To enhance mission performance, TSA is committed to promoting a culture founded on its values of Integrity, Innovation, and Team Spirit.

REVISION: This revised directive supersedes TSA MD 2800.16, *Identification Media and Access Control Program*, dated October 20, 2015.

SUMMARY OF CHANGES: Section 6.I, removed the requirement for Accountable Property Officers to hold and maintain a Secret security clearance.

1. **PURPOSE:** This directive provides TSA policy and procedures for TSA identification media and access control standards and requirements designed to protect TSA facilities, personnel, and assets from unlawful acts.

2. **SCOPE:** This directive applies to all TSA employees and contractors.

3. **AUTHORITIES:**

   A. Title 41, CFR, Part 102-74, *Facility Management*, and Part 102-81, *Security*

   B. DHS Delegation 12000, *Delegation for Security Operations within the DHS*

   C. DHS Directive 121-01, Revision 01, *Office of the Chief Security Officer*

   D. DHS Directive 121-03, *Common Identification Standard for DHS Employees and Contractors*

   E. DHS Instruction Manual 121-01-010-01, Revision #01, *Physical Security*

   F. Federal Information Processing Standards Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*

   G. Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*

   H. TSA MD 1100.73-5, *Employee Responsibilities and Code of Conduct*

   I. TSA MD 2800.71, *Pre-Employment Investigative Standards for TSA Non-Screener Employees and Contractors*

4. **DEFINITIONS:**

   A. Access: Authorization for TSA personnel and contractors who have been issued an official form of TSA identification media that permits unescorted access into TSA-controlled facilities.

   B. Access Control Program: Designed to prevent loss of TSA property and material, provide for the protection of employees and contractors, as well as minimize potential breaches of security by

limiting access to only those individuals possessing legitimate reasons to enter TSA-controlled facilities.

C. Accountable Property Officer (APO): The individual responsible for the accountability and control of personal property within his or her jurisdiction. The responsibility may be a collateral duty designated to an individual with a different title within the organization.

D. Identification Media: Photographic access cards that identify the individual as having been authorized for both physical and logical (i.e., electronic) access to TSA-controlled facilities and property.

E. National Capital Region (NCR): TSA locations and facilities located within 50 miles of Washington, DC.

F. Personal Identity Verification (PIV) Card: A security access card used to identify the cardholder as a Federal employee or contractor, to obtain unescorted access to TSA facilities, and to gain access to TSA information systems such as e-mail and network access when approved equipment is deployed for use throughout the agency.

G. TSA-controlled Facility: A building, area, room, or leased space, whether for single or multitenant occupancy, and its grounds and approaches, all or any portion of which is under the jurisdiction, custody, or control of TSA. It includes TSA-controlled commercial space shared with non-government tenants; TSA-owned contractor-operated facilities; and facilities under a management and operating contract, such as for the operation, maintenance, or support of a Government-owned or controlled research, development, special production, or testing establishment.

H. TSA Personnel: Persons permanently or temporarily assigned, attached, detailed to, employed by, or under contract with TSA (including student volunteers and foreign nationals).

I. Visitors: Individuals who are not employed by or under contract to TSA, including vendors, suppliers, business representatives, state and local government employees, other Federal Government employees, and members of the general public.

5. RESPONSIBILITIES:

A. Assistant Administrators and equivalents are responsible for ensuring that subordinate organizations comply with DHS and TSA policy and procedures related to TSA identification media and access control.

B. The Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) Security Services and Assessments Division (SSAD) Chief Security Officer (CSO) is responsible for:

(1) Developing and implementing the *Identification Media and Access Control Program* through the establishment of standards and requirements as set forth in this directive and Handbook.

(2) Overseeing the *Identification Media and Access Control Program* for TSA facilities in the National Capital Region and field Organizational Elements (OEs), including conducting periodic audits of identification media and access control policies and procedures to ensure compliance with the provisions of HSPD-12, applicable DHS/TSA directives, and current Standard Operating Procedures (SOP), handbooks, or other supplemental materials.

(3) Conduct a nationwide audit of PIV Cards issued to TSA employees and contractors once a year to ensure accuracy of cards issued and to ensure personnel who have separated from TSA have had their PIV Cards revoked.

C. Federal Security Directors (FSDs), Supervisory Air Marshals in Charge (SACs), and equivalents are responsible for ensuring that their personnel comply with standards and requirements set forth in this directive and supplementary guidance.

D. SSAD Physical Security Section Unit Chiefs are responsible for:

(1) Identifying, via memorandum, one primary and one alternate for each TSA controlled facility to serve as the Access Control Liaison responsible for all matters relating to access control for personnel; and

(2) Providing day-to-day oversight of the security guards located at their respective locations.

E. Access Control Officers or the responsible program officials are responsible for:

(1) Implementing access control requirements within their areas of responsibility;

(2) Providing for the protection of employees, contractors, and visitors, as well as minimizing potential breaches of security by limiting access to only those individuals needing to enter the facility; and

(3) Ensuring that individuals who enter open storage areas for classified information or other sensitive areas are briefed and clearly understand access control procedures and measures to protect classified national security information.

F. Accountable Property Officers are responsible for:

(1) The accountability of identification media and access control issued to personnel in accordance with procedures set forth by their respective Organizational Element Issuing Office.

(2) Maintaining local records for the storage, issuance, control, accountability, retention, return, destruction, or disposition of PIV cards and access control media (e.g., keys) under their area of responsibility, and complying with audits and inspections, as required, by this and other TSA and/or DHS directives.

