IMPLEMENTING AN HSPD-12 SOLUTION

PAVING THE PATH TO SUCCESS

Prepared by:

Nabil Ghadiali

Electrosoft

11417 Sunset Hills Road, Suite 228
Reston, VA – 20190
Tel: (703)-437-9451 Fax: (703)-437-9452
http://www.electrosoft-inc.com

July 2007

INTRODUCTION

On August 27, 2004, a Homeland Security Presidential Directive, (HSPD-12) - "*Policy for a Common Identification Standard for Federal Employees and Contractors*" was issued. The goals of this Directive are to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors. HSPD-12 requires agencies to adopt controls and procedures designed to prevent unauthorized access to government facilities and systems, reducing the potential for terrorist attacks.

In response to this directive, the National Institute of Standards and Technology (NIST) published a Federal Information Processing Standard (FIPS) 201 – "*Personal Identity Verification (PIV) for Federal Employees and Contractors*" on February 25, 2005. FIPS 201 and its associated publications provide detailed specifications for Federal agencies and departments, in order for them to deploy PIV cards to their personnel. This FIPS 201 Standard and all other related publications can be obtained from the NIST website at http://csrc.nist.gov/piv-program.

Once implemented and deployed by Federal agencies, the PIV card is envisioned to provide the attributes of security, authentication, trust and privacy using this commonly accepted identification credential.

The FIPS 201 Standard was released in two parts, PIV-I and PIV-II. PIV-I describes the minimum requirements for a Federal personal identity verification system that meets the control and security objectives of HSPD-12, including personal identity proofing, registration, and issuance. PIV-II provides detailed specifications that will support technical interoperability among PIV systems of Federal departments and agencies. It describes the card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the card.

HSPD-12 DOCUMENTATION

Several documents have been published by NIST in support of HSPD-12. All of these documents are critical for Agencies as they implement their HSPD-12 solutions.

FIPS 201: The main Standard for PIV

SP 800-73: Specifies the smart card interfaces (communication and application programming) and data model for the PIV Card

SP 800-76: Specifies the data format and acquisition requirements for cardholder biometric (fingerprint and facial) information

SP 800-78: Specifies the key size and cryptographic algorithm requirements for PIV

SP 800-79: Discusses the guidelines for certifying and accrediting PIV Card Issuing facilities

SP 800-87: Provides the organizational codes necessary to establish the Federal Agency Smart Credential Number (FASC-N) that is required to be included in the FIPS 201 Card Holder Unique Identifier (CHUID)

SP 800-104: Provides a scheme for PIV Visual Card Topography

SP 800-85A: Test guidelines for PIV Card Application and the middleware

SP 800-85B: Test guidelines for conformance to the PIV Data Model

In addition to specifications and guidance published by NIST, the Office of Management and Budget (OMB) as well as the General Services Administration (GSA) have also released Directives/Guidance that Agencies need to follow during their respective implementations.

OMB M-05-24: *Implementation of HSPD-12 – Policy for a Common Identification Standard for Federal Employees and Contractors*

OMB M-06-06: *Sample Privacy Documents for Agency Implementation of Homeland Security Presidential Directive (HSPD) 12*

OMB M-07-06: *Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials*

GSA Acquisition Guidance: *Acquisitions of Products and Services for Implementation of HSPD-12*

HSPD-12 SUPPORT PROGRAMS AND TOOLS

NPIVP – NIST has established the NIST Personal Identity Verification Program (NPIVP) to validate Personal Identity Verification (PIV) components and sub-systems required by FIPS 201 that meet the

NPIVP requirements. At present, the NPIVP validation program includes the Validation of PIV Card Applications and PIV Middleware for conformance to the SP 800-73 specification as documented in SP 800-85A. Additional NPIVP validation programs may be added as the PIV program evolves.
Web URL - http://csrc.nist.gov/npivp/

NIST MINEX Program - The Minutiae Interoperability Exchange Test (MINEX) is an ongoing evaluation of the INCITS 378 fingerprint template. One of the mandates of this test program is to establish compliance for template generators and template matchers for the Personal Identity Verification (PIV) program.
Web URL - http://fingerprint.nist.gov/MINEX/Home.html

