Department of Transportation
Office of the Secretary of Transportation

ORDER

1681.2A

Subject: Department of Transportation (DOT) Homeland Security Presidential Directive 12 (HSPD-12) Personal Identity Verification (PIV) Card Program

Short Title: DOT HSPD-12 PIV Card Program

---

1. PURPOSE

This Order implements the U.S. Department of Transportation (DOT) identification card issuance and management portion of Homeland Security Presidential Directive – 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, subsequent Government-wide policies and directives issued by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST), and Department of Transportation (DOT) Order 1681.1 "DOT Identity, Credential and Access Management (ICAM)/HSPD-12 Implementation Policy." The ICAM/HSPD-12 policy provides overall DOT policy guidance for HSPD-12 and supports implementation of the Federal Identity, Credential, and Access Management (FICAM) requirements.

2. APPLICABILITY

This Order applies to all DOT Operating Administrations, Secretarial Offices, and the Office of Inspector General [components].

3. REFERENCES

a. Homeland Security Presidential Directive-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," dated August 27, 2004.

b. Federal Chief Information Officer (CIO) Council and the Federal Enterprise Architecture publication, "Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 2.0," dated December 2, 2011.

c. NIST Federal Information Processing Standards, "Personal Identity Verification (PIV) of Federal Employees and Contractors" (FIPS 201-2), August 2013, and all subsequent editions.

d. Title II, E-Government Act of 2014, Federal Information Security Management Act (FISMA).

e. NIST Special Publications (SP) listed below are accessible on-line.

(1) SP 800-85A-4, PIV Card Application and Middleware Interface Test Guidelines, dated April 2016.

(2) SP 800-79-2, Guidelines for the Authorization of PIV Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI), dated July 2015

(3) SP 800-73-4 Part 1, Interfaces for PIV – Part 1: End-Point PIV Card Application Namespace, Data Model and Representation, dated May 2015.

(4) SP 800-78-4, Cryptographic Algorithms and Key Sizes for PIV, dated May 2015.

(5) SP 800-76-2, Biometric Specifications for PIV, dated July 2013

(6) SP 800-116, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS), dated November 2008.

(7) SP 800-87, Codes for Identification of Federal and Federally-Assisted Organizations, dated April 2008.

(8) SP 800-96, PIV Card to Reader Interoperability Guidelines, dated September 2006.

(9) SP 800-85B, PIV Data Model Test Guidelines, dated July 2006.

f. Office of Management and Budget (OMB) M-11-11, Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – "Policy for a Common Identification Standard for Federal Employees and Contractors," dated February 3, 2011

g. OMB M-06-18 Acquisition of Products and Services for Implementation of HSPD-12, dated June 30, 2006.

h. OMB M-05-24 Implementation of HSPD-12 - Policy for a Common Identification Standard for Federal Employees and Contractors, dated August 5, 2005.

i. Office of Personnel Management (OPM) Memorandum, Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12, dated July 31, 2008.

j. DOT Order 1630.2C, Personnel Security Management, dated April 27, 2015, and all subsequent revisions.

k. DOT Order 1600.26B, DOT Facilities Protection Program, dated January 31, 2013, and all subsequent revisions.

l. DOT Order 1681.1, DOT ICAM/HSPD-12 Implementation Policy, dated June 23, 2011 and all subsequent revisions.

m. DOT Order and Manual 1680.3A, Identification Media Program, dated January 12, 2005, and all subsequent revisions.

n. DOT Memorandum, Personal Identity Verification (PIV) Cards: Emergency Response Official Designations, dated February 24, 2010.

o. DOT Memorandum, Requirements for DOT Identification Cards Not Meeting the HSPD-12 Standard, dated December 10, 2007.

p. DOT Order 1011.1, Procedures for Processing Reasonable Accommodation Requests by DOT Job Applicants and Employees with Disabilities, dated September 16, 2002.

q. DOT PIV Resources Links, ("Get It, Use It, Protect It") http://one10.dot.gov/office/ost/security/hspd-12/SitePages/Home.aspx.

4. CANCELLATIONS

DOT Order 1681.2 Homeland Security Presidential Directive 12 (HSPD-12) Personal Identity Verification (PIV) Card Program, dated December 21, 2011.

The following DOT memoranda were previously cancelled by the December 21, 2011 Order and are noted here for information purposes, as follows:

(1) DOT Memorandum, DOT Implementation of Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, dated January 28, 2005.

(2) DOT Memorandum, Requirements for Issuing Identification Cards Meeting the Standards of HSPD-12, dated May 24, 2006.

(3) DOT Memorandum, Updated DOT PIV Identification Card Format, dated February 1, 2008.

5. APPENDICES

a. Appendix A, Definitions.

b. Appendix B, Acronyms.

c. Appendix C, Roles.

d. Appendix D, PIV Card Issuance Process.

6. POLICY

Per DOT Order 1681.1, the Department shall issue identification cards meeting the requirements of HSPD-12 and Federal Information Processing Standard (FIPS) 201-2 (and all its successors), identified as PIV Cards, to its Federal employees and contractors who require access to DOT facilities and information technology systems, who meet the criteria outlined in DOT Order 1680.3A DOT Identification Media Program, and its successors.

7. BACKGROUND

a. On August 27, 2004, the President issued HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors. HSPD-12 mandated the establishment of a "Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors." Departments and agencies are required to use the PIV specifications resulting from this standard as a foundation for securely identifying individuals seeking access to sensitive Federal resources, including buildings, information systems, and computer networks. In addition to providing secure physical (location) and logical (information system/computer network) access to Government resources, provisions must be in place to keep personal information collected and used for identification private and secure.

b. NIST developed and published Federal Information Processing Standard (FIPS) 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors, as well as several Special Publications, which provide additional specifications and supporting information for compliance with HSPD-12. NIST also developed Guidelines for the Accreditation of PIV Card Issuers (SP 800-79-2) to provide appropriate and useful guidelines for accrediting the reliability of issuers of PIV Cards. The reliability of these issuers is of utmost importance in order to trust the identity credentials and cards they create and issue. NIST periodically updates these publications. The implementation, issuance, and use of PIV Cards throughout DOT must comply with these standards.

c. Over the past few years, the FICAM initiative has improved physical security and cybersecurity in the Federal Government. FICAM includes programs, processes, technologies, and personnel to create trusted digital identity representations of individuals and non-person entities (NPE), bind those identities to credentials that may serve as a proxy for the individual or NPE in access transactions, and leverage the credentials to provide authorized access to an agency's resources. The PIV Card is one credential that falls under the FICAM umbrella.

d. DOT has issued related policy in DOT Order 1681.1, DOT ICAM/HSPD-12 Implementation Policy, dated June 23, 2011, which specifies DOT will issue PIV Cards to Federal employees and contractors for use in accessing DOT facilities, networks, and information systems, as defined.

