U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION
National Policy

ORDER 1600.78

Effective Date:

05/10/2010

SUBJ: Personal Identity Verification (PIV) Card and Other Identification (ID) Cards

1. Purpose of this Order. This Order provides basic policy governing all Personal Identity Verification (PIV) Card and other Identification (ID) Cards utilized by the Federal Aviation Administration (FAA). This order implements Department of Transportation (DOT) Order 1680.3, DOT Identification Media Program, and policies for the FAA Personal ID Verification (PIV) card as required by Homeland Security Presidential Directive 12 (HSPD-12). The Order identifies offices which have been delegated responsibility for issuing specific ID Cards used FAA-wide. Specific procedures for issuing ID Cards will be identified in supplementing Standard Operating Procedure Manuals.

2. Audience. All FAA employees, contractors, subcontractors and affiliates who require a PIV or other ID Cards for unescorted access to FAA facilities and/or access to sensitive information or resources. This order also applies to all relying agencies that obtain PIV cards from the FAA.

3. Where can I find this Order? The Order can be located on the My FAA Employee Site (FAA Intranet), Tools and Resources, Orders and Notices. Using the following link: https://employees.faa.gov/tools_resources/orders_notices/

4. Applicability. This Order implements DOT Order 1680.3, DOT Identification Media Program, supplemental Government-wide and DOT policies for the PIV card as required by Homeland Security Presidential Directive 12 (HSPD-12) and other applicable DOT directives. The Order identifies offices which have been delegated responsibility for issuing specific ID Cards used FAA-wide.

5. Authority to change this Order. The Assistant Administrator of Security and Hazardous Materials, ASH-1, will establish standards and procedures ensuring the integrity and security of the FAA-wide ID Card program, and as necessary may make changes to ensure compliance with applicable policies.

6. Authorities. Are listed in Appendix A of this Order.

7. Definitions. Are listed in Appendix B of this order.

8. Policy.

a. The FAA will issue PIV and other ID Cards to people who meet following criteria: (See Appendix C for PIV Card samples. See Appendix D for yellow, orange and Temporary ID Card samples).

(1) To individuals whose true identity we verify.

(2) To individuals who have a favorably adjudicated personnel security investigation which satisfies the standards of FIPS PUB 201-1, or some ID Cards (yellow or orange) may require only a favorably adjudicated FBI fingerprint check.

Note: The FAA can issue PIV or ID Cards to individuals who are awaiting the results of their personnel security investigations if the Servicing Security Element (SSE) has initiated their investigation and they have a favorably adjudicated FBI Fingerprint National Criminal History Check, and a waiver/interim suitability has been granted.

(3) When approved by a sponsor.

(4) To individuals who have a need for unescorted access to a FAA facility or certain areas within a FAA facility.

(5) Who present two acceptable and authentic identity source documents in original form, one of which must be a valid and unexpired Federal or State government picture ID (See Appendix E).

b. PIV Registrars will not accept fraudulent or altered identity source documents as being authentic. Registrars and Trusted Agents may question the validity of any source document presented by the applicant.

c. The FAA will not issue a PIV or ID Card to any person suspected by, or known to, the government as being a terrorist.

d. During PIV identity proofing and PIV or ID Card issuance, no substitution of one person for another can occur. Specifically, the person who applies for a PIV or ID Card, who presents identity source documents, who appears for identity proofing, whose fingerprints are checked against applicable databases, and to whom the FAA issues a PIV or ID Card must be the same person.

e. A qualified sponsor must approve requests for a PIV or ID Cards.

f. PIV or ID Cards must be immediately revoked when they expire or become invalid.

g. The system and procedures for issuing cards shall ensure that a single corrupt official in the process does not have the ability to issue a PIV or ID Card to a person not entitled a PIV or ID Card.

h. FAA issued PIV or ID Cards shall not be modified, duplicated, or forged. Identification media issued by the FAA remains the property of DOT/FAA and is issued for official purposes and identification only. Improper use, possession, counterfeiting or alterations is subject to penalties under Title 18, United States Code 499, 506, and 701 as well as FAA administrative and disciplinary sections.

i. The FAA handles personal information collected for PIV or ID Card purposes consistent with the Privacy Act of 1974.

j. Notice of Exception or Noncompliance in accordance with FAA Order 1600.78 are subject to actions in accordance with existing policy and regulations applicable union contracts and/or Human Resources Policy Management Employee Relations 4.1, Standards of Conduct and the accompanying Human Resources Operating Table of penalties. The FAA will enforce the use of penalties against any user who violates the FAA or Federal system security policy or order as appropriate.

