access Management (ICAM) Roadmap and Implementation Guidance. This baseline understanding ensures greater consistency in approach, thereby allowing for more uniform evaluations and ongoing refinement.

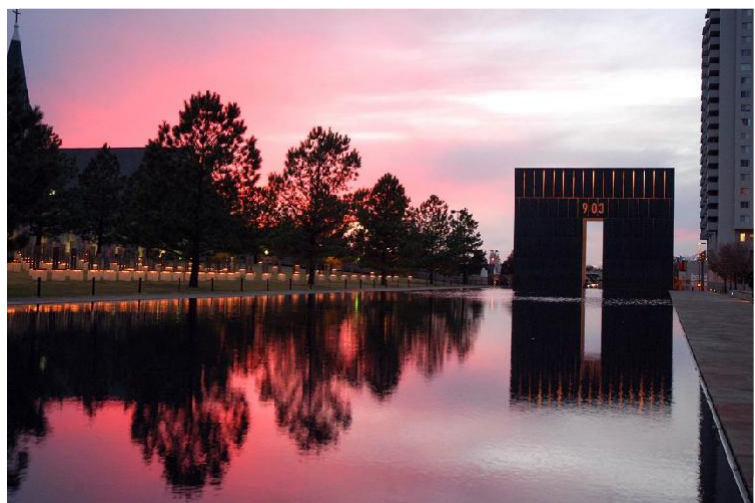


Photo: Sunset over Oklahoma City Memorial.

Additionally, agencies can better identify when to accept risk by comparing their protocols to the best practices outlined in the National Institute of Standards and Technology (NIST) Special Publication 800-116 (hereafter “NIST SP 800-116”) or any successive versions.

3.0 Applicability

Consistent with EO 12977, the guidance in this document applies to all nonmilitary federal Executive Branch departments and agencies within the borders of the United States and its territories. These include: existing owned, to be purchased, or leased facilities; standalone facilities; federal campuses; individual facilities on federal campuses; and special-use facilities.

This document does **not** require agencies to accept, nor individuals to present, identification (ID) where it is not required for access (e.g., to enter the public areas of the Smithsonian). This document also does **not** prohibit an agency from accepting other forms of identification such as a passport or military ID card.

4.0 Access Control

When developing access policies, a Facility Security Committee (FSC) or a representative of the tenant agency¹ should take into consideration the access needs of the tenants. Facility access policies should be consistent with:

- ISC standards;
- OMB and NIST policies and regulations;
- The facility’s current Facility Security Level (FSL), countermeasures, and security procedures (e.g., ability to meet the needs of the operating environment);
- The current tenant(s), visitors, volume of individuals, and security staff;
- The facility’s Occupant Emergency Plan (OEP);
- The Privacy Act of 1974; and
- The REAL ID Act of 2005.

4.1 Developing Access Control Procedures

When developing access control procedures for a federal facility, the facility should match security procedures with the threat against the tenant agencies.

¹ The Facility Security Committee makes most determinations for multi-tenant facilities. For single-tenant facilities, these determinations are generally made by a representative of the tenant agency. For more information about FSCs, refer to the *Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*, available on the ISC website.

4.1.1 Checking Identity Documents

Checking identity documents is useful when a tenant agency has a defined use for the resulting information, such as matching against a security watchlist or invitation list. Checking identity documents is least effective when the action does not tie into an overall security strategy.

A common access control use for a validated identity is to match that identity against an inclusion or exclusion list that establishes an individual's appropriateness to enter the facility. An inclusion list contains the names of individuals preapproved for entry. An exclusion list contains the names of individuals who should be denied entry. The document check provides evidence of the individual's identity, enhancing the effectiveness of inclusion or exclusion lists.



Photo: Checking identity documents.

4.1.2 Forms of Identity Documents Accepted

The type of ID acceptable to validate the individual's identity depends on several factors (e.g., level of risk, the type of federal resource accessed, and organization-specific requirements). The identity assurance level of a document depends on the process used by the issuer of the document to authenticate the document holder's identity as part of its issuance. For example, in issuing a Personal Identity Verification (PIV) card, federal agencies use a standardized process that provides the highest identity assurance appropriate to be able to access federal information systems and federally occupied facilities.

Where additional assurance of identity is needed, agencies should consider enacting policies to check the ID for signs of fraud or tampering and provide the ID verifier with training in fraud detection techniques and tools (e.g., magnifying devices and black lights) to assist in determining the validity of the documents presented.

4.2 Communicating Access Control Procedures

Agencies are encouraged to provide employees and visitors with information regarding access control procedures for the facility. This alleviates confusion and facilitates access by ensuring that employees and visitors have appropriate ID prior to accessing the facility. The best practice is to disseminate the access control procedures to employees and visitors through multiple channels. Such communication does not need to be all inclusive but should include:

- At a minimum, the most commonly accepted ID types; and
- A general statement of what individuals should expect if they are unable to produce an acceptable form of ID.

4.2.1 Standardized Language

To the extent possible, agencies should standardize the language used to explain ID requirements for individuals to access a federal facility. For example:



[AGENCY] requires visitors to present valid government-issued identification for access to its facilities.

For visitors presenting a state-issued driver's license or identification card, [AGENCY] only accepts such documents if they are **REAL ID compliant**. If your license is not REAL ID compliant, please bring an alternate form of government-issued photo ID, such as:

- Passport;
- Enhanced Driver's License; or
- Federal employee, military, or veteran identification card.

4.2.2 Communication Materials

DHS and the General Services Administration (GSA) have electronic files for posters and handouts available for agencies to use at access control points to inform individuals about access control requirements related to REAL ID. For more information about these requirements, refer to the Resources section of this document.

4.2.3 Web-based Information

Agencies are encouraged to post access control requirements on their public websites as a reference for individuals planning to visit their facilities. For example, the Transportation Security Administration (TSA) has a website informing travelers about forms of ID that are accepted at airport security checkpoints.

4.3 Entry Eligibility

In an access-controlled environment, the purpose for which the ID is required governs whether to make an access control decision. The following sections outline the categories of entry eligibility.

As defined below, departments and agencies must conduct a background investigation and adjudicate the results. If the results are favorable, the department or agency must also issue ID credentials to their employees, contractors, and affiliates who require long-term access to federally controlled facilities or information systems.

The phrase "departments and agencies" applies to:

- Executive departments and agencies listed in Title 5 United States Code (U.S.C.) § 101 and DHS;
- Independent establishments as defined by Title 5 U.S.C. § 104(1); and
- The United States Postal Service (USPS), Title 39 U.S.C. § 201.

The phrase "departments and agencies" does **not** apply to:

- Government corporations as defined by Title 5 U.S.C. § 103(1). However, such corporations are encouraged but not required to implement the OMB policy unless specified.