8. RESPONSIBILITIES

a. **The Assistant Secretary for Administration** shall establish DOT policy and procedures for the issuance of credentials meeting the requirements in FIPS 201-2 and

for the integration of the HSPD-12 PIV Card Program into DOT physical access programs.

b. **The DOT Director of Security** shall manage the implementation of policy, procedures, and standards for the issuance of PIV Cards, and shall perform the following functions:

(1) Establish and maintain the business case, architecture, investment(s), acquisition strategy, contracts, and systems necessary for enterprise issuance, maintenance, and revocation of PIV Cards, and support interoperability with PIV Cards issued by other Federal agencies, PIV-I[1] credentials issued by approved issuers, and Common Access Cards (CACs) issued by the Department of Defense.

(2) Issue all PIV Cards at DOT Headquarters and within the Metropolitan Washington, DC area, and in coordination with the Operating Administrations issue PIV Cards in field locations using Trusted Agents.

(3) Oversee and work with DOT components to establish and maintain PIV stations, thereby enabling components to issue PIV Cards at field locations. The DOT component operating these stations shall be responsible for on-going management of the PIV stations in keeping with current Office of Security (M-40) policy and guidance.

(4) Grant waivers or exceptions to PIV Card application and issuance processes as needed for DOT employees and contractors as a reasonable accommodation or for other reasons, provided compliance with FIPS 201-2 is maintained. Requests for waivers or exceptions shall be in accordance with DOT Order 1011.1, Procedures for Processing Reasonable Accommodation Requests. In carrying out this provision, the Director of Security will coordinate with the appropriate authority.

(5) Maintain a working agreement with the Federal Aviation Administration (FAA), and/or other authorized issuers, as appropriate, to provide cost-reimbursable PIV Cards, or other FIPS 201-2 compliant credentials, and related services to DOT components.

(6) Accept and acknowledge notifications of PIV Card loss or theft from the DOT Office of Chief Information Officer's Security Operations Center (SOC).

(7) Notify the DOT SOC of a PIV Card loss, theft, or cyber abuse if directly reported by any source other than the SOC.

c. **The DOT Privacy Officer** in the Office of the CIO, in consultation with the General Counsel, shall provide policy and guidance regarding privacy issues.

d. **The FAA Administrator** shall make available PIV Card services and support to DOT components on a cost-reimbursable basis through the Office of Security in accordance

[1] See APPENDIX A, Definitions, for a description of PIV-I (PIV-Interoperable) credentials and cards.

with the Inter-Agency Agreement (IAA). The FAA Office of Security, AIN-1, and its subordinate offices, is designated as FAA's servicing security organization; for the remaining components of DOT, the Director of Security is the servicing security organization.

e. **Heads of DOT Components** shall implement the HSPD-12 PIV Card Program as required by the provisions of this Order and DOT Order 1681.1, "DOT ICAM/HSPD-12 Implementation Policy." They shall:

(1) Appoint a designated HSPD-12/ICAM Lead to assist in implementing the HSPD-12 PIV Card Program as defined in DOT Order 1681.1, and appoint and obtain training for other staff, as needed, to fulfill roles outlined in APPENDIX C, "Roles."

(2) Follow the PIV Card issuance process outlined in APPENDIX D and the procedures promulgated by FAA and the Director of Security to obtain PIV Cards.

(3) Consult with the Director of Security and other DOT components to identify sites across the United States (field sites) where DOT PIV issuing stations for PIV Card processing (enrollment/activation) should be established. For example, a DOT component that has a field security office in a particular geographic area may host a processing office and share the services with other nearby DOT components that contribute funds or personnel to the effort. A DOT component with the greatest number of assigned personnel in a particular geographic area would most likely host the processing office. Processing offices require the following resources--

(a) Sufficient space, accessible to persons with disabilities, with a physical configuration to discourage deliberate or inadvertent viewing of personal information by unauthorized personnel.

(b) Dedicated products, equipment, and services to support the processing of PIV Cards, selected from those that are approved as compliant with Federal policy, standards and supporting technical specifications as published by the General Services Administration (GSA)[2] and per technical guidance from the DOT Director of Security and FAA.

(c) Trusted Agents who perform Identity Registration/Registrar and/or Issuer duties with the exception of adjudication functions.

(4) Commit to sustaining PIV Card issuance for all new DOT employees and contractors as described in this Order, and reissuance thereafter.

[2] GSA maintains a list of products that have been tested for conformance to FIPS 201-2. The list is available at https://www.idmanagement.gov/ under the Quick Links banner.

(5) Purchase PIV enrollment products, equipment, services and holders for PIV Cards from items approved by GSA as HSPD-12 compliant[3] and that meet the technical requirements for use with the DOT PIV Card.

(6) Ensure responsible personnel are assigned to the roles identified in APPENDIX C to support the HSPD-12 PIV Card Program (e.g., appoint and obtain training for Trusted Agents to perform registration and issuance duties at field locations). Heads of DOT components shall provide a list of these personnel to the Director of Security, or designee, as list updates occur.

(7) Implement the HSPD-12 PIV Card Program in accordance with privacy controls specified and referenced in FIPS 201-2 and its successors (referenced above).

(8) Commit to allocate and budget sufficient resources for the program as needed for sustaining card issuance and reissuance throughout their component.

(9) Ensure all new contracts include standard security clause language as established by the Office of the Senior Procurement Executive in conjunction with the Office of Security. Each DOT component shall ensure that contractors are aware of and compliant with personnel security, agency access and PIV Card requirements for contractors who require access to DOT facilities, sensitive information, information systems, and networks. Existing contracts shall have such language added at the next extension or renewal.

(10) Comply with policy and instructions as specified by the Director of Security regarding Physical Access Control Systems (PACS) and on-going card issuance guidance.

(11) Ensure DOT Federal employees and contractors apply for DOT identity cards, promptly take associated online training (if applying for a PIV Card) in order to complete the application process, and provide proper care for their identity cards.

(12) Ensure Federal employees and contractors take steps to fully enable their PIV Cards for physical and logical access systems when they receive these cards, following desktop enabling instructions to update their certificates, if necessary, in order to retain use of their PIV Cards for logical access.

(13) Ensure Federal employees and contractors reapply for renewal and subsequent reissuance of a new PIV Card no earlier than six (6) weeks prior to the expiration of their current PIV Card.