9. Authorized PIV ID Card Roles. PIV Certification and Accreditation Roles.

(1) Senior Agency Official (SAO). The SAO is the FAA's senior official who is responsible for establishing, financing, and overseeing the PIV functions and services for the FAA. The Assistant Administrator for Security and Hazardous Materials, ASH-1, serves in this role.

(2) Designated Accreditation Authority (DAA). The DAA is a senior official with the authority to formally accredit the reliability of the FAA's PIV Card Issuer (PCI). The Deputy Assistant Administrator for Security and Hazardous Materials, ASH-2, serves in this role.

(3) FAA Identity Management Official (FIMO). The FIMO ensures that FAA PIV or ID Card services are reliable and that FAA produces and issues PIV Cards as FIPS PUB 201-1 specifies. The Director, Office of Security, AIN-1, serves in this role.

(4) Assessor Agent and Team. The Director of Field Operations, AHS-1, is the Certification Agent. A third party certification team under contract with the FIMO certification and accreditation services assists AHS-1.

(5) ASH PIV Card Issuer (PCI) Manager. The Manager, AIN-620, serves in this role.

(6) PIV Card Issuer Facility (PCIF) Manager. Region and Center 700s and AIN-610 serves in this role.

(7) PIV Card Applicant's Representative. Acts as a resource for sponsors, employees and contractors who are applying for or who have PIV or ID Cards. For Headquarters, AIN-10, Program Support Staff serves in this role. In Regions and Centers, the Region or Center 700 will appoint persons to serve in this role. The Applicant Representative assists with:

(a) Denial of PIV Card

(b) Revoked PIV Card

Note: If there is a decision to deny or revoke an Applicants PIV card, the Applicant will be given an opportunity to provide information to clarify or explain any derogatory information, either in writing or via interview. If the derogatory information cannot be favorably resolved, the PIV card will be denied or revoked. The SSE will provide the person with information regarding how to appeal the denial or revocation decision, if they choose. The SSE will establish a file to maintain documentation supporting the reason for denial or revocation of the PIV card. This file will be forwarded to the Director, Office of Security, AIN-1.

(8) Agency Official for Privacy (AOP). The FAA Privacy Officer, AES-200, serves in this role.

10. Responsibilities. The Assistant Administrator of Security and Hazardous Materials, ASH, will establish standards and procedures ensuring the integrity and security of the FAA-wide ID Card program. Changes in standards or procedures will be addressed by the Office of Security, AIN, who will carry out the responsibilities listed in subparagraphs a, d, e and f below. The list is not intended to be all inclusive.

a. The Director, Office of Security, AIN, is responsible for:

(1) Coordinating with the Office of the Secretary of Transportation (OST) Office of Security, M-40, on matters pertaining to the design and implementation of ID Cards used by the FAA.

(2) Developing national standards and procedures governing the FAA-wide ID Card program.

(3) Developing required training for Applicants, Sponsors, Registrars and Issuers (to include Trusted Agents). Note: Each SSE will be responsible for monitoring training within their respective region.

(4) Providing guidance and assistance FAA-wide to offices concerning the acquisition of new forms and/or changes to existing forms of ID Card.

(5) Monitoring and periodically inspecting procedures through program evaluation pertaining to procurement, printing, issuance, accountability, and control of PIV and ID Cards utilized by FAA employees, contractors, or affiliates.

b. Applicant. An individual who needs a PIV or other ID Card for access to FAA facilities or information systems. PIV Cards will be issued to FAA employees, contractors, or affiliates who require access for 6 months or longer. PIV and ID Card applicants are responsible for:

(1) Completing applicant training.

(2) Providing basic demographic data for the PIV or Identification Card.

(3) If needed, completing paperwork for a personnel security background investigation.

(4) Providing their photograph and fingerprints during face-to-face enrollment.

(5) Presenting valid, unexpired and acceptable source documents during enrollment.

(6) Personally picking up their PIV Card. The PIV Card must be activated at a CMS Activation Station. Non-PIV ID Cards can be picked up personally. When distance is involved, the ID Card may be sent via registered mail, FedEx, or courier. Couriers may be other FAA employees. When this option is used the ID Card shall be placed, by the issuing office, in a sealed package.