4.3.1 PIV Cardholders

As defined in OMB Policy M-05-24, PIV cardholders are individuals who meet the following criteria:

- Federal employees, as defined in Title 5 U.S.C. § 2105 "Employee," within a department or agency;
- Individuals employed by, detailed to, or assigned to a department or agency;
- Within the Department of Defense (DoD) and the Department of State (DoS), members of the Armed Forces, Foreign Service, and DoD and DoS civilian employees (including both appropriated fund and non-appropriated fund employees); and
- Individuals under contract to a department or agency requiring routine access to federally owned or controlled facilities or information systems who would be issued federal access control credentials.

Applicability to other agency-specific categories of individuals (e.g., guest researchers with a term of less than six months; volunteers; intermittent, temporary, or seasonal employees) is an agency risk-based decision.

Refer to OMB Policy M-05-24 for more information.

4.3.2 PIV-Interoperable Cardholders

The PIV-Interoperable (PIV-I) Card is an identity card that meets the PIV technical specifications of Federal Information Processing Standards (FIPS) 201 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. Each federal government relying party determines the extent to which it will trust PIV-I cards within its areas of control. Cardholder privileges in any situation are determined solely by the federal government relying party (i.e., PIV-I cards do **not** guarantee access of any kind, nor do they prevent issuance of a PIV card). Each federal government relying party makes access decisions based on the ability to verify the validity of the PIV-I card and on local access policy for external organizations.

The following table provides an example of the minimum criteria needed for the issuance of either a PIV or PIV-I card.



*Photo: Pedestal-mounted card reader.
Courtesy of United States Marshals Service (USMS).*

Table 1: Minimum PIV versus PIV-I Example

ASSURANCE	PIV	PIV-I
IDENTITY PROOFING		
In-person identity proofing	●	●
Two I-9 forms	●	●
At least one (1) federal or state government photo ID	●	●
Signed declaration of identity	●	●
Signed declaration by local registration authority	●	●
Biometric check enrollee is same as cardholder	●	●
SUITABILITY		
FBI criminal history (fingerprint) check	●	
TIER 1 (formerly National Agency Check with written Inquiries (NACI)) initiated	●	

4.3.3 Non-PIV Cardholders

Non-PIV cardholders are individuals who do **not** meet the criteria for PIV or PIV-I card issuance. For example:

- Within DoD and DoS, family members and other eligible beneficiaries;
- Occasional visitors to federal facilities to whom temporary ID would be issued; and
- Personnel under contract to a department or agency who require only intermittent access to federally controlled facilities.

Additional types of acceptable forms of identification for non-PIV cardholders can be found in Appendix B of this document.

4.4 REAL ID

The REAL ID Act of 2005 (hereafter "REAL ID Act") sets security standards for the issuance and production of state-issued driver's licenses and ID cards to enable federal departments and agencies to accept those documents for official purposes (including accessing federal facilities, entering nuclear power plants, and boarding federally regulated commercial aircraft.) For the latest regulatory information on federal implementation, refer to [6 CFR 37.5](#).

As there is no legal requirement to produce identification, REAL ID Act compliant or otherwise, to enter a federal facility, facility policies may allow visitors access for any purpose without producing an ID if consistent with the security posture of the facility. Such purposes may include but are not limited to:

- Health-preserving or life-preserving services;
- Law enforcement;
- Participation in constitutionally protected activities;
- Voting or registering to vote; and
- Applying for or receiving federal benefits.

Other than requirements related to the acceptance of state-issued licenses and ID cards for the purposes laid out in the REAL ID Act, the act does **not** require a facility to change its access control policies. There may be instances where an individual is unable to present acceptable ID at a facility requiring ID for access purposes (e.g., the individual either does not have any form of ID or can only produce a non-compliant state-issued license or identification). In such cases, a facility may need to develop alternate procedures to facilitate access for those who require access to the facility.



Photo: Facility with "Vote Here" sign.

4.4.1 Alternate Access Control Options

If an agency requires identity verification for entry, alternate access control procedures may include, but are not limited to, the following (subject to adoption by the implementing federal agency or responsible authority):

- The agency may choose to establish a list of identification documents that it will accept for access control purposes, including state-issued driver's licenses or identification cards. (See [Appendix B](#).)
- The visitor may be listed in an appointment book so that the guard can call the agency point of contact for access and escort without having to present identification.
- The agency may use a form of knowledge-based authentication, where available.

See [Appendix C](#) for a flow chart to apply these policies.

4.5 Suspension, Removal, and Revocation

Suspension, removal, and revocation of a PIV card can happen for several reasons, including a lost or stolen card. Departments and agencies should follow their specific process for removing access. Immediately upon notification of an employee's suspension or removal, the security office should be informed so that the system can be appropriately updated. Consult with your agency's identity management office and human resources office for assistance.

For those facilities that do **not** use electronic devices for access control, consider developing a "Do Not Admit" roster or similar exclusion list to inform security staff about personnel who are restricted from accessing the facility.

4.6 Foreign Access Management

Foreign access management (FAM) is the management of risks, threats, and accompanying protective measures focused on mission-critical engagement with foreign representatives or foreign counterparts. Generally, a foreign national considered for access to a federal facility is screened in a variety of ways, depending on the agency and its available resources.

A successful FAM methodology requires a coalition of security and intelligence resources, as well as cooperation with United States government (USG) policy and international affairs activities. The correlation and analysis of foreign visits, foreign contacts, foreign travel, foreign disclosure, foreign

access-affected operations, IT network activities, and foreign-related security incidents are key to mitigating the risks posed by foreign access, as well as for identifying potential patterns and anomalies.

Appendix A of this document provides additional information about FAM methodologies.

5.0 Screening

Security screening is an electronic, visual, or manual inspection of persons, vehicles, packages, or containers. The purpose of security screening is to detect the possession or attempted introduction of illegal, prohibited, or other dangerous items carried into a federally occupied space.

Security screening should be accomplished using non-intrusive electronic methods such as X-ray machines and magnetometers (sometimes referred to as metal detectors), but may also include hand searches, visual searches, chemical swabs, or other means.

Exceptions to screening may be implemented in accordance with ISC standards to accommodate law enforcement officials, dignitaries, heads of state, and other individuals. Such exceptions should be determined by the department or agency and communicated to the facility tenant(s) or security organization, including the FSC. These exceptions should be approved in writing, coordinated with the security organization, and available to screening personnel.

Screening personnel must adhere to established procedures for initial and follow-up screenings. Personnel should also receive training on how to conduct screenings and the operation of any technology used. This training should be documented, reviewed, and tested (both overtly and covertly) on a regular basis. It is recommended that training programs use hands-on and scenario-based training. It is also recommended that the security organization develop a training program in conjunction with the manufacturers of the equipment used. This training program should include guidance on integrating the equipment into the overall screening process in addition to machine-specific operation instructions.

5.1 Security Screening Station

The security screening station is a space consisting of an arrangement of multiple security posts and equipment to provide an integrated security process at a specific location. Each piece of security technology requires a physical operator to interpret the response. Typically, a security checkpoint will consist of two primary systems, an X-ray machine and a magnetometer. Magnetometers should be programmed to sufficiently detect firearms and dangerous weapons as defined in *Items Prohibited in Federal Facilities: An Interagency Security Committee Standard*.

