

Homeland Security Presidential Directive 12 (HSPD-12) Overview

Audio: Welcome to the Homeland Security Presidential Directive 12 (HSPD-12) overview module, the first in a series of informational modules designed to familiarize you with the new common identification standard for Federal employees and contractors.

Agenda

- Introduction
- HSPD-12 Overview
 - What is personal identity verification?
 - What identity management challenges does the government face?
 - What is Homeland Security Presidential Directive 12 (HSPD-12)?
 - What is Federal Information Processing Standard 201(FIPS-201)?
 - How will HSPD-12 affect my agency?
- Conclusion

Audio: This overview module contains an introduction, five lessons, and a conclusion.

Each of the five lessons lasts about 10 minutes. The lessons address the topics shown on this page.

Introduction

Audio: In this introduction, you will learn how to navigate within this training. We will also review the goal of the module.

How Do I Use the Training?

Audio: This training has a few simple features.

The controls you will use are located at the lower right of each presentation window.

Use the pause button to pause the training. Once a page has completed playing, you can use the play button to access the next page.

Use the back and next page buttons to access each page in sequential order.

The audio control button controls audio volume or allows you to mute the audio completely.

The switch layout button toggles between the current default layout and an optional layout.

Click the play button to begin Lesson One. You will need to click this button to continue through the rest of the pages.

Goal

- Increase awareness
- Overview of HSPD-12 and FIPS-201
- How these requirements impact Federal agencies

Audio: The goal of this module is to increase your awareness of HSPD-12 and FIPS-201.

HSPD-12 is a policy that establishes a common standard for a secure and reliable form of identification for Federal employees and contractors.

FIPS-201 defines a government-wide personal identity verification (PIV) system, where common identification credentials can be created and later used to verify a claimed identity.

The module also discusses how the new requirements affect Federal agencies deploying the personal identity verification (PIV) credential.

Lesson One

What is Personal Identity Verification?

Audio: In this lesson, you will learn about Personal Identity Verification, or PIV.

Lesson One Objectives

- Define Personal Identity Verification (PIV)
- Describe smart card, biometrics, and public key infrastructure (PKI) technologies
- Distinguish authentication from authorization

Audio: Lesson One defines key concepts relevant to PIV.

The topics covered in Lesson One are as follows:

Personal identity verification
Smart cards
Biometrics
Public key infrastructure (PKI)
Authentication, and
Authorization

PIV Definition

- Requirements for ID credentials
- Foundation of trust among agencies

Audio: A PIV program defines the requirements for a secure, common, and reliable form of identification credential issued by the Federal Government to its employees and contractors.

Such a credential is fundamental to establishing trust among agencies, and to improving efficiency and security.

Why is a PIV Program important?

Why is PIV Important?

- Promotes efficiency
 - Agency ID badge requirements differ
 - Different security requirements and color codes
 - Only locally issued badge trusted
- Reduces identity fraud
- Maintains personal privacy
- Increases security

Audio: A PIV program promotes efficiency, reduces identity fraud, maintains personal privacy, and increases security.

Currently, Federal agencies differ in their identity credential, or ID badge, requirements.

Agencies have different security requirements, and color codes for identifying employee and contractor badges. Many variants exist, even

within agencies. For example, if an agency is headquartered in Washington, DC, but maintains field sites across the country, each site might have a different way of issuing their badges.

Consequently, only badges issued by an individual facility are trusted. All persons holding badges which do not conform with the local standard must sign-in. This requires extra time to access the facility, as well as extra security personnel to grant the access.

Let's learn some basic PIV concepts, starting with smart cards.

What Are Smart Cards?

- Data stored on chip:
 - Card identifying information
 - ID certificates
 - Electronic keys
 - PINs
 - Biometric information

Audio: Smart cards are plastic cards about the size of an ordinary credit card. They contain embedded computer chips that allow them to perform multiple functions. Information can be added or deleted from smart cards. The PIV credential has two chips. The first chip, the gold rectangular area, has contact areas that connect with a chip reader into which the PIV credential is inserted. The other chip, hidden inside the upper right hand area of the credential, uses a radio-like capability to communicate data.

The chip can store various forms of data that help identify the card holder and how long the credential can be used before it expires.