(7) Properly safeguarding, handling and using their PIV or ID Card once issued, including return of PIV or other ID Card upon resignation, termination or upon request.

c. Sponsor. Sponsors are FAA managers or employees who verify an applicant's need for a new, or renewal of an existing, PIV or ID Card. Generally, managers and supervisors sponsor FAA employees and affiliates. Contracting Officers (CO), or Contracting Officer's Technical Representatives (COTR), will normally sponsor FAA contract employees. Sponsors must be Federal employees designated by management and may not perform other card issuance roles for the same applicant. Sponsors are responsible for:

(1) Completing required sponsor training.

(2) Changing, approving, or disapproving a request for a PIV or ID Card to include re-issuances and/or revocations.

(3) Verifying applicants information for PIV or ID Card.

(4) Recommends enrollment changes to local SSE for revocation or suspension of applicants they sponsored.

d. Registrar. Registrars are responsible for identity proofing and enrollment of an applicant. The individual who performs the registrar role may also perform the Issuer/Delivery role in the PIV or ID Card issuance process for an applicant. However, they may not perform any other card issuance roles for the same applicant. Some of these processes may be performed by a Trusted Agent of the Registrar, however, generally a designated Personnel Security Specialist (PSS) may approve an ID Card. Registrars are responsible for:

(1) Taking required Registrar training.

(2) Capturing fingerprints and photograph for PIV and ID Card applicants.

(3) Checks identity source documents for authenticity (questionable identity source documents will be validated through Docutector). Relevant details of the identity source documents will be stored in the Card Management System (CMS).

(4) Compares name and demographic data between the application and identity source documents.

e. Authorizer/Validator. The PIV authorizer/validator is a Federal employee, generally a PSS. The individual performing this role may not hold any other card issuance role for the same applicant in the PIV or ID Card process, nor may they approve their own PIV or ID Card. Authorizers are responsible for:

(1) Reviewing, verifying and adjudicating background investigations to include verifications of prior background investigations, recording results of these investigations in Investigations Tracking

System (ITS) and on favorable adjudications, authorizing production and issuance of a PIV or ID Card for a given applicant.

(2) Initiating the applicant's background investigation submission process through the Office of Personnel Management's Electronic Questionnaires for Investigations Processing (e-QIP).

(3) Choosing the type of ID Card in ITS based on the type of appointment.

f. Issuer. The PIV Issuer is the individual that issues and personalizes the PIV or ID Card to the applicant after all identity proofing, background checks, and approvals are completed. Issuers are responsible for:

(1) Taking the required Issuer training.

(2) Delivering card to applicant for activation.

(3) Providing assistance/guidance to Applicant at time of activation.

(4) Securing and accounting for PIV or ID Cards, by preventing unauthorized access, before issuance to the Applicant in accordance with latest version of FAA Order 1600.69.

(5) Delivering the card to the applicant to complete the PIV or ID Card issuance process. Deactivates PIV Cards not delivered within 90 days, unless an exception has been granted.

11. Authorized ID Cards, Forms, and PIV Card Sleeve/Holders.

a. Only DOT/FAA ID Cards described below are specifically authorized for use throughout the FAA. Regions and Centers shall not issue other ID Cards without appropriate coordination as required by this order. No badges, miniature emblems, sticker, ribbons, etc., may be affixed to any DOT/FAA ID Card.

(1) 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 person (human readable and verifiable) or an automated process (computer readable and verifiable). Issued to employees and contractors employed for more than 6 months. See Appendix C for sample PIV Cards.

(2) Yellow ID Card. SSEs are responsible for the printing of Yellow ID Cards. See Appendix D for sample and further information.

(3) Orange ID Card. SSEs are responsible for the printing of Orange ID Cards. See Appendix D for sample and further information.

(4) DOT Green Employee and Blue Contractor ID Cards are being phased out. However such cards will be acceptable forms of ID until replaced by PIV Cards or Other ID Media issued pursuant this Order.

b. An Automated Application Form will be used to apply for all ID Cards. This automated form includes applicant training to ensure applicants are aware of their responsibilities in handling their ID Card. This form will be used in lieu of DOT Form 1681, Application for Credential or ID Card. Individuals with paper application forms will be assisted in completing the automated form when they appear for registration.

c. FIPS Pub 201-1 requires that PIV biometric and other data is protected from contactless access. PIV Cards are required to be kept in an electromagnetically opaque sleeve/holder or other technology meeting FIPS Pub 201-1 requirements to protect against any unauthorized contactless access to information stored on PIV Cards. FAA Employees and Contractors will only use sleeves/holders provided by AIN.