Screening equipment should be functionally tested (preferably daily) and calibrated according to manufacturer's specifications. The testing and calibration should be documented for each piece of equipment.



Photo: Guards at security screening station. Courtesy of Administrative Office of the United States Courts (AOUSC).

5.2 Random Security Screening

Full-time random security screening is the most resource-intensive screening policy, but also the most effective. The tenant agency or FSC, in consultation with the security organization, determines the appropriate screening procedures based on their risk assessment. Depending on the personnel and screening equipment resources available, the tenant or FSC should consider developing and implementing random security screening procedures on all occupants entering federally occupied space.

Random security screening also ensures compliance with Title 41 Code of Federal Regulations (C.F.R.) § 102-74 and Title 18 U.S.C. § 930, which prohibits weapons, explosives, and other dangerous items and protects against any form of discrimination. The tenant agency or FSC is ultimately responsible for determining what is allowable (within applicable laws and regulations) and which procedures are implemented regarding prohibited and controlled items. Additional and specific prohibitions can be found in *Items Prohibited from Federal Facilities: An ISC Standard*.



Photo: Items viewed through X-ray machine.
Courtesy of USMS.



Photo: Entrance with rope barricade.

Organizations or facilities with limited resources or personnel to conduct random security screenings may wish to consider partial-day or periodic options. The facility should ensure all perimeter entry points are or can be secured to prevent individuals from accessing the facility without passing through the screening or approved entry areas. This is a factor to consider if an organization or facility is transitioning to implementation of random security screening. If the organization or facility does **not** implement random security screenings, then usable entry points need to be secured to ensure individuals are directed only through the screening areas. This could be as simple as locking exterior access to certain doors through the agency's PACS or posting security personnel if there are open areas (such as loading docks) through which individuals could circumvent the screening stations.

5.2.1 Methodology

Randomly selected individuals are screened in order to maximize the effectiveness of screening and mask any patterns from observers. The following variables can be randomized:

- The interval between selected individuals;
- Alternate entrance locations;
- Time allotted before changing interval; and
- Continuous or paused counting.

The interval between selected individuals is the primary randomizing factor. This interval should be bounded by reasonable expectations of individual throughput into the facility. Peak times will generally be between 6:00 a.m. and 9:30 a.m. for the day.

Continuous or reset counting refers to how the screener tracks incoming individuals. With continuous counting, the screening team continues to track incoming individuals at the stated interval. With paused counting, the screening team conducts screening on the selected individuals but does **not** track other incoming individuals until screening is complete, at which point the interval counter resets to one. The advantage of continuous counting is that more individuals will be screened; however, the interval may be discernable by an observer. With paused counting, more individuals may enter the building unscreened; however, the random interval may be more difficult to determine and there is less chance of queuing at the screening station, leading to delayed throughput.

The methodology and associated software tools, training, and personnel requirements employed at a given facility may be unique but should be defensible and reproducible. Various methods can be used to determine the unpredictability; these include online resources called randomizers that aid in making random selections (e.g., coin flip, dice toss). Any method that removes premeditated or deliberate results is acceptable. Once all factors have been determined, the information should be documented.

For agencies that do not have the resources to conduct full-time random screenings, an additional set of variables can be used to help maximize randomness. These additional variables include:

- The random interval, in days, between screening sessions; or
- The random length, in hours, of a screening session.

An important aspect of the randomization process is to ensure limited access to the randomized variable prior to and during screening. As random security screening events are completed, the organization or facility should maintain a log (by name only) in case of audit or complaint. If the organization or facility tracks the actual interval numbers over time, access to these numbers should be limited to the security team only, as the numerical data can identify the upper and lower bounds of the randomization method.

The methodology should correlate to the population of the facility. For example, a low number may not be appropriate for a population over 1,000; a high number, given the anticipated throughput, may not be appropriate for a population under 1,000. The interval can affect the throughput at screening locations. As a result, additional security personnel may be required to avoid potential slowdowns due to processing individuals not selected for screening.



Photo (above): Coin (heads or tails).

Photo (below): Dice roll.



The following is an example of a monthly chart to document and track the factors. The variables listed in the chart (interval, area, frequency, and duration) can and should be adjusted to meet the specific needs of the facility.

Figure 1: Example of a Random Screening Chart

Date	Interval	Security Screening Location	Frequency	Duration
1 Jan	5	Post 1	Daily	1 hour
2 Jan	15	Post 3	Every 3 hours	1 hour
3 Jan	8	Posts 2 and 5	0630-1830	12 hours

5.2.2 Implementation

The screening personnel will track incoming individuals according to the randomized variables for that random screening session (e.g., interval between employees, continuous versus paused counting). When the count interval is reached, the individual selected for periodic screening must pass through the security checkpoint. The FSC or tenant agency should develop a policy to address individuals² refusing to adhere to screening. If an individual is unwilling, upon the request of security personnel, to comply with the screening process, the individual may be denied access to the federal facility in accordance with the facility security plan, post orders, or applicable regulations.³ The appropriate stakeholders will be notified of the denial.

For organizations or facilities transitioning to random screening, a comprehensive approval and communication plan should also be established to ensure that employees who undergo random screening understand the process and are prepared to participate. The approval decision and communications plan should include:

- Outreach to senior leadership;
- Coordination with union officials;
- Agency newsletter articles and posters;
- In-person information sessions or town halls; and
- Well-publicized initial screening sessions to help acclimate individuals before transitioning to random screening.

6.0 Escort Procedures

When organizations or facilities determine that visitors require accompaniment by an authorized person (escort) while within federally occupied space, they should develop local security policies and procedures that account for individual operational requirements and agency culture. Visitors needing an escort are processed following the local security policies and procedures prior to being granted access to the facility.

² “[Persons] or belongings passing through the magnetometer or X-ray.”

³ 41 C.F.R. § 102-74 C (Inspection) and 18 U.S.C. § 930.



Photo: Visitor badge on lanyard.

The visit sponsor, their designee, or the dedicated agency escort is responsible for escorting the individual while within federally occupied space.

Escort procedures and ratios should be appropriate to the type of individual and associated risk. Personnel escorting visitors must maintain a visual line of sight, physical proximity, or other means of control of the visitor. The ratio of visitors to escorts shall be established by the FSC or tenant agency in consultation with the security organization based on operational requirements.

The following chart identifies three levels to aid in determining the appropriate escort level.