Data stored on the chip include: card identifying information, identity certificates, electronic keys that can be used for encryption, personal identification numbers, and biometric information. This data is used to verify a card holder's identity in order to grant access to a facility or information system.

Next, we'll discuss biometrics.

What Is Biometrics?

- Science of measuring and analyzing biological data

- Measurable physical characteristics used to recognize identity or verify claimed identity

Audio: Biometrics is the science of measuring and comparing biologically-derived data.

Biometrics are a measurable, physical characteristic used to recognize, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scans are all examples of biometric data.

Our next basic concept is public key infrastructure, or PKI.

What Is Public Key Infrastructure (PKI)?

- Set of hardware/software technologies
- Certificates signed and issued by Certificate Authorities (CAs)
- Public/private key pairs

Audio: What is Public Key Infrastructure? A PKI consists of hardware and software technologies, accompanied by formal processes, to provide services that strengthen identity assurance and the integrity of digital transactions. By issuing and managing electronic identity certificates, a PKI allows computer users to trust one another. Certificates are issued only after passport-like identity proofing is successfully completed.

Certificates are created, digitally signed and issued to individuals by accredited providers known as Certificate Authorities, or CAs. Certificates identify an individual and “bind” that person to a particular public/private key pair.

Key pairs are small strings of numbers and letters that are mathematically related. Key pairs and certificates provide the basis for strong electronic authentication.

We’ll conclude this lesson with a scenario that illustrates the distinction between two vital concepts: authentication and authorization.

Authentication

- Authentication is the determination of a person’s identity
- Physical access typically authenticated by hand-carried credentials

- Access to computers and data authenticated by passwords

Audio: Let's start by defining authentication. Authentication is the process of identifying an individual. During authentication, an individual's identity is validated and associated with some sort of credential presented by that person.

For physical access, individual identity has traditionally been authenticated by the use of hardcopy credentials, such as driver's licenses and badges.

Access to computers is typically authenticated through user-selected passwords. More recently, hardware tokens, cryptographic means, and biometric techniques also have been used to supplement or replace the traditional credentials.

Authentication

- Authentication strength determined by number of factors used
 - Something you know
(user ID and password)
 - Something you have
(smart card)
 - Something you are
(fingerprint)

Audio: The term *authentication strength* refers to the degree of confidence one can have in the person's identity based upon how thoroughly that person was vetted, and the type of credential used. An important consideration in determining authentication strength is the number of factors used by the authentication mechanism.

There are three factors: Something you *know*, something you *have*, and something you *are*.

A user ID and password combination is an example of something you know.

A smart card is an example of something you have.

A fingerprint is an example of something you are.

Factors may be relied upon singly or in combination. Authentication strength is higher when two or more factors are used together.

Authentication of an individual's identity is needed in order to make sound

access control decisions, but should not be confused with *authorization*.

Authorization

- Process to determine if a person should be granted access
- Protects resources
- Not part of HSPD-12 or FIPS-201 standard

Audio: Authorization determines if a person is allowed to have access to data, services, or facilities, including restricted areas. Authorization takes place only after an individual is authenticated and their identity is adequately trusted.

Authorization protects physical and IT resources by allowing users to access only those resources for which they have been granted permission. Authorization can be performed in many ways, such as by maintaining access lists or by checking databases.

Authorization is specifically not included in HSPD-12 or the PIV standards. Departments and agencies are required to determine how they will perform authorization.

In summary, authentication determines who you are and how much confidence someone can have in your credentials, based on the authentication mechanisms they employ. Authorization determines what you can do on a system, or what facilities you may enter once you have been successfully authenticated.

Scenario

Audio: Miss Casey Moore works for the Department of Energy Conservation (DEC) and has an Energy Conservation ID badge. Casey goes to the Office of Oil Exploration (OOE) for business. However, Casey discovers that OOE cannot accept her Energy Conservation badge to prove her identity because the two agencies have differing security requirements for issuing the badge. They also have different colors for indicating employee or contractor status which the security guards are not trained to recognize, and use different card technologies.

No common framework exists to support the use of badges between agencies. Casey may not be able to easily carry out her business, but

would be admitted to the building easily if OOE trusted her badge to prove her identity.

Self-Assessment #1

Is Casey Moore's problem one of authorization or authentication?