GSA FIPS 201 Evaluation Program - OMB has designated GSA as the Executive Agent for government-wide acquisitions for the implementation of HSPD-12. OMB has directed Federal agencies to purchase only products and services that are compliant with the Federal policy, standards and numerous supporting technical specifications. In this respect, GSA has initiated the FIPS 201 evaluation program that will evaluate products and services against the requirements stated by FIPS 201 and its supporting documentation. If found to be compliant, these will be posted on an approved list thereafter which agencies can procure the same for their HSPD-12 solutions.
Web URL – http://www.smart.gov/fips201apl

SP 800-85B Test Tool: NIST has developed a test tool/application based on SP 800-85B test assertions that can be used to test issued PIV Cards for data model conformance to the FIPS 201 standard and its related technical specifications. This tool is envisioned to be used by Agencies to determine whether their PIV Cards are conformant to the Standard and thereby are capable of meeting the requirements of interoperability. The tool can be downloaded from the following URL: - http://www.csrc.nist.gov/piv-program/dm_tester/install_data_model_tester_enc.zip.

HSPD-12 Implementation Roadmap

Agencies need to comply with the Directive through implementation of FIPS 201 according to the following timelines:

June 27, 2005 - Needed to submit their implementation plans to OMB

August 26, 2005 – Provided a list of other potential or planned uses of the Standard to OMB

October 27, 2005 – Complied with FIPS 201, Part 1

October 27, 2006* –Begin compliance with FIPS 201, Part 2

October 27, 2007 – Verify and/or complete background investigations for all current employees and contractors

October 27, 2008** – Complete background investigations for all employees employed over 15 years

* Agencies need to issue and require the use of identity credentials for all new employees and contractors, compliant with Parts 1 and Part 2 of the Standard by this date. For current employees and contractors, issuance and use of identity credentials should be phased in meeting requirements of the Standard no later than October 27, 2007.

** For individuals who have been Federal department or agency employees over 15 years, a new investigation may be delayed, commensurate with risk, but must be completed no later than October 27, 2008.

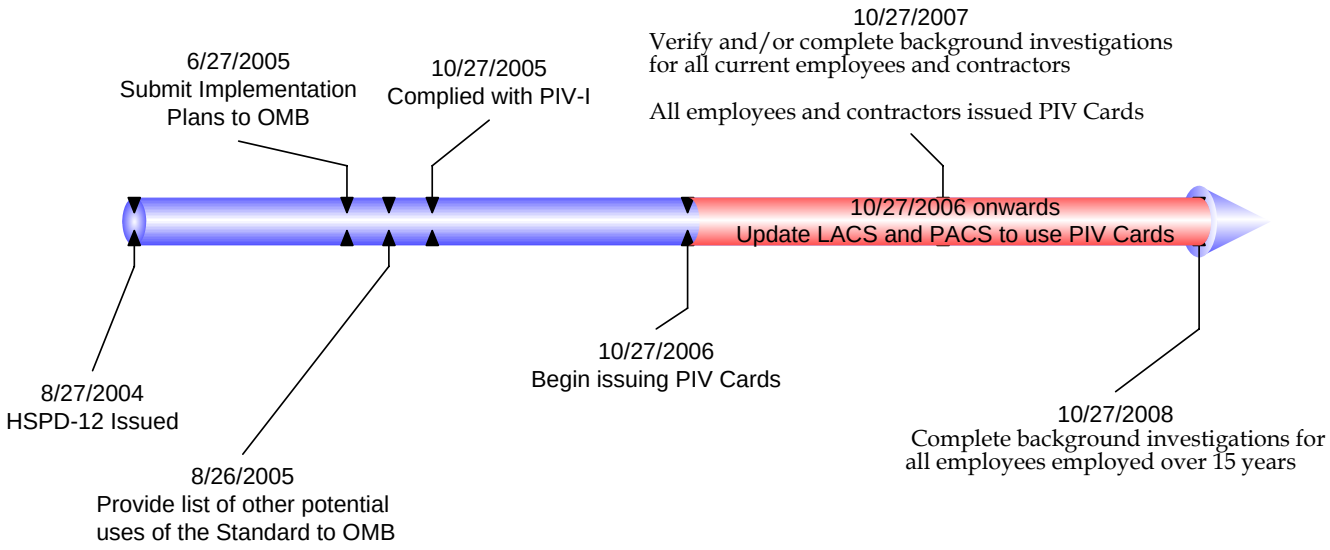

Figure 1 - HSPD-12 Implementation Timelines

HSPD-12 AND ELECTROSOFT

Electrosoft is an Information Technology Services company focused on solving complex problems in the Information Technology space, with a special focus on IT security and information assurance Electrosoft provides top-notch Identity Management, Public Key Infrastructure (PKI), Information Security consulting, and software development services to Federal agencies as well as private sector companies.