Table 2: Escort Levels

Level I	<p>Minimal Escorting Practice: Authorized Personnel.</p> <p><i>Examples:</i></p> <ul style="list-style-type: none"> • New hire who has not yet received swipe access to their work area. • Visiting federal agency-cleared personnel who do not have swipe access to your facility.
Level II	<p>High Positive Escorting Practice: Continuous.</p> <p><i>Escorts must ensure that the escorted individual is continuously accompanied or monitored:</i></p> <ul style="list-style-type: none"> • While performing work (after passing through security screening); and • After retrieving items from a vehicle.
Level III	<p>High Risk Escorting Practice.</p> <p><i>Escorts must ensure that the individual is continuously accompanied or monitored.</i></p> <ul style="list-style-type: none"> • Escorts are required to be within a distance not to exceed 10 feet and must be under continuous visual and verbal control. • Escorts are to be briefed prior to escorting and debriefed after escorting.

7.0 Physical Access Control Systems

At a high level, a PACS is a collection of technologies that enforces local access policies for physical access at federally occupied spaces by electronically authenticating identity credentials presented to a PACS card reader by individuals who are requesting access to agency areas. PACS ownership and control varies among facilities depending on lease agreements and individual agency operational postures and policies. Typically, the PACS controlling physical access to the facilities, campus, or shared common areas (e.g., stairwells, elevators) is provided by either the lessor or the federal agency in ownership of the facility. PIV access to suite space internal to a multi-tenant facility is controlled by the individual tenant agency in most instances.

The legacy and most common form of these internal PACS is a standalone deployment (e.g., **not** connected to an agency network or enterprise system). Modernized PACS, by comparison, is agency managed and part of the occupying organization's enterprise networked solution. Less commonly, the building PACS provider (federal or contractor) may offer tenants the option of using PACS services hosted from the building's PACS infrastructure.

In alignment with OMB M-19-17 and ICAM policy, specifically addressing managing identities, credentials, and access in modern government, Executive Branch departments and agencies must implement PACS solutions capable of performing one or more PIV authentication mechanisms. FIPS 201-2 and NIST SP 800-63 Digital Identity Guidelines define characteristics of the interoperable identity credential that can be used government-wide.

To meet this standard, organizations must determine the level of interoperability that will be afforded to PIV cards issued by other agencies. At a minimum, all organizations will ensure that PACS operate on the same current FIPS 201 technology standard. Decisions regarding how individuals and agency partners with PIV cards will be processed are at the determination of the organization's Senior Official(s) responsible for physical security and the Chief Information Officer (CIO) based on assessment of risk.

Access to federally occupied spaces will be managed by installing compliant PACS in accordance with OMB policies M-05-24 and M-19-17, NIST SP 800-116, and all other applicable standards established by OMB, NIST, and the CIO Council.

The facility, in consultation with the property management group, determines implementation actions related to the facility PACS services and countermeasures which support shared facility space. Typically, in multi-tenant facilities the FSC is not involved in PACS decisions for internal individual tenant space unless those decisions impact the overall facility or additional tenants. The FSC or tenant agency representative also needs to be aware of other guidance documents, authorities, and responsibilities that exist when exercising that role.

7.1 PIV Assurance Level

In executing the protection strategy and selecting both a baseline and risk-based access control posture for facility PACS administration, organizations will use the most current FIPS 201 assurance levels. The current version of FIPS 201 defines authentication mechanisms at four assurance levels: (1) LITTLE or NO; (2) SOME; (3) HIGH; and (4) VERY HIGH.

These levels provide a risk-based approach as directed in Homeland Security Presidential Directive (HSPD)-12 to "include graduated criteria, from least secure to most secure, to ensure flexibility in selecting



*Photo: PACS equipment room.
Courtesy of AOUSC.*

the appropriate level of security for each application.” The organization must determine the levels of assurance necessary for each critical area (e.g., perimeter, doors). Methods include the FSL, levels of secure area as defined in NIST SP 800-116, or agency-specific security levels. The key is to have a consistent (reproducible) and logical (defensible) methodology to determine the level of assurance needed throughout the facility.

The current revision of NIST SP 800-116 provides the concept of “Controlled, Limited, Exclusion” areas to govern the development of a security strategy for incorporating HSPD-12 into planning layers of access assurance within a facility.

- Access to **Controlled** areas (restricted areas near or surrounding a Limited or Exclusion area) is least restrictive.
- Access to **Limited** areas is often based on functional subgroups or roles.
- Access to **Exclusion** areas may be gained by individual authorization only.



Photo: Fingerprint scan.

Initial authentication of an individual’s identity, bound to a token or card through an approved common vetting process and credential issuance, establishes inclusion in a specified access group. Federal government facilities can be identified and categorized in these areas and correspond generally to LOW (for Controlled), MODERATE (for Limited), and HIGH (for Exclusion) impact to assets or resources. Authentication factors commensurate with risk factors for each area should align as one factor for Controlled, two for Limited, and three for Exclusion areas.

8.0 FSL and PACS Considerations

The initial FSL determination for newly leased or owned space will be made as soon as practical after the identification of a space requirement, including succeeding leases. As defined in the *Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (hereafter “the RMP”), the FSL determination ranges from Level I (lowest risk) to Level V (highest risk). The determination should be made early enough in the space acquisition process to allow for the implementation of required countermeasures or a reconsideration of the acquisition due to an inability to meet minimum physical security requirements.

As organizations and facilities determine how to implement physical access control, they should keep in mind the following considerations:

- All electronic PACS must be in accordance with the most current version of FIPS 201.
- All electronic PACS must comply with national-level ICAM requirements established by FIPS 201 and OMB guidance (e.g., OMB M-05-24, OMB M-19-17). This includes selection of systems in new construction or modernization projects, determination of authentication mechanisms aligned with facility risk, ensuring compliance with the current version of FIPS 201 Evaluation Program Approved Products List, and ensuring that the system configuration aligns with ICAM guidance.

Organizations and facilities develop plans and budgets to modernize legacy building PACS to ICAM standards as resources allow. Visual PIV checks, lessor-provided building access cards, and non-authenticating card readers are examples of legacy FAC methods requiring modernization.

Since fiscal year 2012, the Federal Acquisitions Regulation (FAR) 48 C.F.R. Subpart 4.13 has required that all modified or newly acquired electronic PACS systems must meet ICAM requirements (e.g., ICAM, NIST standards, OMB policies and supporting technical specifications) and appear on the GSA Approved Product List (APL). As defined by OMB Circular A-130, electronic PACS are information technology (IT) systems and must comply with ICAM requirements. The APL provides federal agencies with products and services that have been approved for ICAM implementation based on rigorous security vulnerability and interoperability testing performed by the FIPS 201 Evaluation Program. As IT systems, PACS are assessed under NIST approved procedures and appropriate security controls are considered as part of the Risk Management Framework (RMF) process.

NIST SP 800-116 outlines options for different levels of authentication as they relate to FSLs and Limited, Controlled, and Exclusion areas. Although there is no simple one-to-one mapping between FSL and the authentication mechanism(s), the FSL indicates the estimate of the level of risk to the facility.



