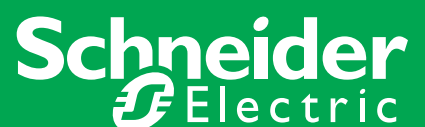


US Security Directive FIPS 201 Compliance Strategies

Learn about compliance strategies for governmental agencies in meeting requirements of Homeland Security Presidential Directive 12 (HSPD-12), and Federal Information Processing Standards Publication 201 (FIPS 201).

March 2008 / White Paper

Make the most of your energy



Summary

I. Executive Summary	3
II. Issues, Definitions, and Governmental Roles	4
III. Challenges and Benefits of Integration	8
IV. HSPD-12/FIPS -201 Compliance Solutions from TAC	9
V. Conclusion.....	13

I. Executive Summary

All U.S. government agencies are faced with a major challenge of combating and preventing terrorism in order to improve homeland security. Today, the U.S. government operates a combination of newer and older legacy systems requiring significant, costly, and time consuming integrations and the adherence to multiple, incompatible standards. Terrorists, however, do not have similar legacy systems and are starting with new technologies that can penetrate these older systems throughout the world.

To meet this challenge, The Homeland Security Presidential Directive 12 (HSPD-12) was issued on August 27, 2004 mandating the implementation of a common card to be used for logical and physical access to federally controlled facilities and information system owners by both government employees and contractors; this led to the actual standard requirement of FIPS 201.

Although this common card provides proof of identity, it does not provide cardholder privileges. Individual physical and logical access control systems and agencies retain the ability to grant or deny privileges to cardholders.

Requirements of this common card include:

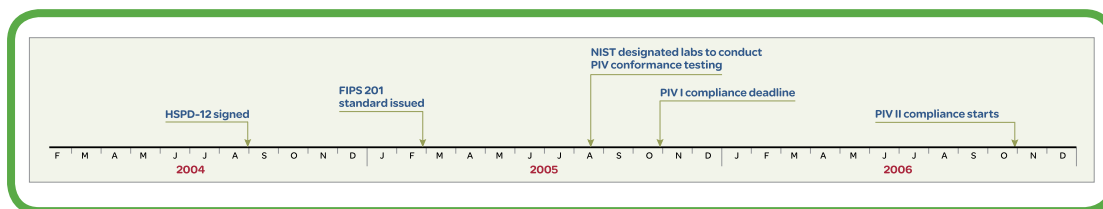
- Strong criteria for verifying an individual's identity
- High resistance to identity fraud, tampering, counterfeiting, etc.
- Fast electronic authentication
- Issuance by official accredited bodies in a secure manner

The National Institute of Standards and Technology (NIST) published the Federal Information Processing Standards Publication 201 (FIPS 201) Personal Identity Verification (PIV) of Federal Employees and Contractors on February 25, 2005.

- PIV part 1 addresses the security requirements of HSPD-12. This part has been implemented by policy in most agencies.
- PIV part 2 addresses technical interoperability requirements and specifies the use of common identity cards for use in a Federal PIV system. This part is being addressed by numerous NIST technical specifications.

This white paper discusses the implications of HSPD-12 on Physical Access Control Systems and TAC's response to these requirements, and provides actionable information for the impacted government agencies.

II. Issues, Definitions, and Governmental Roles



Timeline

- Homeland Security Presidential Directive-12 (HSPD-12) issued by President Bush in August of 2004, entitled Policy for a Common Identification Standard for Federal Employees and Contractors:
 - o The objectives of HSPD-12 are to remove silos and to develop an improved federal credential system
 - o Required new ID cards for all federal employees and contractors
 - o Includes all DOD employees (but excludes access to national security systems)
- NIST released FIPS-201 on February 25th, 2005
- NIST issues initial PIV-1 (issuance and control process) compliance for 10/27/2005
- NIST issues PIV-2 (credential standards and interoperability) compliance for 10/27/2006
- Reduced information and processing redundancies
- Reduced overlap of passwords and increased security
- Greater convenience and flexibility for federal employees

Which government agencies will manage this directive?