Electrosoft has been involved from Day 1 with HSPD-12 and continues to support NIST and other Federal agencies in their HSPD-12 activities. We have great credibility and experience within this space as is evident from the projects that we've handled.

FIPS 201 Development: Part of the core team at NIST that developed the FIPS 201, Personal Identity Verification (PIV) Standard. Areas of significant contributions included: Identity proofing, registration and issuance, PIV system overview, Graduated assurance levels, and PIV Card usage for identity authentication for logical and physical access control.

NIST SP 800-73 Development: Assisted in the development of NIST SP 800-73 (PIV Data Model, PIV Authentication Use Cases).

NIST SP 800-79 Revision: Currently supporting NIST as the primary authors for a major revision to SP 800-79 – *Guidelines for the Certification and Accreditation of PIV Card Issuing Organization*

PIV Card Demonstration Laboratory: Currently implementing a PIV Card Demonstration Laboratory at NIST. Secure applications being demonstrated to operate with a PIV Card include: (i) Windows Smart Card Logon, (ii) Client-Authenticated SSL/TLS secure web session, (iii) S/MIME, and (iv) VPN.

Microsoft Cryptographic Service Provider: Development of a Microsoft Cryptographic Service Provider (CSP) using the NIST PIV Middleware reference implementation, thereby allowing the use of a PIV Card for smart card logon to a Windows domain-based computing environment.

Public Key Cryptography Standard: Development of the Public Key Cryptography Standard (PKCS) #11 using the NIST PIV Middleware reference implementation, thereby allowing the use of a PIV Card for smart card logon to a Linux Workstation as well as for S/MIME transactions and client-authenticated TLS/SSL sessions.

NIST SP 800-85B Development: Supporting the NIST Personal Identity Verification Program (NPIVP) by developing Derived Test Requirements (DTRs), Test Assertions for cryptographic and PKI aspects of PIV for inclusion within NIST SP 800-85B.

GSA FIPS 201 Evaluation Program: Supporting GSA's FIPS 201 Evaluation Program by providing

Program Management and Technical Support. Develop and maintain all approval and test procedures as well as performed over 300 evaluations for the different product and service categories. Maintain the FIPS 201 Approved Products List (APL).

DoC PIV-I Compliance: Provided support to the Department of Commerce (DoC) in their PIV-I compliance effort. Developed role-based processes for identity proofing, registration and issuance of Personal Identity Verification (PIV) Credentials for all of DoC's PIV credential issuing facilities. Activities also included the development of guidelines (e.g. Implementation Guidance, Privacy Impact Assessment Guidance), and a compliance assessment checklist to assist DoC's PCI Facilities comply with FIPS 201 and SP 800-79 requirements.

NASA PIV-II Compliance: Provided support to the National Aeronautics and Space Administration (NASA) in their PIV-II compliance effort. Performed a third-party independent assessment of the NASA PIV Card Issuing Facilities based on SP 800-79 guidance to determine compliance with the FIPS 201 Standard.

BBG PIV-II Compliance: Provided support to the Broadcasting Board of Governors (BBG) in their PIV-II compliance effort. Developed all documentation necessary for accreditation (e.g. Operations Plan, Implementation Plan, Training Plan, Appointment Memos etc), as well as performed an independent assessment of their PCI Facility to determine compliance with the FIPS 201 Standard.

PIV System Architecture

A notional architecture for an agency's PIV solution has been depicted in Figure 2. This figure has been adapted from GSA's architectural model and illustrates the various functional components that form a PIV System. Based on an agency's requirement for centralized or decentralized identity management, enrollment and card issuance; multiple instances of the following components are necessary.