*Photo: PACS equipment room.
Courtesy of AOUSC.*

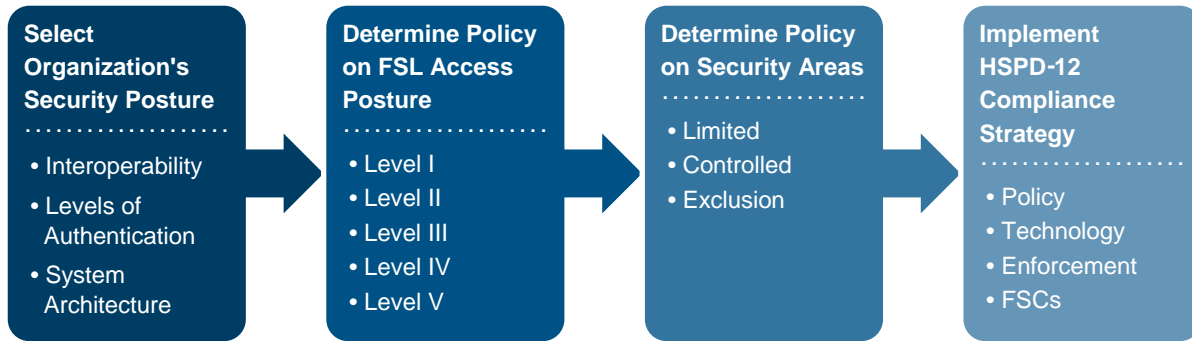
8.1 Perimeter Considerations

Based on the risk, an agency should identify and categorize PACS perimeters as protecting Controlled, Limited, or Exclusion areas. The following steps demonstrate an example process for identifying and categorizing perimeters.

1. Select the organization's baseline HSPD-12 access policy.
2. Determine the policy based on FSL access requirement (e.g., Levels I-V).
3. Determine the policy based on Controlled, Limited, and Exclusion areas.
4. Implement HSPD-12 strategy through policy issuance and enforcement.

The following diagram illustrates this process.

Figure 2: PACS Strategy Process Flow



Organizations and facilities may protect entry to the federally occupied site or campus perimeter by alignment with FSL, the necessary level of protection (LOP), or another risk-based approach. An example method with authentication measures is outlined in the following table. Authentication mechanisms include: Public Key Infrastructure (PKI); Card Authentication Key (CAK); and PIV Authentication Key (PAK).

Table 3: Aligning Perimeter Authentication Mechanisms with FSL

FSL Determination	Authentication Factors Required	Authentication Mechanism	Interface
I	1	PKI-CAK	Contactless
II	1	PKI-CAK	Contactless
III	1	PKI-CAK	Contactless
IV	2	PKI-PAK + PIN	Contact
V	3	PKI-PAK + PIN + BIOMETRIC	Contact

8.2 Internal Agency Space Considerations

The FSL or LOP criteria are generally not as helpful to internal areas in multi-tenant facilities where individual agency leased spaces are protected by agency-owned or agency-operated PACS. Shared or common space internal to the facility will follow NIST SP 800-116 guidelines for protection. NIST SP 800-116 recommends applying the IT system FIPS 199 Loss Impact Assessment Methodology to physical space for the purpose of determining authentication mechanisms.

The following table provides an example of how authentication mechanisms are determined for internal space using the RMF or FIPS 199 methodology.

Table 4: Authentication for Internal Agency Space

FIPS-199 Assessed Impact of Breach	Determination	Authentication Factors Required	Authentication Mechanism	Interface
Low	Controlled	1	PKI-CAK	Contactless
Moderate	Limited	2	PKI-PAK + PIN	Contact
High	Exclusion	3	PKI-PAK + PIN BIOMETRIC	Contact

Appendix A: Foreign Access Management

Building relationships and sharing information with our foreign allies and associates is a critical component in the USG mission to execute key functions across a broad spectrum of programs. This mission-essential engagement offers adversarial foreign entities (security, intelligence, terrorist, and criminal) the opportunity to collect information through close and continued access to USG information, people systems, facilities, and resources.

Simply stated, FAM is the correlation of all foreign access activities affecting a federal facility. There are many types of FAM-related activities, such as foreign visits, foreign travel, foreign contact, and foreign disclosure. Many of these activities go unreported between agencies. More importantly, these activities are not always correlated within agencies as a method of pinpointing the true risks of foreign access. The following image depicts some of the many ways that foreign access activities can be overlooked or go uncorrelated.

Figure 3: Methods of Foreign Access



FAM methodology provides the operational context through which the security elements of facilities hosting foreign nationals can conduct a full-scope risk assessment and more effectively guide the vetting process. FAM is broken into two parts:

- Short-term visitors (as defined by department or agency); and
- More permanent, vetted relationships of contractors, exchange partners, researchers, and employees.

The security organization is responsible for controlling access to the facility. The level of restriction is based on the function of the facility and agency. For example: a visitor's center would have no restrictions and might employ foreign translators as a function of the activity; a data processing facility might be so restrictive as to limit entry to United States citizens only.

While vetting foreign visitors, it is important to create a record and use the information to mitigate risk to the facility, the agency, and the USG. Improving the accessibility of this collected information should be a critical concern. Questions that need to be considered include:

- Why is this foreign national requesting access to visit this facility?
- What benefit does the USG achieve by hosting this visit?
- What risk is the sponsor assuming?
- What logistical and administrative burden is this visit placing on the facility?

To truly understand the impact of—and to fully vet—a foreign visit to a federal facility, hosting agencies must consider the foreign visit as an indicator of a process that began long before the visit was announced. That process, which entails foreign contact, exchange of information, and in many cases foreign travel by the host to the country of the visiting foreign official, has already exposed the hosting agency to a variety of risks and has offered security elements of the hosting facility the backdrop through which it could truly assess the risks of the foreign visit to their facility, programs, personnel, information, and systems.

Foreign national access to federal facilities entails close coordination between the security element and the organization's operational security, information security, foreign disclosure, international affairs, and counterintelligence offices. While many agencies may not possess the capabilities at present, security elements should seek to capture foreign contact, foreign travel, foreign disclosure, network anomalies, inbound and outbound email to and from foreign sources, and historical foreign visit reporting in order to best assess the risks to the hosting organization.

Approved visits to federal facilities by foreign nationals must be based on an assessment of risk and planned in accordance with the guidance of the organization's senior security or intelligence officials. A critical factor in a successful FAM program is the use of a case management system (CMS) where, at a minimum, foreign visits, foreign contacts, and foreign travel information can be stored. The CMS should offer remote user access for vetting requests, customer service status notifications, and trend reporting capabilities. This partnership, operational and through policy, is critical to successful determination and mitigation of risk.



FAM is the correlation of all foreign access activities affecting a federal facility.

A.1 Foreign National Vetting

The goal of foreign national vetting is an understanding of the individual's background, their history of contact with the hosting organization, and their total footprint in the United States. To that end, screening programs require access to and information from domestic, foreign, and defense USG systems. An effective screening program will be able to:

- Collect and maintain all identifying foreign national information;
- Collect and maintain contact information for associated employees;
- Determine the history and nature of access to federal facilities and personnel;
- Validate the identity of the individual;
- Access and receive classified resources; and
- Implement policies and procedures.