Authorization

Authentication

The correct answer is authorization. Casey has a problem of proving her identity to OOE. Her identity is not adequately trusted, which is the first step.

Audio: Take a moment to answer a question about the scenario you just heard.

Summary

- Identity and Access Management (IdM)
- You understand PIV concepts, authentication vs. authorization

Audio: All of the items we've talked about thus far are elements of a broad and growing field in security called Identity and Access Management, or IdM. IdM governs the full life cycle of a person's identity and access relationship to an organization.

Now that you have a better understanding of some basic PIV concepts, and the distinctions between authentication and authorization, let's put it all into a larger context.

Lesson Two

What Identity Management Challenges Does the Government Face?

Audio: In Lesson Two, we will discuss what identity management challenges the US Government currently faces.

Lesson Two Objective

- Recognize the importance of Federal identity management challenges

Audio: This lesson will help you understand today's Federal identity management challenges, and their importance.

Current Situation

- No assurance that accounts and privileges are closed
- User info duplicated, inaccurate, obsolete

Audio: The government has created a standardized process for issuing identity credentials. Why is the new standard necessary? To answer that question, let's look at some examples of the current situation within many Federal agencies:

First, no method exists to ensure that the right people have the right access privileges. People are initially issued badges, then sometimes keep their old affiliations and privileges as they move through or leave an agency. There is no assurance that all accounts and privileges have been closed.

Also, user information is often fragmented, duplicated, inaccurate, or obsolete. For example, a person might use their middle name on a daily basis, but also have a record listed in the system under his or her first name.

Current Situation

- Redundant processes
- Limited integration of physical and logical security
- Productivity losses

Audio:

Here are some more examples:

Redundant processes exist, even within agencies. Organizational "stove-pipes" create multiple card formats, and different locations employ different processes.

There is limited integration of physical security and logical security systems. Currently, it is not common to have one credential which

verifies your identity, and also gives you access to the building and information resources.

Productivity losses are normally not accounted for. Productivity diminishes while waiting to get access, change passwords, remove access privileges, and cope with needless redundancy in data collection between systems.

Self-Assessment #2

Take a moment to reflection on your agency's process for managing identity credentials. Do you know of any issues that fit the examples just given?

Audio: Now, take a moment to compare these examples with the situation in your own department or agency. Do any of the examples just mentioned remind you of issues in your office?

Given the current state of most federal systems, let's examine what identity management will look like in the future.

Click anywhere to continue.

Lesson Three

What is HSPS-12?

Audio: In Lesson Three, we will discuss Homeland Security Presidential Directive 12 (HSPD-12).

Lesson Three Objectives

- Define HSPD-12
- Identify the importance of HSPD-12
- State the benefits of HSPD-12

Audio: This lesson conveys the definition, importance, and benefits of HSPD-12.

What Is HSPD-12?

Common Standard for an ID for Federal employees and

contractors that is:

- Issued based on sound criteria
- Resistant to fraud
- Authenticated rapidly
- Issued by officially accredited providers

Audio: Homeland Security Presidential Directive 12 (HSPD-12) establishes a common standard for a secure and reliable form of identification for Federal employees and contractors.

HSPD-12 compliant identification is:

Issued based on sound criteria for verifying an individual employee's identity

Strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation

Rapidly authenticated electronically

Issued only by providers whose reliability has been established by an official accreditation process

So, why is HSPD-12 important?

Why Is HSPD-12 Important?

- Improves interoperability
- Requires agencies to adopt stronger security
- Provides consistency for issuing credentials
- Addresses access to physical facilities and logical assets

Audio: Identity credentials used for physical access to federal facilities vary widely. Therefore, there is often no trust or reciprocity between agencies.

HSPD-12:

- Improves interoperability between agencies
- Requires Federal agencies to adopt stronger security standards and procedures

- Provides a consistent method for issuing identity credentials
- Addresses access to physical facilities, such as buildings, and logical assets, such as information systems

What Are the Benefits of HSPD-12?

- One system – one credential
- Common credential = improved security, efficiency, productivity

Audio: HSPD-12 forces the convergence of physical access control and logical identity management.

In other words, it establishes the concept of “one system - one credential”.