IDMS: The Identity Management System (IDMS) is the central component that interacts either directly or indirectly with all other components of the PIV-II Architecture. The IDMS interfaces with the authoritative data source (Personnel systems) to receive applicant information, the registration stations to receive identity proofing information and biometrics, the card management system to initiate activities related to card issuance and card lifecycle management, and to the client physical access and logical access control systems (PACS and LACS) to provision cardholder access control information.

Enrollment Stations: Enrollment stations are used to identity proof applicants and capture their biometrics for use in conducting background investigations and printing information on the PIV card. They typically will interface with the IDMS to receive and send information. Each enrollment station consists of the following components: digital camera for capturing the photograph and a fingerprint scanner for fingerprints. Additionally, a document scanner may also be present for scanning in identity source documents.

CMS: The card management system (CMS) is used to manage card lifecycle activities. The CMS interfaces with the IDMS as well as the certificate authority, card printing station, and the PIV card itself. The CMS will be used to manage the issuance and printing of a PIV card and the PKI certificate associated with that card. In addition, any updates that need to be made to the card post issuance, as well as card revocation, suspension, and PIN unblocks will be handled by the CMS.

PKI Certification Authority: The PKI component of the system will issue digital certificates, manage the keys associated with those certificates, and maintain up to date information on certificate status. PKI will include the certification authority, key management capabilities (if key escrow is required for key management keys), as well as certificate status information using certificate revocation list (CRL) or using the online certificate status protocol (OCSP). The PKI component will interface directly with the CMS and indirectly with the IDMS, and LACS and PACS in order to determine the revocation status of a PIV cardholder at the time of granting access to a federally controlled facility or system.

CPS: The card printing system (CPS) will manage the printing (includes both graphical and logical personalization) and finally distribution of the actual PIV cards. Card printing and distribution will interface directly with the CMS and the applicant and indirectly with PKI, and IDMS.