The primary focus of the FAM vetting process is to determine the risks associated with granting a foreign national access to the organization's facility, personnel, programs, information, and systems. By leveraging all necessary resources, hosting organizations can better determine whether the individual:

- Is using a fraudulent identity or credentials;
- Is not legally permitted to enter or otherwise conduct business within the United States;
- Has outstanding warrants;
- Is or has been involved in activities or associated with persons or organizations whose aim is to weaken or damage United States national security, economy, competitiveness, or strategic markets;
- Is or has been involved in activities or associated with persons or organizations whose aim is to overthrow the USG or alter the form of government by force, violence, or other unconstitutional means;
- Has an association with terrorism, organized crime, narcotics, or human trafficking; or
- Has a history of conduct of such a nature that official association could prove damaging to the reputation or mission of the USG or its representatives.

Since foreign national employees and contractors may not have lived in the United States long enough for a Tier 1 investigation to be meaningful, agencies should conduct an equivalent investigation consistent with existing policy. Agencies should investigate and provide an alternative form of ID. A single identity-proofing and registration process is defined in the most current version of FIPS 201 for government employees and contractors, which includes successful completion and adjudication of the Tier 1.

Exceptions to foreign visitor screening may be implemented to accommodate high-profile government officials (e.g., President, Agency Head) and other such individuals as determined by the department or agency and communicated to the facility, including the FSC in multi-tenant facilities. These exceptions should be approved in writing, coordinated with the security organization, and available to the screening personnel.

Appendix B: List of Acceptable Forms of Identification

Each agency may determine which identification documents it will accept for the purpose of accessing its facilities based on the facility's risk profile. The Act only affects acceptance of state-issued documents as part of access control policies where individuals are required to present an identification document for official purposes.

The ISC recommends that agencies accept a federal or foreign government-issued passport containing a photograph, first and last name, expiration date, and any additional elements the agency uses in its verification processes. The ISC does not recommend accepting a document if it has visible signs of tampering. The ISC recommends that preference be given to documents that have not expired, particularly for facilities at greater risk, such as facilities designated at FSL 3 or greater.

In the interest of promoting consistent policies across the federal government, the ISC provides the following list of possible forms of identification to assist agencies in setting their facility's access control policies. This list is neither authoritative nor exhaustive.

1. Federally Issued Identification

- US Passport
- US Passport Card
- PIV or federally issued Personal Identification Verification – Interoperable (PIV-I) Card
- Driver's License issued by the US Department of State
- Border Crossing Card (Form DSP-150)
- DHS "Trusted Traveler" Card (Global Entry, NEXUS, SENTRI, FAST)
- US Military ID (All members of the US Armed Forces, including retirees and dependent ID card holders, and veterans. Visit the DoD's Common Access Card website for more information: <https://www.cac.mil>)
- Veteran Health Identification Card issued by the US Department of Veterans Affairs
- US Permanent Resident Card (Form I-551)
- US Certificate of Naturalization or Certificate of Citizenship (Form N-550)
- Employment Authorization Document issued by DHS (Form I-766)
- US Refugee Travel Document or other travel document or evidence of immigration status issued by DHS and containing a photograph (Permit to Reenter Form I-327 and Refugee Travel Document Form I-571)
- Transportation Worker Identification Credential (TWIC)
- Merchant Mariner Card issued by DHS/US Coast Guard (USCG)

2. State-Issued Identification

For additional enforcement information, visit [Real ID Homeland Security](#) website.

- A REAL ID-compliant driver's license or identification card issued by the state may be accepted.
- Enhanced Driver's License (EDL): <https://www.dhs.gov/enhanced-drivers-licenses-what-are-they>
- State prisoner identification card

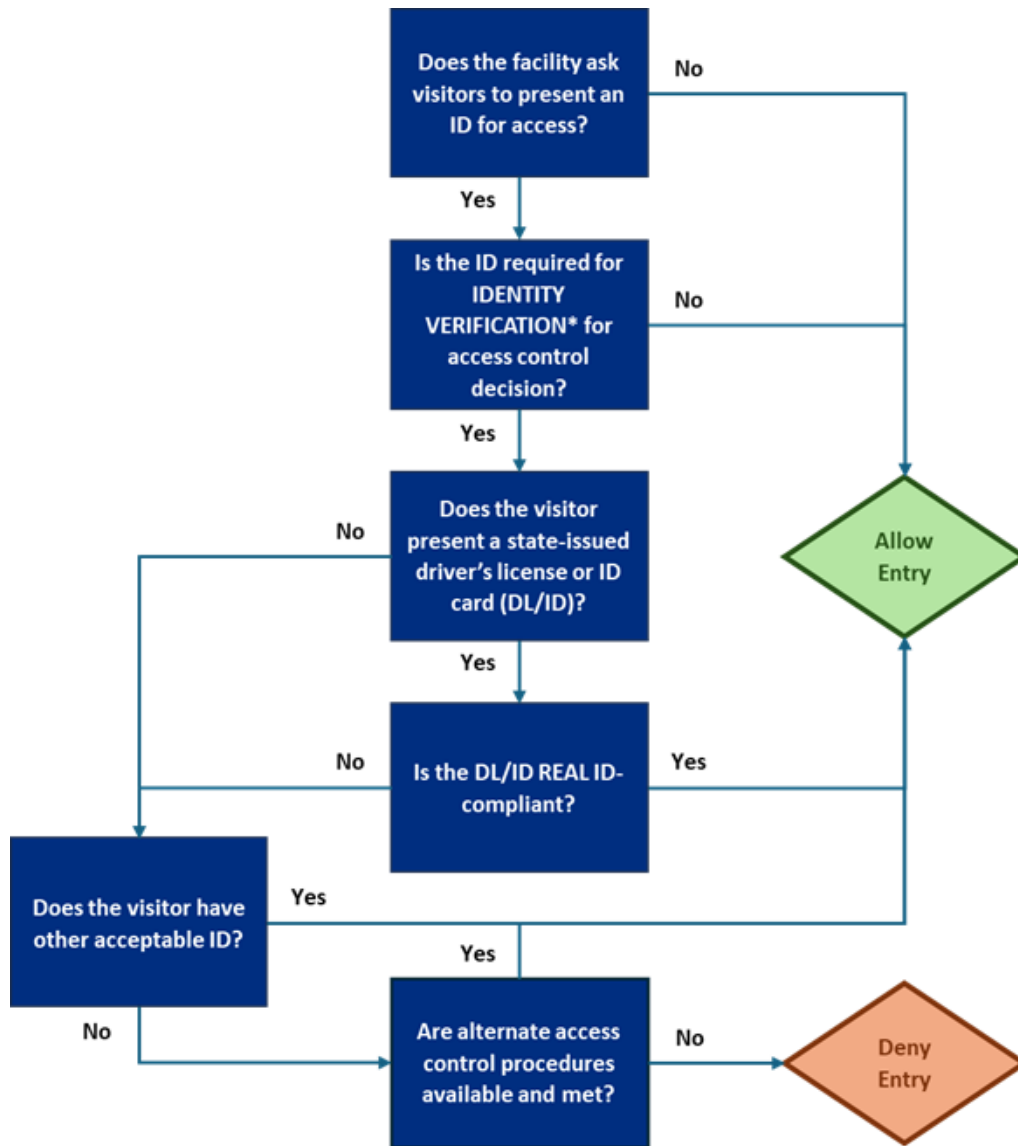
3. Other

- Federally Registered Native American Tribal Photo ID
- Foreign government-issued passport
- PIV-I card issued by non-federal government entities

Facilities may also consider the following higher-risk identity documents, which may be appropriate for facilities with a low risk profile or that have a relationship with the issuing body that mitigates the risk of fraud.