(14) Advise the Director of Security of those individuals who have been appointed to serve as Emergency Response Officials (EROs) per the criteria

[3] [id] management.gov: Qualified HSPD-12 Service Providers
https://www.idmanagement.gov/IDM/IDMFicamProductSearchPage

developed jointly by the Director of Security and the Director of Intelligence, Security and Emergency Response, to authorize the ERO designation to be placed on the employee's PIV Card.

(15) Direct requests for waivers, exceptions, or accommodations to the provisions of this Order to the Director of Security or work with the Disability Resource Center to direct such requests. Requests for waivers or exceptions may be made as a reasonable accommodation for DOT Federal employees or contractors or for other reasons as needed.

f. **DOT Security Operations Center shall:**

(1) Accept notifications for lost or stolen PIV Cards from any reporting source, create a security tracking incident, and capture pertinent information related to the loss or theft.

(2) Notify the Office of Security concerning the physical loss of the PIV Card.

(3) Notify the Office of Chief Information Officer (S-82) through the Incident Management Center for the logical access loss of the PIV Card.

(4) Process the security incident closure at the direction of the Information System Security Manager, Secretarial Office Director, or the Operating Administration Associate Administrator for Administration for the PIV Card user.

g. **DOT Federal employees and contractors[4] shall:**

(1) Apply for a PIV Card and promptly complete the associated training including the review and understanding of the DOT PIV Cardholder Responsibility Agreement. Upon notification of the approved application, complete the process of being issued a PIV Card.

(2) Properly handle and care for their card, keeping it in a GSA-approved cardholder except when actively used for physical or logical access.

(3) Wear the PIV Card in plain view on the front of an outer garment (e.g., blouse, shirt or jacket) at or above the waistline at all times while in a DOT facility. *Exception* –the PIV Card is not required to be worn if it interferes with carrying out their roles and responsibilities, while in use at a DOT computer or printer, or while participating in other activities such as exercising at the gym while inside a DOT facility.

(4) Fully enable their PIV Card immediately upon receiving the card by following desktop enabling instructions. Comply with policy and instructions from the DOT CIO regarding PIV Card use for logical access to DOT information systems.

[4] The contracting company is responsible for ensuring compliance by its employees with all requirements cited herein.

(5) Not use PIV Cards to gain influence or favors not specifically authorized by the DOT PIV Card Program, including but not limited to avoiding arrests or fines, gaining access to restricted areas not normally available to the PIV cardholder, obtaining travel priorities, or to imply an authority greater than granted to the PIV cardholder. Use of one's public office for one's own private gain, or for the gain of others, is a violation of the Standards of Conduct for Executive Branch employees per 5 CFR 2635.702.

(6) Protect and conserve Government property (including PIV Cards) and not use the PIV Card for other than authorized purposes, per 5 CFR 2635.704. Releasing a government issued PIV Card to other employees, contractors, family, or friends for beneficial gain is not authorized.

(a) Instances of misuse may result in adverse administrative or legal action.

(b) This section does not prohibit employees from taking advantage of commercial programs that offer discounts, upgrades, or other considerations upon showing of government identification. The Standards of Conduct specifically allow acceptance of such discounts provided they are offered to all Government employees [See 5 CFR 2635.203(b)(4)].

(7) Immediately report the loss or theft of their PIV Card to the DOT SOC at 1-866-580-1852, selecting option one (Report a Cyber/Security Incident) and to their Trusted Agent or local servicing security organization immediately upon discovery but not later than 18 hours after the incident as attempts to relocate the PIV Card or report the theft to law enforcement authorities are made. If the loss or theft of the PIV Card resulted in a police report, provide a copy of the report to the SOC, or the case number if the report cannot be immediately obtained from officials. Employees and contractors shall also immediately advise their supervisor, Contracting Officer Representative (COR), or servicing security organization, via phone and email, of the lost or stolen PIV Card to include the date and time when the loss or theft of the PIV Card was reported to the DOT SOC.

(8) Promptly return the PIV Card when no longer needed (e.g., due to separation from employment) to the immediate supervisor or Trusted Agent (for Federal employees) or to the DOT COR for contractors. For convenience and efficiency, PIV cards can be sent via FedEx, UPS, DHL or other accountable mail system with tracking capability to the following address:

U.S. Department of Transportation
Office of Security
ATTN: HSPD-12 Program Manager, W12-396
1200 New Jersey Avenue, SE
Washington D.C. 20590

A current list of Trusted Agents and PIV service locations at DOT Headquarters and in field office locations nationwide may be found at: http://one10.dot.gov/office/ost/security/hspd-12/SitePages/Home.aspx

(9) Apply for renewal and reissuance of a PIV Card no earlier than six (6) weeks prior to the expiration of the existing PIV Card and until the expiration date depicted on the front of the PIV Card, thereby allowing for continued use of the PIV Card without interruptions.

(10) Make requests for an accessible alternative, as needed, to the Director of Security or work with their supervisors or the Disability Resource Center to submit these requests. The Director of Security will work with appropriate personnel to ensure an effective alternative is identified.

(11) Report suspected inappropriate use of the PIV Card to their immediate supervisor or Office of Security via email to PHYSEC@dot.gov for investigation.

(12) Maintain physical control and not leave an unattended PIV Card in a computer or other device.

h. **Contracting Officers (COs) and Contracting Officer Representatives (CORs):**

(1) Federal employees who are COs and CORs shall ensure the applicable Federal and departmental security clauses are included in their assigned contracts, and CORs shall also ensure contractors are aware of and understand the security clauses in their assigned contracts. COs and CORs shall advise contractors of their responsibility to properly care for and protect the PIV Cards or other DOT identity cards that are in their control.

(2) CORs shall sponsor and approve PIV applications for contract employees submitted by the contractor for contracts to which they have been appointed as the COR. The CORs (or the CO if a COR is not appointed) shall promptly collect DOT PIV Cards and identity cards from contractors when no longer needed (i.e., due to completion of the work, contract termination, or contractor employee resignation) and immediately forward the cards to the DOT Headquarters ID Media Center or to the nearest Trusted Agent site.

9. ELIGIBILITY FOR A PIV CARD

a. DOT shall issue PIV Cards to:

(1) DOT Federal employees who are expected to be employed for a period of time in excess of six (6) months except as provided in 9.b below.