Four federal agencies have specific responsibilities for implementing this directive: Department of Commerce, Office of Management and Budget (OMB), General Services Administration (GSA), and Office of Personnel Management (OPM). NIST, as stated above, is establishing standards, recommendations, guidelines, and conformance tests for components of the PIV system. OMB is responsible for overseeing agency implementation of the directive and will develop implementation guidance for federal agencies. GSA is responsible for assisting agencies in procuring and operating PIV sub-systems such as card and biometric readers. OPM is responsible for assisting agencies in authenticating and vetting applicants for the PIV card.



Key information requirements for HSPD-12

- Is issued based on sound criteria for verifying an individual employee's identity
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
- Can be rapidly authenticated electronically
- Is issued only by providers whose reliability has been established by an official accreditation process.

Long term benefits of HSPD-12

- Improved efficiencies in service delivery
- Leverage the costs of investment for new systems and technology

Key points:

- The OMB Memorandum M-05-24 requires that government agencies purchase only federally approved products and services for implementation of HSPD-12.
- The GSA is responsible for purchasing of products by Federal agencies and developed the GSA Approved Product List (APL) for FIPS 201.

The role of the National Institute of Standards and Technology on FIPS 201

In response to HSPD 12, the National Institute of Standards and Technology Computer Security Division initiated a new program for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems. Federal Information Processing Standard (FIPS) 201, entitled Personal Identity Verification of Federal Employees and Contractors, was developed to satisfy the requirements of HSPD 12, approved by the Secretary of Commerce, and issued on February 25, 2005.

FIPS 201 incorporates three technical publications specifying several aspects of the required administrative procedures and technical specifications that may change as the standard is implemented and used. NIST Special Publication 800-73, "Interfaces for Personal Identity Verification" specifies the interface and data elements of the PIV card; NIST Special Publication 800-76, Biometric Data Specification for Personal Identity Verification" specifies the technical acquisition and formatting requirements for biometric data of the PIV system; and NIST Special Publication 800-78, "Cryptographic Algorithms and Key Sizes for Personal Identity Verification" specifies the acceptable cryptographic algorithms and key sizes to be implemented and used for the PIV system.

In addition, a number of guidelines, reference implementations, and conformance tests have been identified as being needed to:

- implement and use the PIV system
- protect the personal privacy of all subscribers of the PIV system
- authenticate identity source documents to obtain the correct legal name of the person applying for a PIV "card"
- electronically obtain and store required biometric data (e.g., fingerprints, facial images) from the PIV system subscriber
- create a PIV "card" that is "personalized" with data needed by the PIV system to later grant access to the subscriber to Federal facilities and information systems; assure appropriate levels of security for all applicable Federal applications
- and provide interoperability among Federal organizations using the standards

These activities will be pursued as NIST resources permit.

The following link to the NIST Question and Answer web site is an excellent resource <http://piv.nist.gov/pivqa/index.php> for obtaining the details of this action.

PIV I – The issuance process

- Put a process in place which:
 - o Requires a background investigation
 - o Requires two identity source documents
 - o Prevents the use of fraudulent identity source documents
 - o Prevents credential issuance to a suspected or known terrorist



- o Ensures the individual whose background is checked is the person to whom the credential is issued
- o No credential is issued unless requested by proper authority. No single official may issue a credential.
- o All credentials have expiration dates and a process for revocation.
- Each agency's process to be approved

PIV II – The card & card management system

- Put a system in place which:
 - o Specifies a secure smart card
 - o Standardizes the appearance of the card
 - o Standardizes a minimum set of data inside the card
 - o Ensures interoperability between agencies

Getting started on FIPS 201

- **Applicant:** The applicant is the government employee or contractor in need of a PIV card to access federal sites or resources.
- **Sponsor:** The applicant's request for a PIV card must be sponsored or approved by someone with authority within the agency, such as the applicant's manager.
- **Registrar:** The registrar is responsible for processing approved PIV card requests, which includes validating the identity of applicants and initiating background checks.
- **Issuer:** The issuer is responsible for personalizing the PIV card and securely delivering it to the applicant.