- Identification card issued by local government (including county or city) and containing a photograph, name, and expiration date
- University, library, or school card containing a photograph, name, and expiration date
- Any identification that is not state issued, but is deemed acceptable by the FSC or DO

Appendix C: Flow Chart for Access Control



*REAL ID Requirements only apply when an individual's identity needs to be confirmed or verified for access control purposes (for example, to match the individual's identity to pre-vetted list of expected visitors).

Appendix D: Resources

Glossary

Access Control: The use of physical and procedural controls to ensure only authorized individuals are given access to a facility or secure area.

Controlled Area: A portion of a restricted area, usually near or surrounding a Limited or Exclusion area. Entry to the Controlled area is restricted to personnel with a need for access.

Exclusion Area: A restricted area containing a security interest.

Facility Security Committee (FSC): The committee responsible for addressing facility-specific security issues and approving the implementation of security measures and practices.

Facility Security Level (FSL): A categorization based on the analysis of several security-related factors that serves as the basis for the implementation of physical security measures specified in ISC standards and policies.

Federal Facility: Government leased and owned facilities in the United States (inclusive of its territories) occupied by federal employees for nonmilitary activities.

Foreign Access: A potentially exploitable proximity to or ability by foreign nationals to access information, personnel, systems, technologies, facilities, resources, and programs that expose an organization to loss or compromise.

Foreign Access Management (FAM): The management of risks, threats, and accompanying protective measures focused on mission-critical engagement with foreign representatives or counterparts.

Foreign Engagement: Activities involved in coordination, collaboration, and exchanges between the USG and foreign nationals and foreign entities. This includes meetings on and off USG property, access to USG information, and other actions necessary to carry out the USG mission.

Foreign Individual: A person who is not a naturalized citizen of the country in which they are living or visiting.

Foreign National: A person who is not a citizen or national of the United States.

Identity-based Access Control: Policies and practices requiring the presentation, inspection, and acceptance of an individual's photo ID for access to a federal facility.

Knowledge-based Authentication: A method of authentication that seeks to prove the identity of someone using the knowledge of personal information associated with the asserted identity. This may involve the use of information sent to the individual in advance as part of the access control process or use answers to questions generated from a wider base of personal information (e.g., previous addresses) to which the agency has access.

Occupant: Any person who is permanently or regularly assigned to the federal facility and displays the required identification badge or pass for access, with the exception of those individuals providing a service at the facility (e.g., guards, custodians).

State-issued Identification Card: A driver's license or non-driver identification card issued by a Department of Motor Vehicles or equivalent office in a state, the District of Columbia, or a territory of the United States. This does not include identification cards issued by other state agencies, such as an employee ID, hunting license, library card, or student ID.

List of Abbreviations, Acronyms, and Initializations

Term	Definition
APL	Approved Product List
CAK	Card Authentication Key
C.F.R.	Code of Federal Regulations
CIO	Chief Information Officer
CMS	Case Management System
DHS	Department of Homeland Security
DoD	Department of Defense
DoS	Department of State
EO	Executive Order
FAC	Facility Access Control
FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standards
FSC	Facility Security Committee
FSL	Facility Security Level
GAO	Government Accountability Office
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
ICAM	Identity, Credential, and Access Management
ID	Identification Document
ISC	Interagency Security Committee
IT	Information Technology
LOP	Level of Protection
NIST	National Institute of Standards and Technology
OEP	Occupant Emergency Plan
OMB	Office of Management and Budget
PACS	Physical Access Control Systems
PAK	PIV Authentication Key
PIV	Personal Identity Verification
PIV-I	PIV-Interoperable
PKI	Public Key Infrastructure
RMF	Risk Management Framework
RMP	Risk Management Process
TSA	Transportation Security Administration
USC	United States Code
USG	United States Government
USMS	U.S. Marshals Service
USPS	United States Postal Service

References: General

This section contains a non-exhaustive list of guidance documents for facility access control.

Federal Policies, Standards, and Regulations

41 C.F.R. § 102-74 (2020). "Facility Management." Accessed June 17, 2020. https://ecfr.io/Title-41/pt41.3.102_674

41 C.F.R. § 102-74, Appendix (2020). "Rules and Regulations Governing Conduct on Federal Property." Accessed June 17, 2020. https://ecfr.io/Title-41/pt41.3.102_674#ap41.3.102_674_1600.1

Crimes and Criminal Procedure, 18 U.S.C. § 930 (2020). Accessed June 17, 2020. [https://uscode.house.gov/view.xhtml?req=\(title:18%20section:930%20edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:18%20section:930%20edition:prelim))

U.S. Department of Homeland Security. Cybersecurity and Infrastructure Security Agency. Interagency Security Committee. *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*. Accessed June 17, 2020. <https://www.cisa.gov/publication/isc-risk-management-process>

Executive Office of the President. E.O. 12977 (1995). "Interagency Security Committee." Accessed June 17, 2020. <https://www.federalregister.gov/documents/1995/10/24/95-26497/interagency-security-committee>

Executive Office of the President. Office of Management and Budget. Memorandum M-05-24 (2005). "Enabling Mission Delivery through Improved Identity, Credential, and Access Management." Access June 17, 2020. <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2005/m05-24.pdf>

Executive Office of the President. Office of Management and Budget. Memorandum M-19-17 (2019). "Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors." Access June 17, 2020. <https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf>

Government Organization and Employees, 5 U.S.C. § 101 (2020). Accessed June 17, 2020. [https://uscode.house.gov/view.xhtml?req=\(title:5a%20section:101%20edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:5a%20section:101%20edition:prelim))

Government Organization and Employees, 5 U.S.C. § 103 (2020). Accessed June 17, 2020. [https://uscode.house.gov/view.xhtml?req=\(title:5a%20section:103%20edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:5a%20section:103%20edition:prelim))

Government Organization and Employees, 5 U.S.C. § 104 (2020). Accessed June 17, 2020. [https://uscode.house.gov/view.xhtml?req=\(title:5a%20section:104%20edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:5a%20section:104%20edition:prelim))