(2) DOT contractors who meet the criteria for an identification card as stated in DOT Order and Manual 1680.3A Identification Media Program (and all its successors) and are expected to need access to a DOT physical facility or information system for a period of time in excess of six (6) months including optional contract renewal periods.

b. Issuing offices may choose to issue PIV Cards to Federal employees and contractors who are expected to be employed or need access for less than six (6) months when it is necessary to meet a requirement for access to a DOT network or information system or when it is in the best interests of the Department to do so.

c. Applicants must meet the requirements of HSPD-12. See APPENDIX D.

d. Generally, issuing offices will choose to issue DOT approved non-PIV Cards to other types of personnel who meet the minimum requirements for DOT identification cards but only require physical access to DOT facilities. These categories may include but are not limited to: contractors working for the owner of leased facilities (such as custodial and maintenance personnel); cafeteria and snack bar workers; credit union personnel; child care workers, volunteers, and parents of children receiving care at DOT facilities; members of carpools using DOT parking facilities; and visitors. Organizations may issue DOT approved non-PIV Cards to such individuals as described in the DOT Memorandum "Requirements for DOT Identification Cards Not Meeting the HSPD-12 Standard" dated December 10, 2007. Temporary DOT identification cards may be issued to individuals who meet initial investigative requirements and who require immediate physical access.

e. Individuals assigned to work at DOT may already possess electronic identification cards (including PIV Cards or PIV-I [Interoperable] Cards) issued by other Federal agencies or by an authorized PIV-I issuer. These PIV Cards should, under normal circumstances, be compatible with DOT physical and logical access control systems. Unless authorized by the Director of Security, issuing offices shall not issue a second PIV Card to Federal employees or contractors who already have PIV Cards or PIV-I cards as long as those cards have been electronically verified as not revoked or expired, and the employees satisfy all other determinations of suitability for employment at DOT.

f. If a PIV Card is revoked after being issued (for example, if unfavorable information is uncovered during the background investigation after the employee has received the initial PIV Card), the individual may appeal the action to the Director of Security through the procedures identified in subparagraph 9.f(2) below.[5]

(1) Individuals do not have a right to appeal a revocation or denial decision under any of the following circumstances:

(a) A DOT component or OPM has determined that the individual is not suitable for Federal employment or employment at DOT under the provisions of 5 CFR 731 and he or she has been removed from employment or the component intends to remove him or her from employment.

(b) The individual has been denied a security clearance required for employment in a position that he or she holds and the DOT component has removed him or her from employment or is proposing his or her removal.

[5] FAA Federal employees, FAA contractors, and FAA affiliated personnel shall first follow any FAA appeal procedures before submitting an appeal to the Director of Security.

(c) A DOT component has determined the individual is not suitable to hold a position in the excepted service or the CO has determined the individual is not suitable to perform work on a DOT contract, or the individual is removed from his or her position or from work on the contract and will no longer have need for regular access to a DOT facility or information system.

(d) The individual no longer meets other criteria for holding a DOT identification card.

(2) Appeals may be filed by individuals not excluded as described above. For these individuals the appeal procedures are as follows:

(a) The appeal must be submitted in writing to the Director of Security within 10 business days of notification of the denial or revocation of the PIV Card. The Director of Security may grant an additional five business days to appeal, provided that the request for additional time is made within ten business days of being notified of the denial or revocation.

(b) If, as part of an appeal, the individual submits additional information not previously known that may be pertinent to a final decision, the Director of Security may refer the matter back to the official who made the denial or revocation decision for further consideration and review before the case is returned to the Director for a final decision. If the Director refers the case back to original decision maker, the official receiving the referral shall complete any additional adjudication within five business days. If the official re-affirms the initial decision to deny or revoke the card, then he/she shall provide all information supporting the denial back to the Director of Security. If the official finds in favor of the individual, the card shall be issued and no further action is required from the Director of Security.

(c) The Director of Security shall review all information regarding the appeal and, within 10 business days after receipt (assuming a five day extension was not requested and approved), the Director of Security will make a final decision to either uphold or reverse the decision. The decision of the Director is final and there is no further right of review.

10. PIV CARD MANAGEMENT

a. Issuance

(1) DOT shall issue PIV Cards only through systems and providers that meet NIST and GSA requirements. The PIV Card issuance process shall meet or exceed the minimum requirements of FIPS 201-2, PIV Card Issuance Requirements. All new and replacement PIV Cards shall be issued with the mandatory PIV Card features as required by FIPS 201-2.

(2) Trusted Agents shall manage the issuance of PIV Cards according to the requirements of this Order, following the "PIV Card Issuance Process," APPENDIX D.

(3) Applicants for PIV Cards must first meet DOT suitability requirements and be authorized to receive a card under the provisions of DOT Order 1680.3A Identification Media Program, all its successors, and this Order.

(4) The PIV Card expiration date shall be as follows:

(a) For Federal employees, the PIV Card shall be valid for no more than six years starting from the date of card issuance as specified in the current publication of FIPS 201-2.

(b) For contractors, the access programmed on the PIV Card shall not exceed three years or the lifetime of the contract including its option periods, whichever is shorter. PIV Cards issued to contractors will be valid up to three years or as otherwise specified by the Director of Security.

(c) Or as otherwise specified for other affiliations assigned to DOT and defined by the Director of Security.

(5) The PIV Card expiration date (month and year in uppercase) shall be printed in the upper right-hand corner and to the bottom right of the photo on the front of the PIV Card as mandated by FIPS 201-2.

b. Grace Period.

(1) A Grace Period affects a Federal employee or contractor whose employment status lapses briefly such as might occur with an interagency transfer. A contractor may experience a brief lapse of time between the expiration of a previous contract and the start of a new contract. PIV Cards reissued to an employee or contractor within a Grace Period shall be authorized by the proper authority with confirmation of a valid background investigation.

(2) Such individuals may be issued a new PIV Card without repeating the identity proofing and registration process if the card issuer can authenticate the individual's chain-of-trust data records and the issuer performs a 1:1 biometric match. In the event of an unsuccessful match or missing biometric data, the cardholder shall provide two identity source documents[6] for inspection and comparison of all enrollment data by the Trusted Agent.

(3) Re-investigations shall be performed, if required, in accordance with OPM guidance.

[6] See FIPS-201-2, page 9

11. PIV CARD MAINTENANCE

a. Prior to its expiration, a PIV Card may be updated or invalidated due to changes in a cardholder's data or credentials. The cardholder may initiate these changes, or the agency may do so to maintain operational readiness of the PIV Card. For example, when cardholders institute a name change or transfer agencies within the Federal government, a previously issued PIV Card must be invalidated and a new PIV Card reissued.

b. Under the reissuance process:

(1) A new PIV Card is issued to a cardholder without the need to repeat the entire identity proofing and registration procedure. PIV Cards may be reissued when: replacing a PIV Card nearing expiration; there is an employee status or attribute change; the card has been compromised, lost, stolen or damaged; or when a cardholder applies for reissuance because one or more logical credentials have been compromised. The old card is revoked when a new card is reissued. A re-investigation shall be performed if required.