Processes for FIPS 201

There are three primary processes involved in FIPS 201 projects:

- identity proofing and registration
- card issuance and maintenance
- access control.



Identity Proofing and Registration

The identity proofing and registration process involves the applicant, the sponsor and the registrar. The applicant must make an in-person appearance at a registrar enrollment station and present two forms of I-9 approved identification, known as breeder documents. Breeder documents may be scanned and must go through a document proofing process that authenticates them. Biometric information is also captured, which includes multiple fingerprints and a facial photograph. The sponsor signs the original PIV card request for verification at issuance.

The registrar also must have background checks performed on each applicant, which include cross-checking applicants against numerous federal databases, such as terrorist watch lists.

Requests for PIV cards, approvals, breeder document images, demographic data, biometric information and other registration data are securely stored in an identity management system (IDMS). The IDMS controls the process flow from registration through issuance and enables administrators to create or cancel privileges associated with each applicant.

Card Issuance and Maintenance

The card issuance and maintenance phase involves the applicant and the issuer. The issuer can personalize and print a card request before issuance or on-demand when an applicant appears at an issuance station. The issuance officer validates the identity of the applicant via identity documents and biometrics, and then activates the card. In a PIV II compliant system, the issuer embeds a cardholder authentication certificate for logical access, signed biometric data and signed physical access credentials on the smart card and issues the card.

Access

Physical Access: When a PIV smart card user presents his or her card at a point of physical access, such as a door, verification occurs to grant entry. If the physical area is being secured with a High Assurance profile, the point of physical access will rapidly communicate with an online certificate status protocol (OCSP) responder to verify the physical access credential signature and grant entry.

Logical Access: When a PIV smart card user presents his or her card for network access to data via interfaces such as Microsoft smart card login, a validation authority rapidly validates the user's logical access certificate with an OCSP responder that confirms the credential is still valid.

Many technology providers and components are necessary to implement the full range of PIV processes from registration to issuance to access. These include certification authority management, biometrics capture, identity proofing, an IDMS, a smart card manufacturer and a validation authority. There are many considerations and choices that HSPD-12 project managers must take into account when planning their deployments.

III. Challenges and Benefits of Integration

An agencies' HSPD-12 solution must operate within their existing infrastructure. Integration of PIV-II cards into legacy physical and logical access control systems is a challenge which must be addressed in the initial planning stages.

Good guidelines on compliance preparedness provided by the American Council for Technology

(ACT) include:

- Are there badging systems already in place?
- Have physical access control systems been assessed to determine what features are needed on PIV cards to support these systems?
- Is there an understanding of what current ID cards are used for and when they will need to operate in parallel until applications and systems are migrated to the new credential?
- Is there a migration strategy in place for moving to the new system?
- Has a budget been established for the cost of migration?
- Is a public key infrastructure (PKI) currently being used?
- Is there an electronic connection to OPM to conduct clearance requests and background checks?
- Is there an automated system for storing and retrieving personnel data?

The issues addressed within the checklist are fundamental for effectively implementing PIV-I and PIV-II to support HSPD-12. However, they are not comprehensive. Secure hosting, certified card issuers, and other issues must also be addressed. Agencies must also deal with defining and implementing an issuance system, smart cards, and evaluating options for leveraging this new authentication infrastructure to improve access control, current and future applications, and strategic, government-wide initiatives. Finally, agencies should review PIV-I policies and decisions to be sure that they in fact migrate to PIV-II, and manage new approaches evolving since the PIV-I

Benefits of Integrating the Security System with the BAS

- A site-wide seat interface enables one person to be trained on multiple security systems.
- Security components become multiuse. A motion sensor can be used for lighting control during occupied hours, and intrusion detection during unoccupied hours.
- During design, flexibility, efficiency, and economy provide room for additional security expansion or integration at the lowest cost.
- Better response to occupant needs, offering employees greater security and peace of mind.
- More information put to effective use, which gives agency security staff solid ground to stand on for prosecution and proof of loss. CCTV records also aid law enforcement authorities.
- Vendor independence, allowing the customer to choose from among best-of-class security products.
- Single source responsibility, whereby one integrator is held accountable for the entire security system.

deadline, such as the consideration of a national shared enrollment system where a single facility is shared by multiple agencies within a given area.