A common credential will improve security by providing a common way of authenticating identity for access to facilities and systems, and use a consistent and reliable issuance process.

Next, we will discuss FIPS-201, which defines the technical standards for a PIV system.

Lesson Four

What is FIPS-201?

Audio: The topic of Lesson Four is Federal Information Processing Standard 201.

Lesson Four Objectives

- Define FIPS-201
- Explain the importance of FIPS-201
- Distinguish PIV-1 from PIV-2

Audio: This lesson conveys the definition, importance, and requirements of FIPS-201.

What Is FIPS-201?

- Defines a PIV system

- Common ID credentials are created
- Credentials later used to verify identity
- Does not address authorization

Audio: The FIPS-201 standard defines a Government-wide PIV system where common identification credentials can be created and later used to verify a claimed identity.

FIPS 201 does not specify who can access which system resources. In other words, it only addresses authentication and not authorization. Decisions pertaining to policies, technologies and controls regarding authorization have been left to the Departments and agencies.

Why Is FIPS-201 Important?

- Establishes consistent processes
- Creates a uniform and interoperable credential
- Provides centralized means of identity authentication
- PIV-1 and PIV-2

Audio: FIPS-201 is an important standard because it establishes consistent, repeatable processes to ensure personnel are properly identified.

It provides for a uniform credential that can be recognized and electronically processed within and between agencies.

FIPS-201 also improves authentication by relying on centralized systems and management processes to create reliable credentials and interoperable information exchange capabilities.

FIPS 201 has two parts, PIV-1 and PIV-2. Let's start with PIV-1.

What Is PIV-1?

Policies and procedures for verifying a person and issuing a trusted identity credential.

- Identity proofing— providing enough information to reliably establish identity
- Registration – making person's identity known to the PIV

system

Audio: PIV-1 defines the requirements for issuing a trusted identity credential that is recognized as valid outside the facility or agency which issued it. PIV-1 includes policies and procedures for identity proofing and registration.

Identity proofing means providing sufficient information, such as identity history, credentials, or documents, to a PIV registrar when attempting to establish an identity.

Registration makes a person's identity known to the PIV system, associates a unique identifier with that identity, then collects and records the person's relevant attributes in the system.

What Are PIV-1's Requirements?

- Use an approved ID proofing and registration process
- Initiate a national agency check (NAC)
- Complete an FBI fingerprint check
- Require the person to appear at least once
- Require two forms of ID source documents
- Enforce separation of duties

Audio: In accordance with PIV-1, when issuing identity credentials, agencies must:

- Adopt and use an approved identity proofing and registration process
- Initiate a National Agency Check
- Complete an FBI fingerprint check
- Require the individual to appear in person at least once before the agency issues a PIV credential
- Require two forms of identity source documents in original form during identity proofing
- Assure that no single individual can issue a PIV credential without the cooperation of another authorized person

PIV-1 does not address the issuance of a smart card. In other words, under PIV-1, neither interoperability nor a single, universal credential is required. Instead, PIV-1 addresses the process required to issue valid identity credentials in a uniform way.

What Is PIV-2?

- Technical standards for PIV credential to electronically authenticate personnel
- Provides for interoperability across the Federal Government

Audio: PIV-2 defines the technical standards for the PIV credential to electronically authenticate personnel. The credential issued must contain the embedded chips discussed earlier. Agencies must have the ability to load the required data and certificates onto the credential.

PIV-2 defines a common framework for how the PIV credential can provide basic interoperability across the Federal Government.

Using our earlier example, if Casey Moore would have had a Department of Energy Conservation PIV credential, that credential could have been recognized and processed at the Office of Oil Exploration to authenticate her identity. She would have been able to enter the OOE facility because each of the agencies would have trusted the other's credentials.

It's time for a self-assessment about the difference between PIV-1 and PIV-2.

Self-Assessment #3

An agency issues a plain plastic identity credential that was issued using an approved identity proofing process. To which set of requirements is the agency adhering?

PIV-1

PIV-2

The correct answer is PIV-1.

Audio: Take a moment to answer a question about what you've just learned.

Lesson Five

How Will HSPD-12 Affect My Agency?

Audio: In Lesson Five, we will describe the adjustments that your agency will need to make to implement a PIV program.