G. TSA personnel and contractors are responsible for complying with all requirements for the proper use, display, and control of TSA-issued identification media and any other types of access control media in accordance with standards and requirements established by TSA policy, including this directive, and the associated Handbook. In accordance with the Handbook to TSA MD 1100.73-5, *Employee Responsibilities and Code of Conduct*, "Employees will use official (TSA or DHS issued or authorized) identification media only for official or other permissible purposes… Applicable requirements and restrictions include, but are not limited to, a prohibition against allowing another individual to use an employee identification badge, a requirement to

wear, and visibly display an employee identification badge while on duty, and a prohibition from facility access during non-duty hours unless authorized."

6. POLICY: HSPD-12 requires that the Federal executive departments and agencies issue secure and reliable forms of identification to their employees and contractors. Identification cards must be issued based on sound criteria for verifying an individual's identity; strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; able to be rapidly authenticated electronically; and issued only by providers whose reliability has been established by an official accreditation process.

A. All individuals are required to carry, display, and use their PIV card while on duty and for access into TSA-controlled properties, facilities, checkpoints, and other areas under TSA control. Effective January 1, 2012, the HSPD-12 PIV card is the only recognized TSA identification.

B. TSA identification media and access control media are the property of TSA. They must be surrendered in accordance with DHS and TSA policies, immediately upon request by an authorized TSA official, or when access to TSA-controlled facilities is no longer required.

C. The CSO is the agency official with authority for:

(1) The establishment, implementation, oversight, and periodic assessment of the *Identification Media and Access Control Program* for all agency OEs.

(2) Amending or modifying security-related procedures to meet the area/program-specific needs.

(3) Overseeing all TSA identification media regarding issuance, storage, control, accountability, retention, return, destruction, or disposition as set forth in HSPD-12.

D. TSA personnel and contractors shall:

(1) Display a valid form of TSA identification while in TSA-controlled facilities, on-duty, and/or conducting official business.

(2) Ensure proper handling and safeguarding of TSA-issued identification, to include refraining from allowing another person to use such identification for any purpose and storing the identification in an unsafe manner when not in use (e.g., in a locked vehicle).

(3) Follow established procedures for reporting TSA identification or access control media (e.g., PIV card, TSA-issued key) in the event it is lost, stolen, or damaged, as set forth in the Handbook and/or local procedures.

(4) Comply with established procedures when requesting access for, granting access to, and/or escorting visitors through TSA-controlled facilities.

(5) Notify the Facilities Security Manager (FSM) immediately upon observing any person(s) not complying with access control standards and requirements.

(6) Comply with access control standards and requirements, as set forth in this directive and supplementary guidance materials, to include *Identification Media and Access Control Program Handbook* for TSA MD 2800.16.

E. Visitor's failure to adhere to all requirements may result in their removal from the TSA-controlled facility.

F. Contractors shall not be granted access as a visitor to perform work affiliated with a contract in lieu of completing the requirements set forth in TSA MD 2800.71, *Pre-Employment Investigative Standards for TSA Non-Screener Employees and Contractors*. Exemptions shall be granted in accordance with those conditions specified in TSA MD 2800.71.

G. In the event of a medical or safety emergency, emergency service personnel with legitimate identification may be permitted access to the TSA-controlled facilities without undergoing screening. However, emergency service personnel must be escorted at all times while in the facility by TSA personnel unless the incident requires evacuation of non-emergency service personnel.

H. TSA personnel located in the National Capital Region who do not use their PIV card for 30 days at their regular duty station shall have their access privileges suspended. To have their access privileges restored, personnel must present their PIV card to the Security Branch/Physical Security Section Representative.

I. Security officers, custodial staff, vendors, and building engineers shall be issued a PIV card following a favorable background check by the OLE/FAMS Personnel Security Section. Security officers must also have proof of at least an Interim Secret security clearance. Engineering and Custodial staff must be escorted in restricted areas, and only if cleared by authorized personnel and advance notice is given to the individual in charge of the restricted area so that the area may be sanitized of classified or other sensitive information.

J. Access Control Officers, or the responsible program officials, shall be required to hold and maintain a security clearance equal to, or above, the highest level of classified material handled and stored at their respective location. Special Security Officers (SSOs) and Facility Security Managers (FSMs) at locations with Sensitive Compartmented Information Facilities (SCIFs) will need clearance at the Top Secret/Sensitive Compartmented Information (TS/SCI) level.

7. PROCEDURES: Reference the Identification Media and Access Control Program Handbook for TSA MD 2800.16 for procedures associated with TSA media and access control. For assistance or to report noncompliance or violations, contact the Security Section at (571) 227-2600 or CredentialBadgeCustS@tsa.dhs.gov.

8. APPROVAL AND EFFECTIVE DATE: This policy is approved and effective the date of signature unless otherwise specified.

APPROVAL

Signed September 21, 2016

Roderick Allison
Assistant Administrator/Director
Office of Law Enforcement/Federal Air Marshal Service

EFFECTIVE

September 28, 2016

Date

Distribution: Assistant Administrators and equivalents, Managers and Supervisors, Business Management Office Directors, Federal Security Directors, Supervisory Air Marshals in Charge, Property Management Division, Accountable Property Officers

Point-of-Contact: Chief Security Officer, Security Section, CredentialBadgeCustS@tsa.dhs.gov, (571) 227-3061