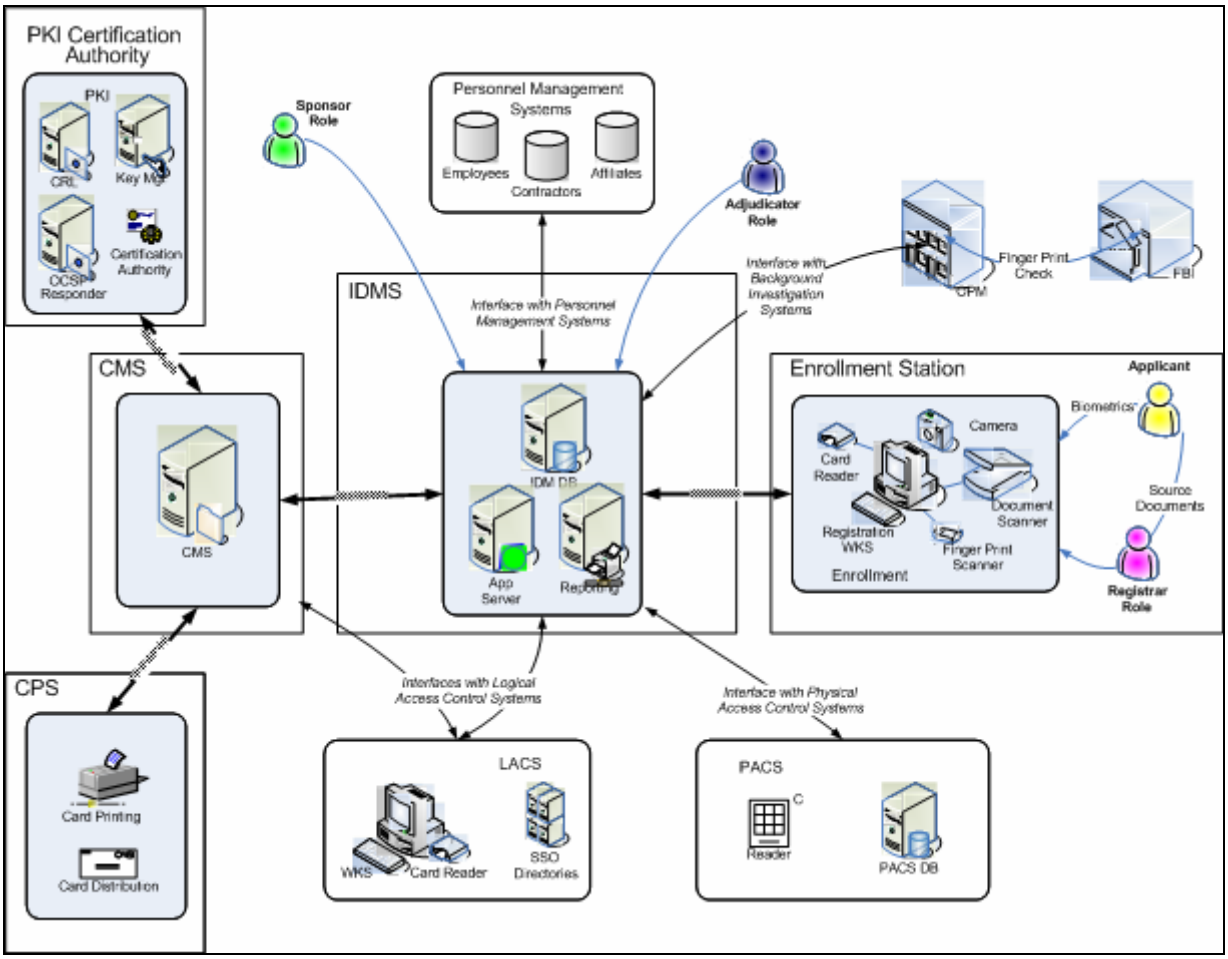

Figure 2 - PIV System Architecture (adapted from GSA)

Most agencies have one or more of these components today and therefore it is most probable that the agency's PIV system will be developed by adding new components to any existing components to arrive at the final PIV solution. Any new components need to be fully and transparently integrated with existing components (such as the physical access control systems, PKI, biometric capture systems) currently deployed within the agency. As components are integrated, compliance to all FIPS 201 requirements needs to be verified. Potential non-compliance areas need to be identified early on in the development lifecycle and these need to be rectified through collaborative work with the agency representatives. Professional service consultants of the vendors that supply the component products and services for the PIV solution need to be involved and utilized to ensure that the integration team understand the current status and constraints of the agency's environment, and thereby use this information into their integration strategy. Additionally, all disparate teams need to work in conjunction with one another to ensure that the agency timelines are met.

PROJECT MANAGEMENT APPROACH

Implementing an agency's HSPD-12 solution requires special management attention because of its (i) importance to the agency's mission, (ii) high development, operating and maintenance costs, and (iv) significant role in the agency's day-to-day operations. It is absolutely imperative that system integrators work collaboratively with the agency to provide administrative services to ensure that individual tasks proceed through a systematic sequence of initiating, planning, executing, controlling, and closing.

Scope Management: Ensuring that the project includes all work required and the boundaries are well defined.

Time Management: Ensuring that the project gets completed in a timely fashion.

Cost Management: Ensuring that the project is within the approved budget.

Integration Management: Ensuring that various elements of the project are properly coordinated amongst different integration team members.

Quality Management: Ensuring that quality is maintained at every stage within the project and the resulting solution will satisfy the needs for which it was undertaken.

Risk Management: Identifying, analyzing and responding to project risk by taking all eventualities into consideration and developing appropriate contingency plans.

Communications Management: Ensuring timely and appropriate generation, collection, dissemination, storage and transmission of information within the team and the agency representatives.

Procurement Management: Managing the processes required to acquire products and services from a variety of vendors in the most economical manner for the agency.

IMPLEMENTATION METHODOLOGY

An implementation strategy to support an agency's HSPD-12 implementation is described within this section. Each phase contains clearly defined deliverables and milestones with regular checkpoint meetings to ensure success. Figure 3 illustrates the various phases and the key elements of each phase.

Initiation: The initiation phase involves defining and documenting the scope of the project, building an integrated product team (vendors, system integrators, subject matter experts) with the appropriate skills to support the deliver of the project, defining the implementation strategy and then agreeing an achievable project schedule.

The roles and responsibilities of each of the project team members including all agency representatives are documented. A vital element in this phase is the risk assessment, which seeks to ensure that all eventualities have been considered and appropriate contingency plans generated where necessary. A Configuration Management Plan will be developed to ensure that baselines of any documents developed are put under configuration control.

The end result of this phase is a project schedule and Project Execution Plan (PEP). This document must be signed off by the agency prior to any activity being undertaken. Once the PEP has been signed off, any changes to the project scope will be subject to the defined change control process.

