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

1. **PURPOSE:** This directive provides TSA policy and procedures for the establishment, integration, and implementation of the *Insider Threat Program.*

2. **SCOPE:** This directive applies to all TSA personnel.

3. **AUTHORITIES:**

   A. 32 CFR Part 2001, *Classified National Security Information*

   B. 49 CFR Part 1520, *Protection of Sensitive Security Information*

   C. Aviation and Transportation Security Act (ATSA), Public Law 107-71

   D. Executive Order (EO) 13526, *Classified National Security Information*

   E. Executive Order (EO) 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*

   F. DHS Directive 047-01, *Privacy Policy and Compliance*

   G. DHS Directive 4300A, *Sensitive Systems Policy*

   H. DHS Instruction Handbook 121-01-007, *Personnel Suitability and Security Program*

   I. DHS Instruction 121-01-011, *Administrative Security Program, Chapter 10*

   J. DHS MD 11052, *Internal Security Program*

   K. TSA MD 1100.73-5, *Employee Responsibilities and Conduct*

   L. TSA MD 2800.15, *Foreign Visitor Management*

   M. TSA MD 3700.4, *Handling Sensitive Personally Identifiable Information*

   N. TSA MD 1400.3, *Information Technology Security*

   O. TSA MD 2800.5, *Internal Security Reporting: Foreign Contact and Travel*

   P. TSA MD 1100.75-7, *Office of Professional Responsibility*

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

R. TSA MD 2810.1, *SSI Program*

S. TSA MD 1100.75-5, *Whistleblower Protections for Transportation Security Officers*

T. TSA MD 2800.12, *Workplace Violence Program*

4. DEFINITIONS:

A. Concept of Operations (CONOPS): For the purposes of this directive, a document that describes the process used by the Insider Threat Program to deter, detect, and mitigate insider threats to TSA's personnel, operations, information, and critical infrastructure.

B. Insider Threat: One or more individuals with access and/or insider knowledge that allows them to exploit vulnerabilities of the Nation's transportation systems with intent to cause harm. This includes direct risks associated with TSA's security programs and operations, as well as the indirect risks that may compromise our critical infrastructure. For purposes of the TSA *Insider Threat Program*, insiders are, or present themselves to be, current or former transportation sector employees, contractors, or partners who have or have had authorized access to transportation sector facilities, operations, systems, and information.[1]

C. Insider Threat Assessment: A multi-layered approach to gather and analyze information to identify vulnerabilities in personnel and information systems from an insider threat perspective. In addition, the Insider Threat Assessments (ITAs) are designed to increase awareness of potential behaviors exhibited by an insider threat and promote a culture which encourages individuals to report suspicious activity.

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

5. RESPONSIBILITIES:

A. The Administrator, or designee, is responsible for:

(1) Providing strategic guidance and overarching policy direction for the *Insider Threat Program*; and

(2) Ensuring senior-level accountability for the coordinated interagency development, integration, and implementation of policies and procedures, as appropriate.

B. The Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) is responsible for:

[1] This definition is derived, in part, from the President's *National Infrastructure Advisory Council*, dated April 2008.

(1) Providing operational management guidance and administrative direction for the *Insider Threat Program*;

(2) Developing policies and procedures for the effective development, integration, and management of the *Insider Threat Program*;

(3) Advising the TSA Administrator, or designee, on *Insider Threat Program*-related activities;

(4) Ensuring the *Insider Threat Program* is consistent with EO 13587, and meets or exceeds the minimum guidance and standards developed by the Interagency Insider Threat Task Force; and

(5) Designating a Supervisory Air Marshal in Charge (SAC), or equivalent, to oversee the daily operational and administrative efforts of the *Insider Threat Program*.

C. The Office of Inspection (OOI) is responsible for:

(1) Coordinating with the *Insider Threat Program* on insider threat-related investigative activities, as appropriate;

(2) Serving as the primary authority for investigating reports of incidents involving criminal and administrative TSA personnel misconduct when the DHS Office of Inspector General (OIG) chooses not to serve as the lead; and

(3) Collaborating with the DHS OIG on reports of incidents involving criminal and administrative employee misconduct activities, as appropriate.

D. The Office of Professional Responsibility is responsible for ensuring timely, fair, consistent, and appropriate adjudication of discipline resulting from activities of the *Insider Threat Program*.

E. The Office of Intelligence and Analysis is responsible for vetting information and sharing appropriate insider threat-related intelligence with the *Insider Threat Program*.

F. The Office of Training and Workforce Engagement (OTWE) is responsible for:

(1) Developing, in coordination with the *Insider Threat Program*, an Insider Threat training course and providing it to all TSA personnel via the TSA Online Learning Center (OLC); and

(2) Maintaining auditable records of required *Insider Threat Program*-related training provided to TSA personnel.

G. The Office of Security Policy and Industry Engagement (OSPIE) is responsible for:

(1) Coordinating and facilitating communication between the *Insider Threat Program* and private sector transportation stakeholders; and

(2) Providing support to the *Insider Threat Program* as appropriate.

