



Approved On: 12 FEB 2014

DOJ ORDER

INSIDER THREAT

PURPOSE: This Order establishes policy and assigns responsibilities for a Department of Justice (DOJ) Insider Threat Prevention and Detection Program (ITPDP).

SCOPE: This Order is applicable to all DOJ Components with access to classified information, including classified computer networks controlled by DOJ; all classified information on those networks; and DOJ employees, contractors, and others who access classified information or classified computer networks controlled by DOJ (“cleared employee”).


ORIGINATOR: Justice Management Division, Information Technology Security Staff

CATEGORY: (I) Administrative, (II) Information Technology

AUTHORITY: Executive Order (EO) 13587 of October 7, 2011, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information; EO 12968 of August 2, 1995 (as amended), Access to Classified Information; EO 13526 of December 29, 2009, Classified National Security Information; Presidential Memorandum of November 21, 2012, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs

CANCELLATION: None

DISTRIBUTION: This Order is distributed electronically to those components referenced in the “SCOPE” section as well as posted to the DOJ Directives electronic repository ([SharePoint](#)).

APPROVED BY: *Eric H. Holder, Jr.*
Attorney General 

ACTION LOG

All DOJ directives are reviewed, at minimum, every five years and revisions are made as necessary. The action log records dates of approval, recertification, and cancellation, as well as major and minor revisions to this directive. A brief summary of all revisions will be noted. In the event this directive is cancelled or superseded, or supersedes another directive, that will also be noted in the action log.

Action	Authorized by	Date	Summary
Initial Approval	Eric H. Holder, Jr.	Feb. 12, 2014	This Order establishes policy and assigns responsibilities for a Department of Justice (DOJ) Insider Threat Prevention and Detection Program (ITPDP).




TABLE OF CONTENTS

Glossary of Terms.....	4
I. Policy	5
A. Insider Threat Prevention and Detection Program.....	5
B. Insider Threat Working Group.....	5
II. Roles and Responsibilities	5
A. Senior Department Official.....	5
B. CI Executive Agents.	5
C. The DOJ ITWG.....	5
D. DOJ ITPDP	6
E. Heads of Components.....	7
Appendix A: Authorities.....	8

GLOSSARY OF TERMS

DEFINITIONS

Term	Definition
Counterintelligence	Information gathered and activities conducted to identify, deceive, exploit, disrupt or protect against espionage, or other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities (EO 12333, as amended).
Insider	Any person with authorized access to any U.S. Government resource including personnel, facilities, information, equipment, networks or systems.
Insider Threat	The threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the security of the U.S. This threat can include damage to the U.S. through espionage, terrorism, unauthorized disclosure of information, or through the loss or degradation of Departmental resources or capabilities.

ACRONYMS

Acronym	Meaning
AAG/A	Assistant Attorney General for Administration
CI	Counterintelligence
CRM	Criminal Division
DOJ	Department of Justice
EO	Executive Order
FBI	Federal Bureau of Investigation
IA	Information Assurance
ITPDP	Insider Threat Prevention and Detection Program
ITWG	Insider Threat Working Group
JMD	Justice Management Division
NSD	National Security Division
OIG	Office of the Inspector General
SDO	Senior Department Official

I. Policy

- A. Insider Threat Prevention and Detection Program.** This Order establishes a DOJ ITPDP for deterring, detecting, and mitigating insider threats. It uses counterintelligence (CI), security, information assurance (IA), and other relevant functions and resources to identify and counter the insider threat. The ITPDP takes advantage of existing federal laws, statutes, authorities, policies, programs, systems, and architectures in order to counter the threat of those insiders who may use their authorized access to compromise classified information. The DOJ ITPDP shall employ risk management principles, tailored to meet the distinct needs, mission, and systems of individual Components, and shall include appropriate protections for legal, privacy, civil rights, and civil liberties requirements.
- B. Insider Threat Working Group.** The Insider Threat Working Group (ITWG) was established pursuant to Executive Order (EO) 13587 to develop policies, objectives, and priorities for integrating security, counterintelligence, user audits, monitoring, and other safeguarding capabilities within the DOJ, in accordance with its charter. The working group will also develop minimum standards and guidance for implementing the insider threat program initiatives throughout DOJ consistent with the U.S. Government insider threat program's national standards and guidance.