(2) PIV cardholders may apply for the reissuance of their PIV Card no earlier than six (6) weeks prior to the expiration date depicted on the face of the PIV Card. Prior to reissuance of a new card, the Trusted Agent shall verify the employee or contractor has a current, acceptable background investigation and verify that the information contained in the personnel security files and any associated databases is current and accurate.

(3) The Trusted Agent shall ensure a proper authority has authorized the issuance of the new PIV Card.

(4) A servicing security organization must repeat the entire identity proofing, registration, and issuance procedures if the reissuance process was not started before the old PIV Card expired.

c. Cardholder Name Change. When a cardholder notifies a servicing security organization that his or her name has changed and presents evidence of a formal name change (e.g., marriage certificate, divorce decree, judicial recognition of a name change, or other mechanism permitted by State law or regulation), the servicing security organization shall issue the cardholder a new card following the procedures set out in APPENDIX D, PIV Card Issuance Process.

d. Loss or Theft of a PIV Card. Federal employees and contractors shall safeguard and care for their PIV Card at all times. The loss or theft of a PIV Card shall be immediately reported to the DOT Security Operations Center (SOC) at 1-866-580-1852 selecting option one (Report a Cyber/Security Incident) and to the Trusted Agent or local servicing security organization upon discovery. A Trusted Agent shall complete revocation procedures within 18 hours of notification. If the loss or theft of the PIV Card resulted in a police report, the cardholder will provide a copy of the report, or provide the case number if the report cannot be immediately obtained from officials.

The cardholder shall immediately advise the first line supervisor, COR, or servicing security organization, via phone and email, of the lost or stolen PIV Card to include the date and time when the loss or theft of the PIV Card was reported to the DOT SOC.

(a) Per FIPS 201-2, the Trusted Agent shall complete revocation procedures within 18 hours of notification of the lost or stolen PIV Card. The Trusted Agent will ensure action is taken to revoke or suspend the card in any card management system and associated Public Key Infrastructure (PKI) Certificate systems. The reporting process shall reflect whether or not Personally Identifiable Information (PII) or the personal identification number associated with the lost or stolen PIV Card was compromised. The cardholder shall also comply with the reporting instructions described in DOT Order and Manual 1680.3A, Identification Media Program, and all subsequent revisions.

(b) DOT components will require a waiting period of three (3) days before reissuing a replacement PIV Card for one that was lost, to allow time for a lost card to be returned or located by the owner. If a PIV Card is found within three (3) business days, the PIV Card can be reinstated by a Trusted Agent. Exceptions to the waiting period are considered on a case-by-case basis and must be requested in writing to the Office of Security, Associate Director for Personnel Security and ID Media.

e. Revocation. PIV Cards may be revoked for a number of reasons, including but not limited to (1) the loss or expiration of a card, (2) reissuance of a card, (3) an adverse action against the cardholder (administrative or criminal), (4) cardholder separation from Government or contract employment, (5) change of information appearing on the PIV Card (e.g., cardholder name or citizenship change) or (6) compromise of the electronic credential within the PIV card (e.g., the credential was illegally duplicated). The process of revoking PIV Cards shall include the revocation of the PKI certificate.

f. Suspension. A suspension is a temporary retrieval and/or deactivation of the PIV Card by the Trusted Agent. Suspensions may be voluntary or involuntary. If a PIV Card is suspended, the cardholder shall surrender the card to the OA's Trusted Agent until the suspension is lifted, and logical and physical access to DOT facilities and resources shall be temporarily denied. Suspensions may be imposed for reasons that include but are not limited to the following:

(a) The cardholder takes a leave of absence for longer than 90 days. A Trusted Agent shall require suspension of the PIV Card for absences exceeding 90 days.

(b) The cardholder has received an adverse administrative action such as temporary suspension of employment.

(c) Investigators uncover concerns during a background investigation that require further inquiry.

g. PIV Card Personal Identification Number (PIN) Reset

The PIN on a PIV Card may need to be reset by the servicing security organization if the cardholder has forgotten the PIN or if the contents of the card are locked because of multiple unsuccessful PIN entries. Before the reset PIV Card is returned to the cardholder, the card issuer shall ensure the cardholder's biometric matches the stored biometric on the reset PIV Card.

h. Departure, Resignation, Retirement, or Termination of PIV cardholders

DOT components shall immediately collect and return to the Trusted Agent or local servicing security organization all DOT identity cards from departing personnel, including Federal employees, contractors and their employees, and other affiliated individuals. It is the responsibility of the employee to turn in the PIV Card to the Trusted Agent at the DOT issuing office or to their supervisor. Contractors are responsible for returning the cards of their employees to the DOT COR, who will then return them to a DOT issuing office.

12. RECIPROCITY

a. Visitors

HSPD-12 compliant identification cards (PIV Cards) from other Federal agencies, PIV-I (interoperable) cards issued by an authorized PIV-I issuer, or CACs issued by the Department of Defense shall be accepted as evidence of the cardholder's identity provided the card has been electronically verified as not having been revoked or suspended. For DOT field locations, visitors presenting any of these cards shall be treated according to the facility access policies of the DOT component they are visiting (e.g., for these individuals, visitor screening and escort requirements are determined by the DOT component visited).

b. DOT Acceptance of Adjudication

For purposes of PIV Card issuance, DOT shall accept other organizations' favorable adjudications of background investigations when Applicants have PIV, PIV-I, or CAC Cards issued by those organizations and there has been no break in service. A favorable adjudication does not preclude DOT from also initiating a new investigation when necessary because of other personnel security requirements related to the Applicant's position at DOT or as allowed by government-wide policies concerning reciprocity of background investigations or adjudications.

13. ADDITIONAL INFORMATION

For additional information about the Office of Security and the PIV Card program click the following link: http://one10.dot.gov/office/ost/security/SitePages/Home.aspx located on the Office of Security's SharePoint site. Select the HSPD-12 icon.

Questions regarding this Order may be directed to the Office of Security.

FOR THE SECRETARY OF TRANSPORTATION:

Kent Wahl

Jeff Marootian
Assistant Secretary for Administration

9/8/11
DATE

APPENDIX A

DOT Order 1681.2A, DOT HSPD-12 and PIV Card Program

Definition of Terms

The following terms are associated with the Homeland Security Presidential Directive-12 (HSPD-12) Personal Identity Verification (PIV) Card Program.

Adjudication: The process directly following a background investigation where the investigation results are reviewed to determine if an individual is suitable for employment and/or eligible for access to classified information. In the case of a contractor employee, this is a determination regarding the individual's fitness for access to DOT facilities, sensitive information, resources, and/or information technology systems.

