

ORDER

DOT 1642.1

SUBJECT: DEFENSIVE COUNTERINTELLIGENCE AND INSIDER THREAT PROGRAM

- 1) **PURPOSE.** This order establishes U.S. Department of Transportation (DOT) policy and assigns responsibilities for the Defensive Counterintelligence and Insider Threat Program (DCIITP). The DCIITP seeks to establish a secure operating environment for DOT persons, systems, and facilities from foreign intelligence service (FIS) collection and insider threats.
- 2) **SCOPE.** This order applies to all DOT Operating Administrations and Secretarial Offices (DOT Components), and to DOT personnel who have access to classified information systems (as defined in Executive Order [E.O.] 13587). This order also applies to sensitive or proprietary information as determined by DOT and to sensitive computer networks that are certified and accredited or otherwise approved for operation by the Federal Government. For purposes of this order, DOT personnel includes employees and contractors, as defined in E.O. 12968, as well as interns and students.
- 3) **CANCELLATIONS.** None.
- 4) **REFERENCES AND AUTHORITIES.** See Annex A of this Order.
- 5) **BACKGROUND.** President Obama signed E.O. 13587 on October 7, 2011, establishing new Federal entities whose goals are to better safeguard classified information. Additionally, E.O. 13587 and the National Insider Threat Policy directs Executive Branch Departments and Agencies to establish Insider Threat Programs based on counterintelligence (CI) activities to safeguard classified information and protect national security.
- 6) **GUIDING PRINCIPLES.**
 - a) DOT is subject to FIS and insider threats and will take actions to mitigate or eliminate these threats.
 - b) DOT should continually identify and assess threats to DOT and its personnel and institute programs to defeat the threats.
 - c) DOT will leverage best practices used by the U.S. Intelligence Community and other government agencies that operate CI programs and implement them across DOT.

7) **POLICY.** The DCIITP is established as a Departmental program designed to protect classified national security information, as defined in E.O. 13526, Sensitive Security Information, and other designated sensitive, proprietary, or otherwise protected information, as well as all DOT personnel, facilities, and automated systems from FIS and insider threats. The Administrator of the Federal Aviation Administration (FAA) will develop and implement a separate FAA Hub, as described in sections 8 and 9 below.

8) **PROCEDURES.**

- a) The DCIITP will leverage existing DOT security and intelligence programs and activities that are executed by DOT Components, including the Office of Security (M-40), the Office of the General Counsel (OGC), the Office of Intelligence, Security and Emergency Response (S-60), and the Office of the Chief Information Officer (S-80), in order to meet requirements and minimum standards as established by the National Insider Threat Program Task Force for Executive Branch Insider Threat Programs. The FAA Hub will use existing FAA security and intelligence programs and activities and will meet the requirements and minimum standards established by the National Insider Threat Program Task Force for Executive Branch Insider Threat Programs, as well as be consistent with DOT's program.
- b) The following new programs are established and further defined in this order: Insider Threat Program, Suspicious Activity Reporting Program, and the CI Awareness Training Program.

Insider Threat Program: The intent of this DOT program is to better protect both classified information and sensitive information accessed by DOT employees, to include information that is resident on classified and unclassified computer networks. Through enhanced vigilance, the DOT Insider Threat program managers will assist employees in better protecting classified information and networks from malicious insiders.

Suspicious Activity Reporting (SAR): With assistance from the Program Manager, Information Sharing Environment, and officials from the National SAR Initiative, with approval of the deputy secretary, S-60 developed and fielded a SAR database for the express purpose of allowing all DOT employees to report suspicious activity by simply accessing the DOT Intranet and completing a short form giving specifics on the noted activity. All DOT employees are encouraged to use this resource.

CI Awareness Training: This training is essential to enhancing the protection of DOT employees, classified and sensitive information, computer networks, and other key DOT assets; CI training will be given to all employees to raise the awareness that any DOT employee could become the target of a Foreign Intelligence Service. CI awareness training better prepares employees to protect themselves, classified or sensitive information and other important DOT assets.

- c) The Administrator of the FAA will develop, implement, manage, and operate the FAA DCIITP Hub, including a FAA Insider Threat effort and CI Awareness Program. The

FAA Hub will be suitable to the FAA's size, worldwide presence, and missions. The FAA's DCIITP Hub may differ from the Department-wide Hub; however, the FAA Hub will meet the requirements and minimum standards established by the National Insider Threat Program Task Force for Executive Branch Insider Threat Programs.