II. Roles and Responsibilities

- A. Senior Department Official.** The Assistant Attorney General for Administration (AAG/A) is designated as DOJ's Senior Department Official (SDO) with authority to provide and delegate management, accountability, and oversight of the DOJ ITPDP.
1. The SDO or his designee chairs the ITWG, which is composed of senior staff from Departmental Components with responsibilities for counterintelligence, security, information assurance, human resources, general counsel, and any other relevant responsibilities, functions, and/or resources the SDO deems should be associated with the DOJ ITWG, in accordance with its charter.
 2. The SDO shall issue standards, guidance, and policy developed by the ITWG.
- B. CI Executive Agents.** The Executive Agents for Departmental counterintelligence investigations are the Director of the FBI and the Assistant Attorney General for National Security or their designees. The CI Executive Agents will coordinate all counterintelligence operations, investigations, and prosecutions within DOJ.
- C. The DOJ ITWG.** The DOJ ITWG shall:

1. Develop Departmental minimum standards and guidance consistent with the Presidential Memorandum -- National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.
2. Address development and implementation of insider threat detection and prevention capabilities and coordinate Departmental resources and procedures for program effectiveness.
3. Consult with records management, legal counsel, ethics officials, and civil liberties and privacy officials to ensure any legal, privacy, civil rights, or civil liberties issues (including use of personally identifiable information) are appropriately addressed.
4. Consult with OIG regarding the establishment of a referral process for complaints and allegations.

D. DOJ ITPDP. The DOJ ITPDP operates under the joint authorities of the heads of the Justice Management Division (JMD), the National Security Division (NSD), and the Federal Bureau of Investigation (FBI). The DOJ ITPDP shall:

1. Operate jointly at a secure operations facility or facilities designated by the SDO.
2. Establish and operate a centralized organizational entity within the operation center(s) to monitor, collect, audit, and analyze data about employees and contractors for insider threat detection and mitigation. Relevant information defined in Departmental insider threat standards and guidance and stored within Components will be made available to the operation center(s).
3. Monitor user activity on DOJ classified computer networks.
4. Evaluate, on an ongoing basis, personnel security records and reporting information.
5. Develop and promulgate Departmental insider threat education, training and awareness, to include employee insider threat reporting responsibilities.
6. Develop an integrated system for the timely reporting of all insider threat incidents and concerns to the DOJ ITPDP for appropriate action and referral to appropriate Departmental investigative organizations.
7. Identify and recommend to the DOJ ITWG standards for any current or future federal and/or public data sources that should be considered for collection and analysis.
8. Develop and implement insider threat information analysis, reporting, and response capabilities.

9. Refer all counterintelligence inquiries that indicate classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or agent of a foreign power to the DOJ CI Executive Agents.
10. Assist Departmental Components as necessary to implement and improve insider threat detection and prevention capabilities.
11. Conduct assessments of Departmental Components, as directed by the SDO, to determine the level of organizational compliance with this policy and minimum insider threat standards; the results of which shall be reported to the Senior Information Sharing and Safeguarding Steering Committee in accordance with 2.1(c) of EO 13587.

E. Heads of Components. The head of each Departmental Component with employees who have access to classified information, or that operate or access classified computer networks, or the Component head's designee, shall:

1. In coordination with the DOJ ITPDP, implement DOJ policy and minimum standards issued pursuant to this policy.
2. Ensure that insider threat concerns are reported to the DOJ ITPDP as defined in Departmental insider threat standards and guidance issued pursuant to this policy.
3. Promulgate additional Component guidance, if needed, to reflect unique mission requirements consistent with meeting the minimum standards and guidance issued pursuant to this policy.
4. Under the guidance of the DOJ ITPDP, perform self-assessments at least annually of compliance with insider threat policies and standards and report the results to the DOJ ITPDP.
5. Enable independent assessments, in accordance with Section 2.1(d) of EO 13587, of compliance with established insider threat policy and standards by providing information and access to personnel of the ITPDP.
6. Implement insider threat education, training, awareness, and reporting responsibilities issued pursuant to this policy.
7. The Departmental Components with elements that are members of the Intelligence Community (IC) shall establish an Insider Threat Detection and Prevention capability that meets mission and IC requirements and that integrates with the DOJ ITPDP.

APPENDIX A: AUTHORITIES

Nothing in this policy shall be construed to supersede or change the requirements of the National Security Act of 1947, as amended; the Intelligence Reform and Terrorism Prevention Act of 2004; Executive Order 12333, as amended (2008); Executive Order 13467, (2008); Executive Order 13526, (2009); Executive Order 12829, as amended, (1993); Executive Order 13549 (2010); Executive Order 13587 (2011), and Executive Order 12968, (1995) and their successor orders or directive.