12. ID Card Design and Topology.

a. FIPS Pub 201-1, NIST Special Publication 800-104, and DOT policy memorandum, PIV ID Card Format, February 1, 2008, strictly control the design and topology of FAA PIV Cards. These policies and guidance permit the FAA some design flexibility where the FAA can place FAA specific data on the PIV Card. FAA issued PIV Cards are identifiable across the Federal government and can be authenticated electronically.

(1) FAA Identification Media (PIV and Yellow non-PIV Cards) normally will not bear any external markings which make them site-specific nor will they have designators on the exterior of the card which identify the holder as being authorized to enter specific buildings, closed or controlled areas or restricted zones, within a larger FAA Campus or Facility.

(2) Limited exceptions for up to three years duration may be issued which will allow the temporary issuance and use of ID Media bearing site specific geographic or closed/controlled area identifiers for specific facilities may be issued by the Director, Office of Security, based upon a request from the facility manager, providing adequate justification. Such request must be submitted through the Servicing Security Element (Axx-700) with a recommendation for approval/disapproval to FAA Internal Security Division Manager (AIN-100) and will continue in effect only as long as the justifying circumstances continue or for up to three (3) years, whichever is shorter. Extensions beyond three (3) years may be granted if justified.

(a) Large NAS Air Traffic Control Operational Facilities pending Physical Access Control System Upgrades are one category of FAA facilities which may be eligible for exceptions under paragraph 2. Criteria:

i. Large Air Traffic Control Towers, ATCT, Terminal Radar Approach Control Facilities, TRACON, Air Route Traffic Control Center, ARTCC or similar facility.

ii. Unescorted access through one or more perimeter gates, doors or portals is normally limited to locally assigned FAA federal or contract personnel.

iii. Such gate, door or portal is guarded with the inspection of ID media being a critical element in determining if the individual is locally assigned.

iv. No automated or other efficient alternative method of identifying locally assigned personnel is available; (New automated PACS systems have not yet been installed).

v. Facility manager has requested authority to use three letter site identifier codes on PIV and/or yellow cards in writing.

vi. Axx-700 (SSE) has verified the justification offered by the facility manager, and both Axx-700 and AIN-100 have approved/disapproved the request.

(b) Other types of sites and situations may be granted exceptions to policy based upon a similar process (written request by facility manager, adequate justification, facts verified by Axx-700, approval/disapproval recommended by Axx-700 and approved by AIN-100) where circumstances warrant.

Note: Additionally in cases other than those envisioned under paragraph 2.a. above, the technical and procedural feasibility of the requested exception must also be evaluated by AIN-600 (Identification Media Technical Implementation Branch and ID Media Operations and Policy Branch) before approval. The SSE will be notified by AIN-600 when the necessary software has been provided to the site in question and necessary software changes have been made to allow the assignment of the three letter designator during the card enrollment process.

b. All other requests for non DOT/FAA standard ID Cards must be coordinated with AIN for review and approval.

13. Post-Issuance Events. Over the course of a PIV or ID Card's lifecycle, there are post-issuance events. Each of these events requires action by the cardholder, the cardholder's sponsor, the registrar, and the issuer. Post-issuance events may also require a cardholder to appear in person at places designated by AIN or regional SSE for identity proofing, to receive a new PIV or ID Card, or to update a current card. In some cases, a cardholder may have to repeat the full registration process including completing a PIV or ID Card application to request the card in each instance.

a. Renewal:

(1) Renewal occurs before a PIV or ID Card expires with repeat of the full registration process. Failure to renew a PIV or ID Card prior to expiration may result in confiscation of the expired ID.

(2) Before renewing the card, the SSE will verify that the cardholder has a current background investigation and that the cardholder's personnel security (ITS) and CMS records are accurate.

b. Re-issuance.

(1) SSEs will reissue PIV or other ID Cards when a card has expired, or when a card is lost, damaged, stolen, or compromised. SSEs will also reissue PIV or other ID Cards when a Cardholder's status changes and the change requires a new look on the PIV or ID Card, such as a name change.