Federal agencies that are able to successfully address these issues will receive numerous advantages. Foremost, integration provides for reduced installation and operating costs because it eliminates component redundancy and allows employees to streamline operations. Furthermore, it reduces training and empowers system operators by allowing them to perform their duties more efficiently. Integration can simplify the operation and control of complex governmental systems, while enhancing security at the same time.

IV. HSPD-12/FIPS-201 Compliance Solutions from TAC

Andover continuum family of security products

- Powerful interfaces for graphics, schedules, trends, reports, alarms, personnel, programming and more
- Monitor live and recorded video from a Digital Video Management System
- Import and synchronize personnel records from HR databases with ease using LDAP or CSV files
- Battery backed storage for up to 480,000 personnel records
- Flash for easy online software updates
- Compatible with Andover Infinity hardware and CyberStation 1.8 and higher software
- Secure 10/100 Ethernet communications via IPsec/IKE Encryption with hardware acceleration for Authentication and Encryption
- Support for Area Lockdown and Condition “Threat” Level based access rights
- Support for Modbus XDrivers
- HSPD-12/FIPS 201 Ready

TAC goes well beyond traditional security systems with our integrated approach. By combining everything from video monitoring to access control to intrusion detection, we deliver a more complete security understanding.

Powerful System-Wide Control from Workstations or the Web

Andover Continuum provides a single view of all installed security systems, through user-friendly work-stations or over secure web links. For example, reports can be created for any event, with details down to the exact access point, so security breaches can be addressed more effectively, or faulty equipment can be recognized and corrected more rapidly. Continuum also allows for security systems to be connected with personnel information, making it possible to see exactly who accessed what areas and when.



With a single picture of security, and one view of all systems, facilities can be monitored, controlled and secured like never before:

- Access Control – protect every access point in a building
- Intrusion Detection – detect early, respond rapidly
- Digital Video Management – the latest technology, seamlessly integrated