H. The Office of Human Capital (OHC) is responsible for providing personnel-related information as appropriate.

I. The Office of Security Operations (OSO) is responsible for coordinating with the *Insider Threat Program* on Insider Threat Assessments (ITAs), as appropriate.

J. The Office of Security Capabilities is responsible for:

(1) Assisting the *Insider Threat Program* with the identification and prioritization of insider threat populations and scenarios as appropriate; and

(2) Providing analytical support to assess proposed mitigation measures.

K. The Office of Information Technology is responsible for:

(1) Coordinating with the *Insider Threat Program* to detect and prevent insider threat-related exploitation of information systems;

(2) Providing technical support and information-gathering capabilities to enhance insider threat-related inquiries and investigations; and

(3) Providing awareness of cyber security-related topics that educate TSA personnel on the effect of insider threat-related activities.

L. The Office of Chief Counsel is responsible for:

(1) Providing legal guidance and assistance on issues related to the *Insider Threat Program*; and

(2) Reviewing the TSA *Insider Threat Program* procedures to help ensure compliance with legal requirements.

M. The Office of Civil Rights and Liberties, Ombudsman, and Traveler Engagement is responsible for providing guidance to the *Insider Threat Program* on matters involving the appropriate protection of privacy, civil rights, and civil liberties.

N. The OLE/FAMS, Security Services and Assessments Division (SSAD), Security Branch, Personnel Security Section, is responsible for coordinating with the *Insider Threat Program* regarding issues of personnel suitability and security clearance eligibility.

O. The OLE/FAMS, SSAD, Security Branch, Physical Security Section is responsible for coordinating with the Insider Threat Program regarding issues related to access control, credentialing, closed circuit television footage review, and photographs.

P. The SAC, or designee, of the *Insider Threat Program* is responsible for:

(1) Managing the daily operational and administrative efforts of the Insider Threat Section;

(2) Developing, in coordination with the OTWE, insider threat-related training and awareness, as appropriate;

(3) Collaborating and coordinating with the appropriate internal and external stakeholders in deterring, detecting, mitigating, and/or referring insider threat-related inquiries and investigations;

(4) Collaborating with DHS OIG on insider threat-related investigations involving TSA personnel except as provided in Section 5.C.(2), as appropriate;

(5) Collaborating with DHS Office of Intelligence and Analysis, Counterintelligence Programs Division (CIPD) on insider threat-related matters as appropriate;

(6) Conducting ITAs on an established schedule, or as directed by management, at designated transportation venues in coordination with the OSO;

(7) Identifying and promulgating best practices and standards for the *Insider Threat Program*;

(8) Informing TSA's leadership of significant insider threat-related efforts or concerns, as appropriate; and

(9) Performing annual self-assessments of the *Insider Threat Program* to ensure compliance with all applicable laws, regulations, policies, standards, and established management controls.

Q. Supervisors and managers are responsible for ensuring that they and their subordinates understand their responsibilities under this directive and take immediate and appropriate action upon being notified or learning of an insider threat-related suspicious encounter, activity, or behavior.

R. All TSA personnel are responsible for reporting insider threat-related suspicious encounters, activities, and behaviors consistent with this directive and any additional guidance as provided by the *Insider Threat Program*.

6. POLICY:

A. Pursuant to EO 13587, TSA shall develop and implement an *Insider Threat Program* aimed at deterring, detecting, and mitigating insider threats to TSA's personnel, operations, information, and critical infrastructure consistent with the appropriate protections of privacy, civil rights, and civil liberties. The *Insider Threat Program* consists of Training and Awareness, Operations-Referrals and Mitigation, and Insider Threat Assessments.

B. TSA personnel shall report insider threat-related suspicious encounters, activities, and behaviors to their immediate supervisor and/or to the Insider Threat Section immediately upon discovery or as soon as practicable. Assistant Administrators or equivalents may implement Office-specific reporting procedures.

7. PROCEDURES:

A. Contact the *Insider Threat Program* for assistance or to report an insider threat at (855) 257-6919 or InsiderThreat@ole.tsa.dhs.gov. Refer to TSA MD 1100.73-5 for additional guidance on reporting requirements.

B. *Insider Threat Program* activities shall be conducted in accordance with the *Insider Threat Program* SOP, *Insider Threat Program* CONOPS, and other relevant procedures. These documents are available upon request if required for the performance of official duties by contacting InsiderThreat@ole.tsa.dhs.gov.

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

APPROVAL

Signed July 8, 2013

_____ _____

John Pistole Date
TSA Administrator

EFFECTIVE

_____

Date

Distribution: Deputy Administrator, Assistant Administrators or equivalents, Federal Security Directors, BMO Directors, SACs, and all other TSA employees

Point-of-Contact: Insider Threat Program, InsiderThreat@ole.tsa.dhs.gov, 855- 257-6919