9) RESPONSIBILITIES.

- a) Heads of Operating Administrations and the Inspector General (IG) as he/she deems appropriate. Each is required to implement the requirements of the DCIITP by:
 - i. Appointing a CI Program Lead who will act as the Head of the Operating Administrators' representative for the DCIITP implementing activities and by maintaining all associated records and submitting required reports.
 - ii. Enforcing requirements to support the Insider Threat Program, the DOT Suspicious Activity Reporting Program, and the DCIITP Training Programs.
 - iii. Enforcing DOT Foreign Travel Briefing and Foreign Visitor Programs for the purpose of tracking, documenting, and retrieving DOT employee foreign travel and foreign visitors to all DOT locations.
 - iv. Ensuring all requested information pertaining to DOT personnel, systems, and activities is made available and shared, in accordance with applicable laws and privacy and civil liberties policies, with DOT Components conducting inquiries under the DCIITP.

- b) Federal Aviation Administrator: The Administrator of the Federal Aviation Administration is responsible for:
 - i. Developing, implementing, managing, and operating an FAA HUB suitable to the FAA's size, worldwide presence, and missions.
 - ii. Appointing a CI Program Lead from the Office of Security and Hazardous Materials Safety who will act as the FAA's representative for DCIITP Hub implementing activities and maintaining all associated records and submitting required reports. This official will also be responsible for liaison with the Departmental DCIITP program.
 - iii. Directing all FAA lines of business and staff offices to provide appropriate support to the FAA DCIITP Hub.
 - iv. Enforcing applicable DOT and FAA Travel Briefing and Foreign Visitor Program requirements.
 - v. Ensuring all required information pertaining to personnel, systems, and activities is made available to and shared with authorized FAA personnel and, where appropriate,

DOT personnel, conducting defensive counterintelligence and insider threat inquiries, in accordance with applicable laws and privacy and civil liberties policies.

- c) Program Executive: The Director of S-60 is appointed as the DCIITP Executive responsible for:
- i. Leading DOT in establishing and implementing the DCIITP.
 - ii. In coordination with OGC, ensuring the program is executed with all applicable laws and privacy and civil liberties policies.
 - iii. Establishing guidelines and procedures for the retaining, sharing, and safeguarding of records and documents necessary to complete inquiries and assessments under the DCIITP.
 - iv. Establishing and leading a DCIITP Executive Committee for guidance on all DCIITP related issues, conducting program oversight and reviews, and identifying and making program resource recommendations to the Secretary. At a minimum the Executive Committee will be composed of senior representatives from each Operating Administration, M-40, S-80, and OGC.
- d) Program Manager: The S-60 Associate Director for Intelligence is appointed as the DCIITP Manager and is responsible for:
- i. Implementing and managing the DCIITP throughout DOT.
 - ii. Acting as DOT's primary representative on CI and insider threat program matters.
 - iii. Coordinating, collaborating, and advising all Operating Administrations on policy developments affecting the DCIITP execution.
 - iv. Establishing and managing all reporting requirements, to include self-assessments and independent assessments, to and with outside Departments and Agencies regarding the DCIITP.
 - v. Overseeing the collection, analysis, and reporting of information across DOT to support the identification and assessment of CI and insider threats.
- e) DCIITP Coordinator: The CI Coordinator, located in the S-60 Intelligence Division is responsible for:
- i. Coordinating and executing the DCIITP throughout DOT.
 - ii. Meeting with CI Program Leads from Operating Administrations on a quarterly basis to discuss program requirements and other issues as deemed necessary.

- iii. Leading the establishment and execution of a CI and Insider Threat Awareness Training Program.
 - iv. Collecting all required data and preparing annual DCIITP reports that identify program accomplishments, resources allocated, insider threat risks to the agency, recommendations and goals for program improvement, and major program impediments or challenges.
- f) The Assistant Secretary for Administration is responsible for:
- i. Coordinating and supporting the DCIITP Executive, CI Program Manager, and CI Coordinator on all personnel, physical, technical, and communications security issues and national security inquiries that support the execution of the DCIITP.
 - ii. Appointing a human resources (HR), M-40, and Procurement representative to coordinate with the DCIITP Manager on all matters related to DCIITP.
 - iii. Directing the sharing of all relevant HR records, as identified by the DCIITP Coordinator, to support the identification, analysis, assessment, and resolution of all potential insider threat matters.
 - iv. Implementing policies and procedures to inform current and future DOT employees and others performing work for DOT and subject to this policy as defined above as to the existence of the DCIITP.
- g) Office of General Counsel is responsible for:
- i. Providing legal support for the establishment, implementation, execution, management and oversight of the DOT DCIITP.
 - ii. Coordinating all legal aspects of DCIITP with DOT Components and with other departments and agencies, as required.
 - iii. Providing legal review of all responses to any inquiries concerning the execution of the DCIITP.
- h) Investigations and Referrals:

The Office of Inspector General shall receive concurrent notification, along with the Federal Bureau of Investigation (FBI), in CI matters appearing to involve an illegal act when the apparent illegal act appears to be within the purview of the Inspector General Act and in accordance with DOT Orders 8000.5 (Office of Inspector General Investigative Procedures) and 8000.8 (Office of Inspector General Investigative Responsibilities), including any illegal acts in connection with DOT employees, contractors, or grantees affecting DOT programs or activities. In matters where OIG has an investigative interest they will contact and coordinate with the FBI.

- i) Office of Chief Information Officer is responsible for:
- i. Appointing an individual to represent S-80 on all DOT DCIITP coordination matters.
 - ii. Coordinating with Operating Administrations to maintain and enforce a DOT information system security program to identify and mitigate information/system security incidents, threats, and vulnerabilities.
 - iii. Coordinating with Operating Administrations to establish a comprehensive DOT user information assurance and awareness training program to inform DOT personnel of recurring network and system monitoring and auditing, processes in effect throughout DOT enterprise to support CI and insider threat requirements.
 - iv. Establishing and monitoring access rights and related procedures for all unclassified systems managed within DOT.
 - v. Providing M-40 and S-60 periodic reports specific to successful and attempted intrusions and misuse of DOT information systems and networks.
 - vi. Coordinating with the Insider Threat Task Force to identify and adopt best practices and programs used by other agencies to monitor information systems for the purpose of identifying potential insider threat activity.
 - vii. Regularly communicating with S-60 and the Inspector General focal points to share network system use activities and analysis results that illustrate potential CI and insider threat activity.

10) IMPLEMENTATION. This order is effective upon publication and will be reviewed and updated as needed or at a minimum of every 2 years.

Annex A

The following list of references and authorities that should be used in developing, implementing, and executing the overall DOT Defensive Counterintelligence and Insider Threat Program (DCIITP) and any supporting programs. This list is not intended to be all inclusive and will be updated as required.

- a. Public Laws.
 - i. National Security Act of 1947, 50 U.S.C. § 401 note, as amended.
 - ii. Privacy Act of 1974, 5 U.S.C. § 552a as amended.
 - iii. Counterintelligence Enhancement Act of 2002, 50 U.S.C. § 401 (2002), as amended.
 - iv. Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C § 401 note, (2004), as amended.
 - v. Computer fraud and Abuse Act of 1986, 10 USC § 1030 note, as amended.
- b. Executive Orders.
 - i. Executive Order 12333, United States Intelligence Activities, December 4, 1981 as amended.
 - ii. Executive Order 12829, National Industrial Security Program, January 6, 1993, as amended.
 - iii. Executive Order 12968, Access to Classified Information, August, 2, 1995.
 - iv. Executive Order 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, June 30, 2008.
 - v. Executive Order 13526, Classified National Security Information, December 29, 2009.
 - vi. Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011.
- c. Presidential Directives.
 - i. Presidential Decision Directive PDD/NSC-12 Security Awareness and Reporting of Foreign Contacts, August 5, 1993.

- d. Other Applicable Authorities and Guidance.
 - i. Committee on National Security Systems (CNSS) Policy No. 18, National Policy on Classified Information Spillage, June 2006.
 - ii. 32 CFR 2001, Classified National Security Information.
 - iii. DOT Order and Manual 1640.4E, Classified National Security Information.
 - iv. DOT Order 1630.2B, Personnel Security Management, May 30, 2001.
 - v. Personnel Security Management Manual DOT M 1630.2c.
 - vi. DOT Order 1641.1 Foreign Travel Security Requirements and Reporting of Foreign Contacts, March 30, 2007.
 - vii. DOT Suspicious Activity Reporting (SARs) Concept of Operations, December 14, 2011.
 - viii. DOT Deputy Secretary Memorandum designating S-60 as DOT Program Manager for Counterintelligence Matters, June 29, 2010.
 - ix. DOT Secretary Letter to Director of National Intelligence designating Director, S-60, as the DOT Federal Senior Intelligence Coordinator, May 16, 2012.