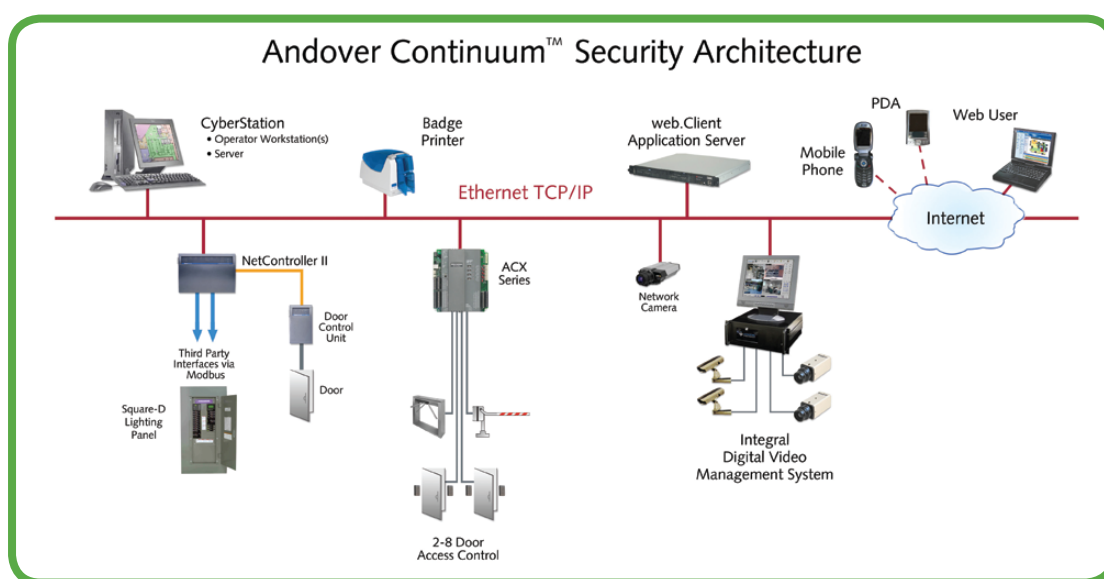
Respond Immediately to New Threats

In today's world, the security risk at a site may change in an instance. TAC has designed Andover Continuum to act swiftly in the event of heightened risk. We have added features such as “Area Lockdown” and “Conditional Level-Based Access Rights” to provide the most secure environment in times of elevated threats. With Area Lockdown, specific areas may be sealed off in an emergency. Card readers and exit requests can be disabled with a simple click of a graphic or an automatic program response. First responders can still gain access with “executive privilege.” Condition Level automatically reduces the access rights of personnel during a high risk period. With the ability to assign up to 255 condition or “threat levels,” the Andover Continuum system can be configured for any situation. Government security warning systems such as the U.S. Homeland Security Threat Levels may be linked to the Andover Continuum system to automatically set conditional levels at a site.

Secure, Encrypted Communications

TAC understands that securing a facility is more than securing doors and gates; the security system itself must be secure from hackers to protect the privacy of the personnel who utilize the system. The Andover Continuum system not only protects access from computers with user-based security, but also protects the information as it is transmitted

down the wire with encryption. To encrypt communications, TAC employs a combination of technologies, including Internet Protocol Security (IPsec) with Internet Key Exchange Protocol (IKE) to ensure tamper-proof communications between Andover Continuum controllers and workstations, and Secure Socket Layer (SSL) to provide secure communications via the Web, using a private key to encrypt data.



Cyberstation & web, client security software

As a complete user interface for the Andover Continuum system, CyberStation can be used to commission, configure, program, and monitor every security device, input and output attached to the network. Cyber-Station provides true integration of security (access control, intrusion monitoring and digital surveillance) within a single user interface.

Monitoring, Video Integration and Reporting

When it comes to monitoring and reporting, CyberStation really shines. Its graphics system is fully featured and provides dynamic updates of point values for any object on the system. Schedules, Live Event Views, Reports and

other tools can be launched from a graphic which provides quick, easy access to manage the whole system. Monitoring is further enhanced with the video integration features, allowing the user to view live and recorded video from a "Video Layout" matrix.

CyberStation's graphical reports can display raw log data in many output formats: html text reports, scalable vector graphic (SVG) bar, pie and line charts, or as an Adobe® Acrobat® PDF file. Furthermore, data can be represented statistically (e.g., the top 10 alarms, most commonly used doors). Reports can be run manually or executed on an alarm or schedule event and emailed to a predefined recipient list.



Alarms & Events

CyberStation serves as a powerful engine for collecting alarms and events and taking automatic actions (e.g., display the active alarm view, send as email, play an audio clip, launch a graphic, launch a live video layout). Users may be required to add a comment and sign off on alarm acknowledgments as an electronic signature of their action.

Programming

CyberStation contains a rich editor for programming Andover Continuum controllers with the Plain English (PE) programming language. This flexible environment allows for the most complex and customer-specific sequences to be programmed.

Simplified Personnel Data Entry and Badge Creation

Personnel records are easily managed using custom forms that require minimal training. Since the forms are customizable, agencies can be certain that these records are managed in a manner consistent with their organization. Assignment of access rights is as simple as assigning a record to a "Profile" that contains the valid areas and schedules for that group. To simplify data entry, CyberStation can import data using LDAP or CSV files.

When it comes time to create a physical badge, CyberStation is equipped with a full function badge creation package that captures photos, signatures and fingerprints, and prints to a wide range of badge printers.

web.Client Browser Interface

web.Client extends the Andover Continuum system to the web. Using the same database as CyberStation, web.Client gives the operator the freedom to access the Andover Continuum system

from anywhere on the network or over the Internet. Many of CyberStation's editors and features are available in web.Client. web.Client even uses the same graphics as CyberStation so there is no need to create or convert a specific graphic for web use. Furthermore, ad hoc reports may be created while connected to Andover Continuum via web.Client.

ACX series of access controllers

Communications

The ACX Series controllers are the industry's most powerful all-in-one access controllers designed for both critical government and public sector security applications. These Andover Continuum controllers are just as attractive for one to eight reader installations.