Government Organization and Employees, 5 U.S.C. § 2105 (2020). Accessed June 17, 2020. [https://uscode.house.gov/view.xhtml?req=\(title:5%20section:2105%20edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:5%20section:2105%20edition:prelim))

National Institute of Standards and Technology. Federal Information Processing Standards 201-2 (2013). "Personal Identity Verification (PIV) of Federal Employees and Contractors." Accessed June 17, 2020. <https://csrc.nist.gov/publications/detail/fips/201/2/final>

National Institute of Standards and Technology. Special Publication 800-63, Revision 3 (2017). *Digital Identity Guidelines*. Access June 17, 2020. <https://pages.nist.gov/800-63-3/sp800-63-3.html>

National Institute of Standards and Technology. Special Publication 800-116, Revision 1 (2018). *Guidelines for the Use of PIV Credentials in Facility Access*. Access June 17, 2020. <https://csrc.nist.gov/publications/detail/sp/800-116/rev-1/final>

Postal Service, 39 U.S.C. § 201 (2020). Accessed June 17, 2020. [https://uscode.house.gov/view.xhtml?req=\(title:39%20section:201%20edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:39%20section:201%20edition:prelim))

REAL ID Act, Title II, H.R. 1268, 109th Cong. (2005) (enacted). Accessed June 17, 2020. <https://www.dhs.gov/xlibrary/assets/real-id-act-text.pdf>

Federal Publications

Executive Office of the President. Office of Management and Budget. Circular No. A-130. "Managing Information as a Strategic Resource." Access June 17, 2020. <https://www.cio.gov/policies-and-priorities/circular-a-130/>

Department of Homeland Security. "REAL ID." Accessed June 22, 2020. <https://www.dhs.gov/real-id>

General Services Administration. "Approved Products List." Accessed June 17, 2020. <https://www.idmanagement.gov/approved-products-list/>

Transportation Security Administration. "Security Screening: Identification." Accessed June 17, 2020. <https://www.tsa.gov/travel/security-screening/identification>

Transportation Security Administration. "Security Screening: REAL ID." Accessed June 17, 2020. <https://www.tsa.gov/real-id>

References: Foreign Access Management

While there is no federal statute or regulation that requires a FAM program, there are many federal statutes, regulations, Presidential Policy Directives, and Executive Orders that mandate the activity.

Facilities:

41 C.F.R. § 102-81.10 (2020). "Security." Accessed June 17, 2020. https://ecfr.io/Title-41/cfr102-81_main. Relevance: DHS enforces federal laws and regulations for the protection of persons and property and provides delegations of same to other agencies.

Public Buildings, Property, and Works, 40 U.S.C. § 1315 (2020). Accessed June 17, 2020. [https://uscode.house.gov/view.xhtml?req=\(title:40%20section:1315%20edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:40%20section:1315%20edition:prelim)). Relevance: Agencies must provide for the security and protection of the real estate they occupy, including the protection of persons within the property.

Information and Technology:

15 C.F.R. § 730 (2020). "Commerce and Foreign Trade." Accessed June 17, 2020. <https://ecfr.io/Title-15/pt15.2.730>. Relevance: Bureau of Industry and Security's Export Administration Regulations regarding control of certain exports, reexports, and activities.

Executive Office of the President. E.O. 12958 (1995). "Classified National Security Information." Accessed June 17, 2020. <https://www.federalregister.gov/documents/1995/04/20/95-9941/classified-national-security-information>. Relevance: Classifying, safeguarding, and declassifying national security information.

Executive Office of the President. E.O. 12968 (1995). "Access to Classified Information." Accessed June 17, 2020. <https://www.federalregister.gov/documents/1995/08/07/95-19654/access-to-classified-information>. Relevance: Agency discretion to grant limited access to classified information to foreign national employees who possess a special expertise when there are compelling reasons in furtherance of an agency mission.

Executive Office of the President. E.O. 13587 (2011). "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information." Accessed June 17, 2020. <https://www.federalregister.gov/documents/2011/10/13/2011-26729/structural-reforms-to-improve-the-security-of-classified-networks-and-the-responsible-sharing-and>. Relevance: Insider Threat Task Force and agency assessments for information access.

Presidential Policy Directive 21. Critical Infrastructure Security and Resilience (2013). Accessed June 17, 2020. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>. Relevance: Strengthen and maintain secure, functioning, and resilient critical infrastructure, which includes facilities and IT.

Public Buildings, Property, and Works, 40 U.S.C. § 11315 (2020). Accessed June 17, 2020. [https://uscode.house.gov/view.xhtml?req=\(title:40%20section:11315%20edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:40%20section:11315%20edition:prelim)). Relevance: CIO is

responsible for developing, maintaining, and facilitating the implementation of a sound, secure, and integrated IT architecture for the executive agency.

Public Buildings, Property, and Works, 40 U.S.C. § 11331 (2020). Accessed June 17, 2020.

[https://uscode.house.gov/view.xhtml?req=\(title:40%20section:11331%20edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:40%20section:11331%20edition:prelim)). Relevance: OMB standards to improve the efficiency of operations or security of federal information systems. The head of an agency may employ standards for the cost-effective information security for all operations and assets within or under the supervision of that agency that are more stringent than OMB's standards.

Acknowledgements

The ISC would like to thank the participants of the FAC Working Group.

Vince Eckert, Chair
General Services Administration

Thad Bennett
Department of Homeland
Security

Jonathan Blaine
Interagency Security
Committee

Joseph Cassone
Department of Homeland
Security

Bryan Cisar
U.S. Army Corps of Engineers

Hank Clyatt
Department of Transportation

Martha Collins
Department of Labor

Christopher Davidson
Department of Health and
Human Services

Colin Doniger
Department of Homeland
Security

John Eskandary
Federal Emergency
Management Agency

Lynn Enos
Interagency Security
Committee

Josh Freedman
Department of Defense

Sarah Golden
Interagency Security
Committee

Jennifer Hammen
Department of Homeland
Security

L.A. Harding
Commodity Futures Trading
Commission

Philip Haynie
Department of Commerce

Mike Hennig
Federal Emergency
Management Agency

Jose Hernandez
Department of Homeland
Security

Fred Jackson
Department of Defense

Scott Lawrence
General Services
Administration

Shannon Miers
Federal Emergency
Management Agency

Nicholas Mikalis
Department of Homeland
Security

Richard Moreta
Department of Homeland
Security

William Morrison
Federal Aviation
Administration

Dan O'Connor
Federal Emergency
Management Agency

Pete Pierluissi
Internal Revenue Service

Wayne Rash
Federal Emergency
Management Agency

Kelvin Spinner
Commodity Futures Trading
Commission

FAC Working Group Participants, Continued

Bruce Sutphin
Federal Emergency
Management Agency

J'son Tyson
Federal Emergency
Management Agency

Mark Wilson
National Science Foundation

William Windsor
Department of Homeland
Security