(a) Lost. A lost PIV or ID Card is defined as a card that is missing beyond three (3) days after notification to a SSE. During the three day waiting period applicant will be required to sign in daily with the guard desk. A card which is lost requires the submission of an Incident Report to AIN or their local SSE within 48 hours of the detected loss. The Automated Lost/Stolen ID Form can be used to report the incident. The three day waiting period may be waived under certain circumstances.

(b) Damaged. A damaged PIV Card is defined as a card that is physically or electronically unreadable. The Cardholder's damaged card must be provided to the SSE before a new PIV or ID Cards can be re-issued.

(c) Stolen. Stolen PIV or ID Cards must be reported to the nearest SSE immediately and revoked. Stolen PIV Cards require the submission of an Incident Report to AIN or the local SSE within 48 hours of the detected theft. The Automated Lost/Stolen ID Form can be used to report the incident.

(d) Compromised. A compromised PIV Card is defined as the successful unauthorized use of a card without the true Cardholder's intention to use the card. Compromised PIV Cards must be reported to the nearest SSE and revoked.

(2) Lost or stolen PIV and ID Cards Incident Reports will normally require a three (3) day wait period before a new PIV Card can be processed or an ID Card reissued. Cards that are recovered during this three day period must be reported to AIN, local SSE or the SSE where the Incident Report was originally submitted.

(3) Before a PIV or ID Card can be reissued the previous PIV Card must be revoked and the cardholder must repeat all applicable registration steps.

c. All PIV and ID Cards that are returned, upon expiration, resignation, termination or upon request must be destroyed to prevent reconstruction or use of card.

14. FAA PIV Standard Operating Procedures (SOP). The SOP provides detailed instructions for the issuance of the PIV or ID Card and will be used to meet the control and security objectives set in HSPD-12. The SOP also provides detailed instructions for processing yellow and orange ID Cards and can be found at https://ash.1.faa.gov/apps/infocenter/hspd12.aspx. The SOP contains specific details such as:

a. Application Procedures

b. Sponsorship Procedures

c. Registration Procedures

d. Adjudication Procedures

e. Delivery Procedures

f. Activation Procedures
g. Maintenance Procedures

h. List of Acceptable Identity Proofing Documents

i. "Docutector" Web Portal Instructions (validation of identity documents)

j. Due Process and Appeals Procedures (denials of PIV or ID Cards)

k. Procedures for issuing yellow and orange ID Cards

15. Privacy Act System of Records. All FAA ID Cards fall under a system of records published in the Federal Register, DOT/OST 018, entitled: ID Card Records System. Under the Privacy Act all ID Cards and applications described in FAA Orders 1280.1, Protecting Personally Identifiable Information and 1600.75 Protecting Sensitive Unclassified Information is protected. Each facility processing ID Cards must display a copy of the Privacy Act Notice shown in Appendix E. The notice is poster size (27 X 20), inches and shall be displayed in an obvious place within the PIV Card processing area. AIN is responsible for supplying the Privacy Act Notice.

Claudio Manno
Assistant Administrator for
Security and Hazardous Materials

Appendix A. List of Authorities

a. Homeland Security Presidential Directive 12 (HSPD-12)

b. Office of Management and Budget (OMB) Memo M-05-24, of August 5, 2005, Implementation of HSPD-12 Policy for a Common ID Standard for Federal Employees and Contractors

c. Federal Information Processing Standards Publication 201-1 (FIPS-201-1), Personal Identity Verification of Federal Employees and Contractors

d. National Institute of Standards and Technology (NIST) Special Publication 800-79-1, Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers (PCI's)

e. NIST Special Publication 800-104, A Scheme for PIV Visual Card Topology

f. Office of Personnel Management (OPM) Memorandum of July 31, 2008, Final Credentialing Standard for Issuing Personal Identity Verification Cards Under HSPD-12

g. Department of Transportation Order 1680.3, DOT Identification Media Program

h. DOT Memorandum of May 24, 2006, Requirements for Issuing ID Cards Meeting the Standards of Homeland Security Presidential Directive 12

i. DOT Memorandum of February 1, 2008, Updated DOT PIV ID Card Format

j. DOT Memorandum of May 31, 2007, Visual Security Device for DOT ID

k. FAA Order 1600.1E, Personnel Security Program

l. FAA Order 1600.72, Contractor and Industrial Security

m. FAA Order 1280.1, Protecting Personally Identifiable Information (PII)

n. FAA Order 1600.69B, FAA Facility Security Management Program

o. FAA Order 1600.75, Protecting Sensitive Unclassified Information (SUI)

Appendix B. Definitions

Access Control System: The system that controls an individual's ability to access a physical location and/or computer system resources.