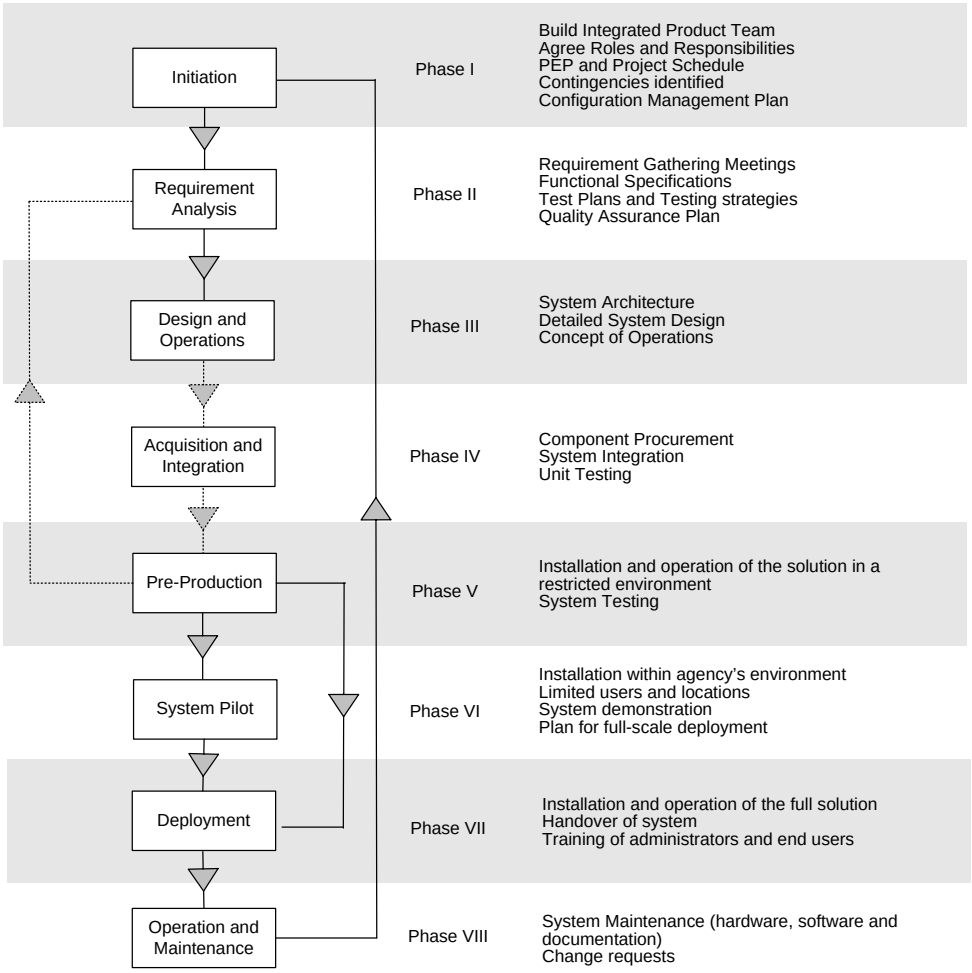

Figure 3 - HSPD-12 Solution Implementation Phases

Requirements Analysis: A critical step in implementing an HSPD-12 solution is to perform analysis and evaluation of current processes to determine how to implement a PIV system to meet the agencies objectives. An agency should've updated their card issuing process by Oct 27, 2005 to be compliant with the requirement for PIV-I.

The requirements analysis phase formally defines and delineates the requirements in terms of functionality, system performance, security, and maintainability requirements for the system. All requirements are defined to a level of detail sufficient for systems design to proceed. Gathering of these requirements may include holding a number of data discovery sessions and investigations (workshops) to ensure that the proposed design fully meets the business requirements of the agency.

Once the requirements have been agreed appropriate functional specification and test plans (including quality assurance plans) will be generated to ensure the solution's conformance to the agreed specification.

Design and Operation: The design and operations phase involves creation of the system architecture, information flow between target system components and includes the high-level design of custom software components or the advanced configuration of standard commercial-off-the-shelf applications.

The operational processes for the system are also developed in detail to cover enrollment, responsibilities of the various identified roles, data security privacy, and various other technical, management and operational controls. An appropriate training delivery methodology and approach is also identified.