Onboard I/O for Access Control

TAC understands that not all security installations are the same. The ACX Series has been designed with flexibility in mind. There are two base hardware models: the 5720 and the 5740. The 5740 has double the universal inputs, reader inputs, and outputs onboard as the 5720. These models come standard with the following I/O configurations:

ACX Series	Model 5720	Model 5740
Universal Inputs	6	12
Reader Inputs	4	8
Tamper Input	1	1
Digital Lock Outputs	2	4

The ACX is designed to support both entry and egress readers while supplying +5 or +12 VDC to each reader.

128 MB of Dynamic Ram And 32 MB of Flash Memory

Each ACX Series controller comes standard with 32 MB of flash memory and 128 MB of DDR SDRAM. The flash memory is used to preserve 12 MB of application and run-time data. The dynamic RAM is partitioned for dedicated functions: a full 12 MB for applications, 48 MB for personnel records and 8 MB for the operating system. The unused memory is available for future enhancements.

Personnel record data is preserved using on-board batteries that can hold the data for at least 7 days without the use of an external UPS. If the controller has its application stored in flash and power loss lasts longer than what the battery can supply for RAM, the controller will send a message to CyberStation and request that the personnel records automatically be reloaded when the power returns.

Internal Support for 480,000 Personnel Records

The ACX Series is perfect for large systems. A controller servicing up to 8 areas can hold 480,000 personnel records. With such a large local storage capacity, access decisions can be made swiftly without waiting for validation by a remote server.

Advanced Reader Inputs with Dedicated Processor

The reader inputs are powered by a dedicated processor allowing the ACX Series controllers to support current and future devices for advanced applications. The ACX Series hardware is ready to support 260-bit encrypted data messages from the reader.

Full Credential Format Support for 260-Bits

The ACX Series controllers are ready to support a wide range of card formats. Ideal for retrofits, an ACX controller lets you preserve existing cards by accepting standard formats (Wiegand, ABA, HID Corporate-1000, CardKey) as well as custom formats (Custom Wiegand, Custom ABA). The ACX can support formats up to 260-bits making the ACX Series controllers ready for government installations that must meet HSPD-12 and FIPS 201 standards.

xP Module Support

Each model supports the use of two xP expansion modules plus an xP-Display unit. The xPBD4 module is ideal for expanding the ACX for special or ADA access to doors. Modules can also be used to provide a cost effective entry reader only solution.

For a complete set of Continuum components data sheets refer to:

<http://www.tac.com/Navigate?node=2901>.

V. Conclusion

HSPD-12 serves as a foundation for enabling future integrated government services. The smart card platform that will result from a FIPS 201 implementation can extend future functionality including:

- Secure remote access
- Single sign-on
- Additional card-based applications
- Government and enterprise integration
- Investigative capabilities

The importance of these new directives is significant. It is the largest convergence project to date.

The government creates one standard and one standard card.

- o One credential for physical access
- o One credential for computer log-on
- o Both systems interlinked

Requiring +5 million new cards for government employees

Requiring +2 million new cards for government contractors

Requiring upwards of 140,000 new high-end readers

Technology must work effectively as a tool for a well-trained security staff. Evaluating intrusion detection, card access control, and video surveillance systems for compliance with HSPD-12/FIPS-201 must also include an assessment that the technology can increase security and minimize the training and burden to agency security personnel. Government agencies should ask how integration with the facility's building automation system could provide further efficiencies of operation.

Schneider Electric

One High Street,
North Andover, MA 01845 USA
Telephone: +1 978 975 9600
Fax: +1 978 975 9674
www.schneider-electric.com/buildings

All brand names, trademarks and registered trademarks are the property of their respective owners. Information contained within this document is subject to change without notice.

On October 1st, 2009, TAC became the Buildings Business of its parent company Schneider Electric. This document reflects the visual identity of Schneider Electric, however there remains references to TAC as a corporate brand in the body copy. As each document is updated, the body copy will be changed to reflect appropriate corporate brand changes.