Applicant: An individual applying for a PIV Card. The applicant can be a current or prospective Federal hire, a Federal employee, a government affiliate, or a contractor.

Authentication: The process of establishing confidence in the validity of a person's identity and a DOT PIV Card.

Biometric: A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity of an Applicant. Facial images, fingerprints, and iris scans are all examples of biometrics.

Biometric Information: The stored electronic information pertaining to a biometric. This information can be in terms of raw or compressed pixels or some characteristic (e.g., patterns).

Cardholder: An individual possessing a DOT-issued PIV Card.

Card Management System: The DOT Identity Management system comprised of one or more systems or applications used to manage the identity verification, validation, and issuance processes. This system stores information regarding Applicant and cardholder identity vetting and verification information for DOT.

Certification: The process of verifying the correctness of a statement or claim and issuing a certificate associated with that information.

Chain-of-Trust: A sequence of related enrollment data records that is created and maintained by PIV Card issuers through the methods of contemporaneous acquisition of data within each enrollment data record, and biometric matching of samples between enrollment data records.

Code of Federal Regulations (CFR): An annual codification of the general and permanent rules published in the Federal Register by the executive departments and agencies of the Federal Government.

Credential: Evidence attesting to one's right to credit or authority. In this Order, it is the PIV Card and data elements associated with an individual that authoritatively bind an identity (and, optionally, additional attributes) to that individual.

DOT Component: Any DOT Operating Administration or Secretarial Office.

Enabling: Writing certificates required for authentication to physical and logical access control systems onto PIV credentials that have been issued to DOT Federal employees and contractors.

Expired PIV Card: The day or more after the date shown on the front of the PIV card.

Federal Information Processing Standards (FIPS): Standards for adoption and use by Federal departments and agencies that have been developed within the Information Technology Laboratory and published by the National Institute for Standards and Technology (NIST), a component of the U.S. Department of Commerce. These NIST standards address topics in information technology to achieve a common level of quality or some level of interoperability.

Identity: The set of physical and behavioral characteristics by which an individual is uniquely recognizable.

Identity Proofing: The process of obtaining sufficient information (e.g., identity history, credentials, documents) to establish an identity.

Identity Registration: The process of making a person's identity known to the PIV system, associating a unique identifier (example: name or a card number) with that identity, and collecting and recording the person's relevant attributes into the system.

Identity Verification: The process of confirming or denying that a claimed identity is correct by comparing the credentials (e.g. something you know, something you have, and something you are) of a person requesting access with those previously proven and stored within the DOT PIV Card or related information technology system and associated with the identity being claimed.

Issuing Office: The DOT Headquarters ID Media Center or DOT field offices where Trusted Agents enroll, issue, and activate PIV Cards for DOT employees and contractors.

Logical Access: Access to computer or other electronic IT systems, files and data.

Match/Matching: The process of comparing biometric information against previously stored biometric data and scoring the level of similarity.

National Agency Check with Inquiries (NACI): The minimum level background investigation that must be initiated before a PIV Card can be issued.

Non-Person Entities (NPE): A non-human entity with a digital identity that acts in cyberspace. NPEs include organizations, hardware devices (e.g., servers and routers), software applications, and information artifacts.

Non-PIV Card: An identity card issued by DOT that fulfills basic background investigation requirements and does not have all the electronic circuitry or capabilities of a PIV Card. Non-PIV Cards may be issued to categories of personnel who would otherwise meet the criteria for DOT identification cards, but who do not meet the time requirements or need for access to be issued a PIV Card.

Personal Identification Number (PIN): A private number created and used by the cardholder to authenticate his or her identity. PINs consist of six to eight numeric digits.

Personal Identity Verification (PIV) Card: A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, and digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another individual (human readable and verifiable) or an automated process (computer readable and verifiable).

Personal Identity Verification Interoperable (PIV-I) Card: A card or credential that meets the PIV technical specifications to work with Federal PIV infrastructure elements such as PACS and is issued in a manner that allows Federal Government agencies to trust the card. The PIV-I card is suitable for level of assurance 4 as defined in OMB Memorandum M-04-04 and NIST SP 800-63, as well as multi-factor authentication as defined in NIST SP 800-116.

Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity, such as name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Personnel Security Enterprise System (PSES): The DOT system that stores information regarding an Applicant's background investigation and final adjudication

Physical Access Control System (PACS): A system that controls an individual's ability to physically access the perimeter and interior space of DOT facilities.

PIV Card: See Personal Identity Verification Card.

PIV-I Card: See Personal Identity Verification Interoperable Card.

Public Key Infrastructure (PKI): A support service to the PIV system that provides the cryptographic keys needed to perform digital signature-based identity verification and to protect communications and storage of sensitive verification system data within identity cards and the verification system.

Reissuance: The process by which a new PIV Card is issued to a cardholder without the need to repeat the entire identity proofing and registration procedure. Reissuance occurs for PIV Cards when they are nearing expiration, lost, stolen, or damaged; when there is a change of employee status; or due to compromised logical credentials. If the chain-of-trust is broken or the reissuance process was not started before the current PIV Card expired, the identity proofing, registration, and issuance process must be repeated.

Security Operations Center (SOC): The 24-hour operations center where lost and stolen PIV cards are reported immediately or no later than18 hours after discovery.

Servicing Security Organization: In the context of this Order, the organization responsible for the ultimate oversight of an Applicant's background investigations and identification card issuance. For the Federal Aviation Administration, the servicing security organization is the

Office of Security, AIN-1, and its subordinate offices; for the rest of DOT, the DOT Office of Security is the servicing security organization.

Trusted Agent: A Trusted Agent is a person designated by an organization to perform Identity Registration/Registrar and/or Issuer duties, but may not perform adjudication functions.

Validation: The process of demonstrating that the system or entity under consideration meets, in all respects, the specifications of that system or entity.