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, a determination regarding the individual's fitness for access to DOT facilities, sensitive information, resources, and/or information technology systems.

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 scan samples 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 in terms of some characteristic (e.g., patterns).

Capture: The method of taking a biometric sample from an end user.

Cardholder: An individual possessing an issued FAA PIV card.

Certification: The process of verifying the correctness of a statement or claim and issuing a certificate as to its correctness.

Certification and Accreditation: The process to insure that an information system meets and maintains documented security requirements.

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 binds an identity (and, optionally, additional attributes) to that individual.

e-QIP: Electronic Questionnaires for Investigations processing (e-Qip)

Federal Information Processing Standards (FIPS): A standard for adoption and use by federal departments and agencies that has been developed within the Information Technology Laboratory and published by NIST, a part of the U.S. Department of Commerce. A FIPS covers some topic 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.

Identification Management System (IMS): The DOT 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.

Identity Proofing: The process of providing sufficient information (e.g., identity history, credentials, documents) to a PIV Registrar when attempting to establish an identity.

Identity Registration: The process of making a person's identity known to the PIV system, associating a unique identifier (ex.; 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 (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the DOT PIV card or system and associated with the identity being claimed.

Investigation Tracking System (ITS): The DOT system that stores information regarding an applicant's background investigation and final adjudication.

Logical Access Control System (LACS): The system that controls an individual's ability to access computer system resources.

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

National Agency Check with Inquiries (NACI): The minimum level background investigations required by HSPD-12 in order to obtain a PIV Card.

Personal Identification Number (PIN): A secret number that a claimant memorizes and uses to authenticate his or her identity. PINs are generally only decimal 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 person (human readable and verifiable) or an automated process (computer readable and verifiable).

Personnel Security Specialist: An individual in the Servicing Security Element who conducts security adjudication.

Physical Access Control System (PACS): The system that controls an individual's ability to access a physical location.

Privacy Impact Assessment (PIA): A PIA is an analysis of how personally identifiable information is collected, used, disseminated, and maintained. "Personally identifiable information" is defined as any information that permits the identity of an individual to be directly or indirectly inferred. The purpose of a PIA is to demonstrate that privacy protections have been incorporated throughout the development life cycle of a system or program.

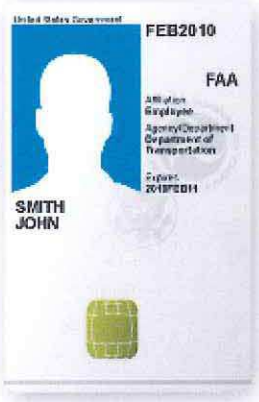
Servicing Security Element: In the context of this order, the security element that is responsible for the ultimate oversight of Applicants' background investigations and identification card issuance.

Trusted Agent: A non-ASH employee or contractor that performs the duties of a Registrar and/or Issuer in the PIV ID Card process.

Appendix C. PIV Samples

SMART CARD ENABLED FAA AUTHORIZED ID CARDS

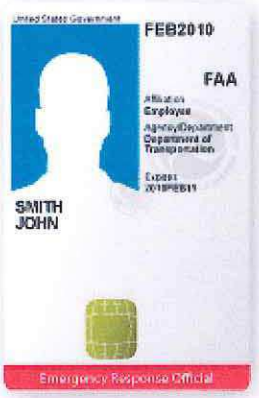
Authorized FAA ID Cards issued on a Smart Card. Sponsor has determined ID Card Holder will require a smart card for logical and electronic physical access.