Acquisition and Integration: Once the system architecture and design has been approved by the Agency, the next step is to procure the different components of the HSPD-12 solution from the different vendors. The various components of the system are integrated and systematically tested. Component Integration and unit testing are key activities that occur during this phase.

Pre-Production: During this phase, the system is put together and tested as a whole within a restricted environment such as a laboratory. Testing (including performance testing) of the system is carried out to ensure that the functional requirements, as defined in the functional requirements document, are satisfied by the developed or modified system. Several iterations of development and testing may be necessary during this phase.

System Pilot: In the system pilot phase, the system is installed within the agency operational environment. The functioning of the system is tested with a limited set of users (pilot users) and possible geographic locations in case of a decentralized system architecture. The functionality of the system is demonstrated at this time and full-scale deployment is planned.

Additionally, the pilot system needs to be accredited using the NIST 800-37 methodology for IT Certification and Accreditation followed by NIST SP 800-79 methodology for PIV accreditation prior to making the pilot system operational.

Deployment: The phase is initiated after the system has been tested and accepted by the agency in the pilot phase. Once the system pilot is considered to be functioning as per the agency requirements, the next phase involves the full scale roll-out of the system. The system or system modifications are installed and made operational in a production environment. This phase continues until the system is operating in production in accordance with the defined functional requirements.

On-site training to administrators and end-users of the system is conducted and may include the use of Computer Based Training (CBT). During this phase the system is officially handed over to the agency.

Operations and Maintenance: This is the last phase and unlike each of the other phase is an on-going activity that continues throughout the lifecycle of the system.

The system is monitored for continued performance in accordance with user requirements, and needed system modifications are incorporated. All system documentation (including C&A documentation) is kept current. The operational system is periodically assessed through In-Process Reviews to determine how the system can be made more efficient and effective. When modifications or changes are identified as necessary, the system may reenter the initiation phase. Activities include all necessary support services such as provisioning, installation, operational and maintenance, and repair as well as help desk support.

CERTIFICATION AND ACCREDITATION OF PCI FACILITIES

One of the control objectives of HSPD-12 is that the identification credential be "*issued only by providers whose reliability has been established by an official accreditation process*". In order to meet this requirement of HSPD-12, NIST published SP 800-79 - *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations.* Agencies cannot issue PIV Cards until their PCI Facilities have been accredited as meeting the requirements from FIP 201 and SP 800-79. The guidelines discussed within SP 800-79 intend to help Federal agency officials in the following:

- Satisfy the requirement in HSPD-12 that all identity cards be issued by providers whose reliability has been established by an official accreditation process;
- Answer several questions about the PCI including— Does the PCI Manager and staff understand the requirements specified in FIPS 201? Can the PCI reliably provide the required services?
- Ensure more consistent, comparable, and repeatable assessments of the required attributes of PCI's;
- Ensure more complete, reliable, and trusted identification of individuals; and
- Facilitate informed PCI accreditation decisions without significant delay or use of resources.

At the highest-level, the main tasks within an SP 800-79 include the following:

1) Assign the appropriate roles and responsibilities in accordance to the PIV Card Issuing organization structure
2) Make sure that the PCI has adopted and will use an approved identity proofing, registration, issuance and maintenance processes as required in FIPS 201.
3) Develop the operations plan. Confirm that the PCI system, all required roles, responsibilities, activities, and actions specified in the organizational structure are adequately documented in the PCI's operations plan are used for performing the required services.
4) Assess the required and desired attributes of the PCI using methods and procedures selected or developed i.e. perform the certification on the PCI Facility.
5) Prepare the assessment report and develop a corrective action plan (if needed). Assemble the accreditation package and submit to the Designated Accreditation Authority (DAA)
6) Once accredited to operate, continuously provide oversight and monitoring of the day-to-day operations of the PCI on an ongoing basis so as to evaluate any impact of a change on the reliability of the PIV System or any of its components.

Agencies need to note that in addition to an SP 800-79, in order to be compliant with the provisions of OMB Circular A-130, App III, the IT system(s) used by PIV service providers need to be also certified in accordance with NIST SP 800-37 - *Guide for the Security Certification and Accreditation of Federal Information Systems.*