APPENDIX B

DOT Order 1681.2A, DOT HSPD-12 and PIV Card Program

Acronyms

The following acronyms and abbreviations are used throughout this document:

CAC – Common Access Card, issued by the Department of Defense

CO - Contracting Officer

COR - Contracting Officer's Representative

CFR – Code of Federal Regulations

DOT - Department of Transportation

e-QIP - Electronic Questionnaire for Investigations Processing

ERO - Emergency Response Official

FAA - Federal Aviation Administration

FIPS - Federal Information Processing Standard

FICAM - Federal Enterprise Architecture publication, "Federal Identity, Credential, and Access Management"

GSA – General Services Administration

HSPD-12 - Homeland Security Presidential Directive 12

ICAM - Identity, Credential and Access Management

NACI - National Agency Check with Inquiries

NIST - National Institute of Standards and Technology

OMB - Office of Management and Budget

OPM - Office of Personnel Management

PACS - Physical Access Control System

PSES – Personnel Security Enterprise System

PIN - Personal Identification Number

PIV - Personal Identity Verification

PIV-I – Personal Identity Verification - Interoperable

PKI - Public Key Infrastructure

SOC – Security Operations Center

SP - Special Publication

APPENDIX C

DOT Order 1681.2A and DOT HSPD-12 PIV Card Program

ROLES

ROLES IN THE HSPD-12 PIV CARD PROGRAM

DOT has established Applicant, Sponsor, Registrar, Authorizer/Validator, Issuer, and the Trusted Agent as the primary roles in the PIV Card issuance process. Other key roles that support the PIV Card program are the OST/M-40 HSPD-12 Coordinator, the DOT Components HSPD-12 Coordinator, and the HSPD-12 PIV Sponsors.

1. The primary roles ensure a separation of duties in the issuance process so that a credential cannot be issued with an incorrect identity or to a person not entitled to obtain a credential. The Applicant, Sponsor, Registrar, Authorizer/Validator, Issuer, and Trusted Agent roles are mutually exclusive for the same Applicant. A member of a servicing security organization may perform multiple roles (e.g., a Registrar might also be an Authorizer/Validator or Issuer), but not for the same Applicant. An exception is that a Registrar may also serve as the Issuer for the same Applicant, but then may not act as an Authorizer/Validator for that Applicant.

2. The following primary roles shall support the issuance of PIV Cards. Prior to performing any of the roles, individuals shall complete the appropriate training for the role.

   a. Applicant

      A PIV Card Applicant is an individual who needs a PIV Card for access to DOT facilities or information systems as specified in this Order. Applicants shall complete all paper or electronic applications that may be required for processing a background investigation and/or a PIV Card, provide valid identity documents to establish their identity, and complete required training. Applicants shall be fingerprinted and photographed during the enrollment process.

   b. Sponsor

      Sponsors must be Federal employees who can substantiate the Applicant's need for a PIV Card and the Applicant's request. Generally, managers, supervisors, or human resources specialists act as sponsors for Federal employee Applicants. Contractor employee Applicants must be submitted by the contracting company and will be sponsored by a Contracting Officer (CO), the CO's Representative (COR), or a responsible Federal employee identified to the Registrar by the office that receives the contractor support as permitted by the DOT component's procedures. After successfully completing required training, Sponsors perform the following functions:

      (1) Verify an Applicant need for a PIV Card.

      (2) Verify the information that will be placed on the Applicant PIV Card.

(3) Indicate the facilities and information systems to which the Applicant is authorized to have access when known in advance.

(4) Request the issuance of a card for the Applicant.

(5) Request renewal or reissuance for current or previous cardholders.

(6) Identify whether or not the Applicant should have the Emergency Response Official (ERO) designation on his/her PIV Card in accordance with guidance issued by the Director of Security.

c. Identity Registration/Registrar

A Registrar may be a member of the servicing security organization or a Trusted Agent of the organization. Trusted Agents (see paragraph "f" below) are limited in the roles they may perform. After successfully completing required training, Registrars perform the following functions:

(1) Ensure Applicant has completed a PIV Card application.

(2) Ensure Applicant has successfully completed Applicant training.

(3) Check Applicant identity source documents for authenticity.

(4) Ensure the name and demographic data on the Applicant's PIV Card application and the individual's identity source documents are consistent.

(5) Capture the Applicant's photograph.

(6) Capture the Applicant's fingerprints.

(7) Input the details of the Applicant's identity source documents into the DOT Identification Management System (IDMS).

d. Authorizer/Validator

The PIV Card Authorizer or Validator shall be a Federal employee and a personnel security assistant or specialist in a servicing security organization. An Authorizer or Validator checks the information that was processed by the Registrar, and if all information collected is correct, the Authorizer or Validator approves the PIV Card production.[7]

After successfully completing required training, Authorizers or Validators shall check for existing background investigations for card Applicants and determine whether or not they have investigations meeting all current requirements for their employment at DOT.

[7] In automated systems, the approval for production of a PIV Card may be automatically transmitted to the production facility; or the approval may be passed to the card Issuer who would take an action to produce the card. An Authorizer or Validator may not approve the production of his/her own PIV Card.

(1) For Applicants who have favorably adjudicated background investigations meeting all current requirements:

(a) Review the PIV Card application, sponsor's approval, and results of identity proofing; and

(b) Authorize the production and issuance of a PIV Card.

(2) For Applicants who do not have background investigations meeting all current requirements, the Authorizer or Validator shall:

(a) Review all forms and electronic submissions.

(b) Adjudicate fingerprint results.

(c) Either directly or through the servicing security organization, initiate the required investigation.

(d) Record the results of an Applicant's Federal Bureau of Investigation National Criminal History Check and background investigation into the DOT Personnel Security Enterprise System (PSES).

(e) Review PIV Card application, Sponsor's approval, and results of identity proofing.

(f) Authorize the production and issuance of a PIV Card to the Applicant.

e. Issuer

An Issuer shall be a member of the servicing security organization and be a Federal employee or contractor who is appointed by the head of the servicing security organization. The Issuer receives PIV Cards from the production facility and distributes the cards to the Applicants. After successfully completing required training, Issuers shall perform the following functions:

(1) Secure and account for PIV Cards awaiting issue.

(2) Ensure that the photograph on the PIV Card matches the Applicant.

(3) Perform a 1:1 biometric match of the Applicant against the biometric included in the PIV Card or in the PIV enrollment record.

(4) Ensure the Applicant has selected a Personal Identification Number between six and eight numeric digits long.

(5) Deliver the PIV Card to the Applicant.

(6) Guide the Applicant through the card activation process to complete PIV Card issuance.

f. Trusted Agent

Each OST office or OA has one or more HSPD-12 representatives, also known as Trusted Agents. Trusted Agents may be designated by an organization to perform Identity Registration/Registrar and/or Issuer duties. A Trusted Agent may not perform adjudication functions. The Trusted Agent shall maintain, for each PIV Card issued, the documentary chain-of-trust data that include sequence of enrollment data records and any unique identifiers that have been acquired with the biometric matching of samples between enrollment data records. A Trusted Agent shall perform the following functions:

(1) Assist in implementing this Order.

(2) Follow the policy and guidelines issued by the DOT Privacy Officer in the Office of the CIO regarding privacy issues to maintain integrity of the chain-of-trust record.

(3) Complete required training.