FAA PIV Government Employee ID Card

FAA PIV Contractor Employee ID Card

FAA PIV Foreign National Government/ Contractor Employee ID Card



FAA PIV Emergency Response Official (ERO)

Authorized Back of Smart Card ID

Appendix D. Yellow/Orange Matrix

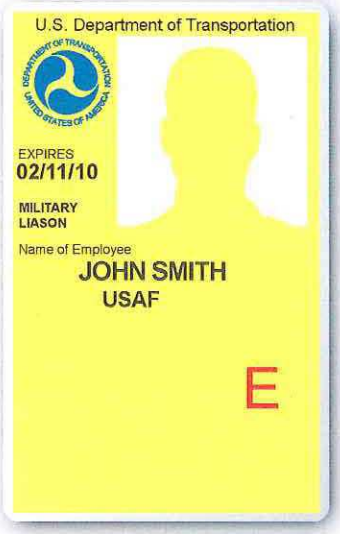
August 25th, 2009

FAA IDENTIFICATION CARD MATRIX

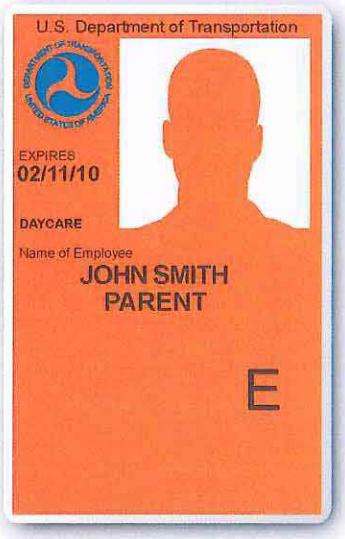
YELLOW

Only to be issued to individuals requiring access to multiple facilities or a single facility and whose access is not restricted to certain areas of that facility. The following guidelines are provided to determine if a yellow ID Card should be issued to an individual:

- Expectation of Employment is less than 6 months for an FAA employee or FAA contractor. For some contractors or non-employees, the card may be issued for up to 3 years.
- Minimum Fingerprint Check Required.
- If they have the minimum of a favorably adjudicated NACI they are authorized to escort employees and will receive a red "E" printed on their card to designate the requirement.
- They may or may not be restricted to a single facility. If they are restricted to a single facility, then they must have the Location ID and Facility Type on their card.
- Card may also be issued as a Temporary card to employees pending issuance of a PIV Card. Expiration on a Temporary Card cannot exceed 30 days.
- Examples may include: Military Liason, GSA Contractors, Summer Hires/Interns, ATC Students, construction workers, or cafeteria workers



ORANGE



Only to be issued to individuals requiring access to a single facility and whose access is restricted to certain areas of that facility. If they have the minimum of a favorably adjudicated NACI then they are authorized to escort employees and will receive a black "E" printed on their card to designate the requirement. The following guidelines are provided to determine if an, orange ID Card should be issued to an individual:

- Limited Access within the Facility.
- Single Facility Only.
- Minimum Fingerprint Check Required.
- Location ID and Facility Type must be printed on the ID.
- Expiration date is NTE 1 year.
- Examples may include: Credit Union Employees and other individuals not requiring an HSPD-12 PIV ID Card or Yellow ID Card and whose access needs to be restricted.

Appendix E. Identity Source Documents

Acceptable Form of Identification

The list below identifies the acceptable documents that a PIV Applicant must bring at the time of identity proofing and registration.

The PIV Applicant must bring two of these documents, one of which must be a Federal or State-issued photo identification.

The documents must be originals.

Primary Forms of Identification	
1. FAA ID Badge	12. Military dependent's ID card
2. U.S. Passport (unexpired)	13. U.S. Coast Guard Merchant Mariner Card
3. Permanent Resident Card or Alien Registration Receipt Card (Form I-551)	14. Native American tribal document
4. An unexpired foreign passport with a temporary I-551 stamp	15. Driver's license issued by a Canadian government authority
5. An unexpired Employment Authorization Document that contains a photograph (Form I-766, I-688, I-688A, I-688B)	16. U.S. Social Security card issued by the Social Security Administration (other than a card stating it is not valid for employment)
6. An unexpired foreign passport with an unexpired Arrival-Departure Record, Form I-94, bearing the same name as the passport and containing an endorsement of the alien's nonimmigrant status, if that status authorizes the alien to work for the employer	17. Certification of Birth Abroad issued by the Department of State (Form FS-545 or Form DS-1350)
7. Driver's license or ID card issued by a state or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address	18. Original or certified copy of a birth certificate issued by a state, county, municipal authority or outlying possession of the United States bearing an official seal
8. ID card issued by federal, state or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address	19. U.S. Citizen ID Card (Form I-197)
9. School ID card with a photograph	20. ID Card for use of Resident Citizen in the United States (Form I-179)
10. Voter's registration card	21. Unexpired employment authorization document issued by DHS
11. U.S. Military card or draft record	For persons under age 18 who are unable to present one of the documents listed above:
	• School record or report card
	• Clinic, doctor or hospital record
	• Day-care or nursery school record