Lesson Five Objectives

- Describe process impacts
- Discuss implementation considerations
- Identify privacy issues

Audio: There are three main considerations:

- Process impacts
- Implementation considerations
- Privacy issues

What Are the Process Impacts?

- Establish PIV program within four months of standard issuance
- Identify and report new uses for the standard within six months of standard issuance
- Comply with PIV-1 by Oct. 27, 2005
- Comply with PIV-2 by Oct. 27, 2006

Audio: In implementing HSPD-12 and FIPS-201, several process changes will affect your day-to-day business operations. To comply with the standard, your agency must take the following actions:

- Establish a program to ensure that the credential issued by your organization meets the PIV standard. This program must be implemented within four months of the issuance of the standard.
- Identify any additional applications for which the standard should also be used, and report them to the Assistant to the President for Homeland Security and the Director of the Office of Management and Budget. This must be done within six months of the issuance of the standard.
- Your agency must comply with PIV-1 by Oct. 27, 2005
- Your agency must comply with PIV-2 by Oct. 27, 2006

What Are the Implementation Considerations?

- Challenges may not be technical

- Policy, planning, and management may play a larger role

Audio: Your agency may face numerous technical challenges in implementing HSPD-12. These include facilities, credentialing, and entity and access management. The majority of the toughest issues you will face, however, may not arise from technical issues. It takes more than a focus on information technology (IT) alone to implement HSPD-12. Organizations that have not had to work together before will need to cooperate in order to implement HSPD-12 effectively.

Success in implementing HSPD-12 also relies on business and industry insights into factors such as policy, process, management, organizational culture and, most of all, good governance. These factors may play a larger role than technology in implementing HSPD-12.

Next, we'll take a look at privacy and PIV.

What Are the Privacy Issues?

- Appoint a PIV privacy officer
- Assess PIV systems for privacy impact
- Identify information and how it will be used
- Ensure systems adhere to fair practices
- Audit systems for compliance

Audio: Protecting personal privacy is a core requirement of HSPD-12. Many of the requirements in the standard are based on longstanding privacy law and policy.

To ensure the privacy of PIV applicants, agencies will:

- Appoint a PIV privacy officer
- Conduct a comprehensive privacy impact assessment on PIV systems
- Identify information to be collected about individuals, and how the information will be used
- Ensure that systems containing personal information adhere to a set of standards governing the collection, accuracy, and use of personal data.
- Audit systems for compliance with privacy policies

What Are the Privacy Issues?

- No central database
- Personal information stored on credential is minimal
- Personal information is PIN protected

Audio: The government will not establish a central database to track movement of employees and contractors or the systems they access.

Personal information stored on the PIV credential is minimal.

Personal information, such as electronic fingerprints, will be protected with a Personal Identification Number (PIN) while stored on a PIV credential.

Self-Assessment #4

Which set of issues would likely require more of your agency's focus when implementing HSPD-12?

Application integration, hardware and software, data storage, business architecture

Regulations, budget, policies, process, governance

The correct answer is regulations, policies, process, governance.

Audio: Please take a moment to answer our last Self-Assessment question.

Conclusion

Audio: We'll conclude this module by reviewing what you have learned and by giving you a list of Web links to consult for more information about HSPD-12 and FIPS-201.

Module Review and Summary

- Basic PIV concepts
- Federal identity management challenges
- Importance and benefits of HSPD-12

- Importance and requirements of FIPS-201
- Effects on Federal agencies on implementing HSPD-12

Audio: In this module, you learned the following:

- Basic PIV concepts
- Identity management challenges facing the Federal Government
- The importance and benefits of HSPD-12
- The importance and requirements of FIPS-201
- The effects on Federal agencies on implementing HSPD-12

Where Do I Get More Information?

- [National Institute of Standards and Technology \(NIST\) PIV Project](#)
- [General Services Administration \(GSA\): Smartcard.gov](#)
- [Federal Identify Credentialing Committee \(FICC\)](#)
- [Interagency Advisory Board \(IAB\)](#)
- [Smart Card Alliance](#)

Audio: If you'd like more information about HSPD-12 and FIPS-201, please visit the links on this page.

Module Completed

You have completed the HSPD-12 Overview Module. Select the "X" in the upper right of the browser window to exit.

Thank You!