(4) Serve as the OST or modal administration HSPD-12 Point-of-Contact.

(5) Attend quarterly HSPD-12 Coordinator meetings, or as needed.

(6) Maintain communications with Office of Security HSPD-12 Program Manager regarding policy changes.

(7) Contact the Office of Security HSPD-12 Program Manager promptly regarding changes pertaining to Trusted Agents, which may occur due to personnel changes or similar reasons when the former agent no longer performs Trusted Agent duties.

(8) Manage the PIV Card issuance process in accordance with the requirements of this Order, and with policy and procedures issued by the DOT Office of Security and FAA.

(9) Ensure PIV Cards have been authorized by the appropriate approvers.

(10) Revoke and destroy PIV Cards that are no longer needed due to employee separation for any reason.

(11) Revoke the PIV Card within 18 hours of notification that the PIV Card is lost, stolen, or compromised. In cases where 18 hours may represent an unacceptable delay, issue emergency notifications to inform the issuing office to cancel the card as rapidly as possible.

g. OST/Office of Security HSPD-12 Program Manager

The Office of Security HSPD-12 Program Manager shall: (1) lead the implementation of this Order; (2) receive information about changes pertaining to Trusted Agents, such as personnel changes when the former agent no longer performs Trusted Agent duties; and (3) keep the POC list updated.

The Office of Security HSPD-12 Program Manager serves as the DOT HSPD-12 Agency Security Officer and technical authority for the DOT HSPD-12 program and performs the following functions:

(1) Coordinates with each DOT Operating Administration (OA), Secretarial Offices, and Office of Inspector General to ensure HSPD-12 cards are issued to each employee and to contractors who need access to DOT facilities and IT systems.

(2) Coordinates with each DOT component to ensure that sufficient funds are available to purchase HSPD-12 cards for their respective employees and contractors.

(3) Serves as the DOT Liaison for the FAA HSPD-12 PIV Card Program.

(4) Prepares presentations, including budget reports, and briefs OAs on the status of the HSPD-12 program.

(5) Evaluates and monitors program effectiveness and recommends corrective actions and improvements.

(6) Performs special studies, research and evaluations to develop new policies and techniques to improve PIV Card security.

(7) Provides advice, guidance and direction to DOT on PIV Card policy interpretation and application, resolution of particularly difficult problems and situations, implementation and application of new techniques and systems, and other areas where assistance is required.

(8) Revokes and/or reactivates PIV Cards; audits and reports on Shared Services activities within DOT; and audits the physical destruction of PIV Cards at termination of cardholder employment.

(9) Establishes and maintains the HSPD-12 web site that provides training, registration and information for DOT Components, Sponsors, Trusted Agents, Employees, and Contractors, keeping information up to date and relevant to the DOT HSPD-12 program.

(10) Assists DOT Components in establishing Trusted Agent Field Sites.

(11) Manages the DOT Headquarters ID Media Center's Trusted Agents.

h. HSPD-12 Coordinators

The OST Program Coordinator and the Modal Program Coordinators serve as the HSPD-12 PIV Card managers for all DOT Components and perform the following functions:

(1) Follows the PIV issuance process that is outlined in DOT Order 1681.2A.

(2) Coordinates with Office of Security HSPD-12 Program Manager for the establishment of DOT Component Trusted Agent Sites.

(3) Identifies and selects DOT Component Trusted Agents.

(4) Maintains DOT Component Trusted Agents list and provide updates to the Office of Security HSPD-12 Program Manager.

(5) Purchases PIV enrollment products and equipment.

(6) Complies with policy and instructions as specified by the Director of Security regarding PACS and on-going card issuance guidance.

(7) Coordinates with OST Office of Security HSPD-12 Program Manager for Trusted Agent training and technical support.

i. HSPD-12 PIV Sponsor

The HSPD-12 PIV Sponsor serves as the designated DOT Component's Personnel Security Coordinator in approving employee and contractor PIV applications and performs the following functions:

(1) Completes Sponsor training, as needed.

(2) Ensures that the application queue is checked on a routine basis to ensure prompt processing of applications.

(3) Keeps abreast of the PIV issuance process that is outlined in APPENDIX D and the procedures promulgated by FAA and the Director of Security to obtain PIV Cards.

(4) Consults with the HSPD-12 Coordinators or the Office of Security HSPD-12 Program Managers concerning personnel security procedures.

(5) Consults with the Trusted Agents and prospective employees to fulfill requests for PIV Cards.

(6) Confirms that the Applicant is a valid DOT Component employee or contractor and meets the requirements to obtain a PIV Card.

APPENDIX D

DOT Order 1681.2A, DOT HSPD-12 - PIV Card Program

PIV CARD ISSUANCE PROCESS

The PIV Card issuance process shall follow the basic sequence listed below:

a. Application

The Applicant provides information necessary to establish his/her identity and to conduct a suitability investigation, e.g., fills out an online application for an identification card (DOT Form 1681, on-line version).

b. Sponsorship

A Sponsor nominates an individual for a PIV Card to the servicing security organization and enters basic information into an automated system. A Sponsor also approves the PIV application after it is completed by the Applicant.

c. Enrollment

The Applicant is notified to go to an enrollment center via a system-generated email. Applicants must bring with them two forms of approved identification as listed in FIPS 201-2. The Registrar at the enrollment center verifies the Applicant matches the descriptions on the identification documents, and then photographs and fingerprints the Applicant.

d. Authorization/Validation

The minimum background investigative requirement for HSPD-12 compliance is a National Agency Check with Inquiries (NACI). The Applicant shall be subject to the investigation that corresponds to the designation of the contract or position they will occupy according to OPM Position Designation standards. When an Applicant does not have an investigation on record that is at least a NACI, DOT may not issue a PIV Card until the Applicant has been fingerprinted and has provided all information, electronic submissions, and paperwork required to initiate the investigation. Electronic submissions include completion of the required investigative questionnaire via OPM's Electronic Questionnaires for Investigations Processing (e-QIP). The Applicant must also have a favorably adjudicated fingerprint check (criminal history records check) before DOT may issue a PIV Card. Retention of a PIV Card already issued is conditional upon favorable adjudication of the results of investigation.

e. Activation

The Applicant is notified the PIV Card is ready for activation/enablement and reports to an issuing office promptly where an Issuer verifies the printed information (including the photograph) and electronic information on the PIV Card match the Applicant. The

Applicant acknowledges receipt of the card, either electronically or on paper, and the Issuer then ensures the Applicant activates the PIV Card.

f. Enabling

If the PIV Card is not already enabled upon receipt by the Applicant, the Applicant will be required to undergo a step to promptly fully enable (store the certificates on) the PIV Card.