08/17/2009

Appendix F. Privacy Act Notice

U.S. Department of Transportation
Federal Aviation Administration

U.S. Department of Transportation
Federal Aviation Administration
ID Proofing and Registration Privacy Act Statement

What is the Personal Identity Verification (PIV) Card?
You are being issued a PIV card that is one part of a system for protecting federal buildings, computers, applications, and data. This is a secure and reliable card based on your verified identity. It is extremely hard to fake, change, or duplicate. It is only issued by accredited employees. If you previously had a government badge, the PIV Card replaces your badge.

What is the Authority for the PIV Card Program?
Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors. The directive can be reviewed at:
http://csrc.nist.gov/drivers/documents/Presidential-Directive-Hspd-12.html.

Why do I need a PIV Card?
Common to all federal agencies, the PIV card is a way for you to prove that you are who you claim to be. We issue PIV cards to reduce identity fraud, protect your privacy, save time, and improve security through a standardized process. As part of this process, the U.S Government conducts a background investigation on you to decide whether you are suitable for your job and eligible to use the buildings, computers, applications and data. The investigation, along with information from the office that hired you, is used to verify your identity, create a PIV card for you, and create a record that you have been issued a card.

What Information Is Stored in the System About Me?
We keep the following information in our records: your full name, facial color photograph, two fingerprints, date of birth, home address, home phone number, your background investigation form, the results of your background check, the approval signature of the person who registers you in the system, your PIV card expiration date, the PIV card serial number, and copies of the documents you used to verify your identity, such as your driver's license or passport.

What Information is Stored on the PIV Card?
The card itself displays a digital color photograph of your face, your full name, agency, organization, a stripe for foreign nationals, card expiration date, card serial number, and an issuer identification number. The card also stores a Personal Identification Number (PIN), a unique identifier, a PIV authentication key, and two electronic fingerprints.

How Will My Information Be Used?
DOT and other agencies will use the information on the PIV card and may use some of the stored information about you when you access federal facilities, computers, applications, or data to prove your identity and your right of access. [Your information will be used after you leave DOT applications, or data to prove your identity and your discontinuance of access to DOT applications or data.] After you leave DOT we keep this information according to the National Archives General Records Schedule. After that time, if it is not needed for security reasons, or to investigate improper behavior, we destroy it.

Who Will See My Information?
Information about you that we store to issue you a PIV Card and run the program may be given without your consent permitted as the Privacy Act of 1974 (5 U.S.C. § 552a(b)) and to the appropriate government organization if your records show a violation or potential violation of the law; to the Department of Justice, a court, or other decision-maker when the records are relevant and necessary to a law suit; to a federal, state, local, tribal, or foreign agency that has records we need to decide whether to retain an employee, continue a security clearance, or agree to a contract; [to a Member of Congress or to Congressional Staff at your written request] to the Office of Management and Budget to evaluate private relief legislation; to agency contractors, grantees, affiliates, or volunteers, who need access to the records to do agency work and who have agreed to comply with the Privacy Act; to the National Archives and Records Administration for records management inspections; and to other federal agencies to notify them when your card is no longer valid.

System of records notices that pertain to this system are DOT/ALL 9 Identification Media Record Systems; DOT/ALL 13 Intranet activity and Access Records; DOT/FAA 815 Investigative Record System DOT/OST 035 Personnel Security Record System. A complete description of the routine uses has been published in the Federal Register and can be viewed at: http://www.dot.gov/privacy/privacyactnotices/

What Happens if I Don't Want a Card?
While there is no legal requirement to use a PIV Card, if you do not give us the full information we need, we may not be able to create your record and complete your identity check, or complete it in a timely manner. If you do not have a PIV card, you will be treated as a visitor when you enter a federal building. You will not have access to certain federal resources. If using a PIV card is a condition of your job, not providing the information will affect your placement or employee prospects.

Where Can I Get More Information About the PIV Card Program?
If you have questions or concerns about the use of your information, you may contact the FAA Privacy Officer Carla Mauney, 800 Independence Ave., SW, Washington DC 20591, (202) 267-9895 or email at Carla.Mauney@faa.gov. Further information is available on the FAA website at www.faa.gov/privacy/