



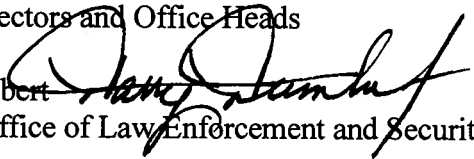
United States Department of the Interior
OFFICE OF THE SECRETARY

Law Enforcement and Security
1849 C Street, N.W.
Washington, D.C. 20240

DEC 06 2013

Memorandum

To: Bureau Directors and Office Heads

From: Harry Humbert 
Director, Office of Law Enforcement and Security

Subject: Interim Law Enforcement and Security Policy – Departmental Manual 445
Counterintelligence and Operational Security Program

In order to provide bureau and office law enforcement and security programs with expedited release of new Departmental policies and policy updates, we have received Secretarial approval to issue interim law enforcement and security policies. All policies will be simultaneously issued to bureaus and office as interim policy and sent through the official sunaming process to become final. Interim policies will be effective immediately.

The development of this policy has been a collaborative effort between the Office of Law Enforcement, Office of Inspector General, Office of the Solicitor, and Office of the Chief Information Officer. This interim policy has been thoroughly reviewed and approved by the signatories listed below.

Please find attached the following policy:

- 445 Departmental Manual, Chapter 1, Counterintelligence Program

Interim policies will not be published outside of this distribution and will not be available on ELIPS. Please assure that the attached policy receives appropriate distribution with bureau and office law enforcement and security programs.

cc: Assistant Secretary, Fish, Wildlife and Parks
Assistant Secretary, Indian Affairs
Assistant Secretary, Insular Affairs
Assistant Secretary, Land and Minerals Management
Assistant Secretary, Policy, Management and Budget
Assistant Secretary, Water and Science
Kim Thorsen, Deputy Assistant Secretary, PRE /s/
Bernard Mazer, Chief Information Officer, OCIO /s/
Edward T. Keable, Office of the Solicitor /s/
Stephen Hardgrove, Office of the Inspector General /s/

Department of the Interior Departmental Manual

Effective Date: TBD

Series: Law Enforcement and Security

Part 445: Counterintelligence and Operational Security Program

Chapter 1: Counterintelligence Program

Originating Office: Office of Law Enforcement and Security

445 DM 1

1.1 **Purpose.** Pursuant to Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, this chapter establishes the Department of the Interior (DOI), Office of Law Enforcement and Security (OLEs), Counterintelligence (CI) Program. This chapter also sensitizes DOI personnel of the potential threats from Foreign Intelligence Entities (FIE) and Trusted Insiders who are a risk to national security; and how to report the potential threats, and take appropriate steps to protect themselves and the DOI. This policy is intended to be used in conjunction with the Departmental Counterintelligence Program Handbook.

1.2 **Scope.** The provisions of this chapter and guidelines as published in the Departmental Counterintelligence Program Handbook apply to all DOI employees, contractors, and other individuals who are associated with or represent the DOI. Nothing within this policy and/or handbook is intended to eliminate or modify requirements established by law, Executive Order, the Office of Inspector General, or departmental policies related to legal, privacy, civil rights, civil liberties, and/or any other reporting requirements.

1.3 **Authority.** This chapter is issued pursuant to 112 DM 17 and 212 DM 17, and the directives, Executive Orders, such as 13587, laws, and regulations reflected in the reference section of the Departmental Counterintelligence Program Handbook.

1.4 **Responsibilities.**

A. Deputy Assistant Secretary – Public Safety, Resource Protection, and Emergency Services is the responsible senior official for the counterintelligence/insider threat program and for providing program status reports annually as required; and providing program guidance and policy compliance for the Department's law enforcement, security, intelligence, counterintelligence/insider threat, fire, aviation, and emergency management programs.

B. The Director – Office of Law Enforcement and Security is responsible for policy development, direction, coordination, compliance of DOI law enforcement, security, intelligence, counterintelligence/insider threat programs and will provide department-wide

guidance and assistance in law enforcement, security, intelligence, and counterintelligence/insider threat matters.

C. The Assistant Director – Office of Law Enforcement and Security – Intelligence Division is responsible for providing management and oversight of the DOI Intelligence, counterintelligence/threat programs. The Assistant Director provides:

- (1) Program management and oversight of the DOI OLES CI Program.
- (2) Professional development of DOI CI personnel.
- (3) Providing an annual status report through the Director – Office of Law Enforcement and Security to the Deputy Assistant Secretary – Public Safety, Resource Protection, and Emergency Services regarding the DOI OLES CI Program.

D. The Chief – National Security Programs – Office of Law Enforcement and Security – Intelligence Division is responsible for:

- (1) Providing management assistance and functional oversight of the DOI OLES CI Program.
- (2) Conducting all CI activities and inquiries in full compliance with privacy, civil liberties and civil rights laws, rules and regulations.
- (3) Establishing and maintaining a secure, computer-based CI Case Tracking System (CICTS).
 - a. DOI OLES CI Program will utilize the CICTS to facilitate:
 - i. referral of CI complaints to the appropriate investigative authority;
 - ii. aiding in the tracking of CI inquiries/investigations;
 - iii. producing statistical reports; and
 - iv. identifying potential issues affecting policy and/or procedures on a department-wide basis.
 - v. assisting to identify CI training needs.
- (4) Coordinating higher-level approval of CI activities through the Assistant Director when required (e.g., forwarding information on matters that require a referral or coordination with the Federal Bureau of Investigation, Office of Inspector General (OIG), DOI Office of the Solicitor, or other appropriate office.

(5) Conducting CI awareness and education training for DOI employees, contractors, and other individuals who are associated or represent the DOI.

E. Coordinating with DOI personnel to provide the DOI OLES CI Unit with access to all relevant:

(1) Databases and files to include but not limited to personnel security files, facility access records, security violation files, travel records, foreign contact reports, and financial disclosure reports.

(2) Network information generated by information assurance elements to include but not limited to, personnel usernames and aliases, levels of network access, audit data, unauthorized use of removable media, print logs, and other data needed for clarification or resolution of an insider threat concern.

(3) Human Resource databases and files to include but not limited to: personnel, security, payroll, and voucher files; outside work/activity requests, disciplinary files, and personal contact records, as may be necessary for resolving or clarifying insider threat matters.

F. DOI Personnel are required to report the following CI-related incidents to the DOI OLES CI Unit or the DOI OIG Hotline in accordance with this policy and/or handbook:

(1) Attempted or actual espionage, subversion, sabotage, terrorism or extremist activities directed against the DOI and its personnel, facilities, resources, and activities;

(2) Unauthorized use of or intrusion into automated information systems;

(3) Unauthorized disclosure of classified, controlled unclassified, sensitive, or proprietary- information or technology; and

G. DOI Personnel are encouraged to report the following CI-related incidents to the DOI OLES CI Unit in accordance with this policy and/or handbook:

(1) Indicators of potential insider threats;

(2) Indicators of other incidents that may indicate FIE activities or an insider threat.

1.5 Counterintelligence Awareness and Education

(1) The CI Program provides CI-awareness training at the unclassified level to ensure it reaches the widest possible audience. The CI Program may provide classified training to DOI personnel who possess appropriate security clearances and need-to-know access.

(2) DOI Personnel are required receive initial, annual, and periodic training on individual reporting responsibilities and potential threats from FIE and the insider threat.

1.6 Reporting Contact Information: The DOI OLES CI Unit can be reached by phone at (202) 208-4216 or via unclassified email DOI_Counterintelligence@ios.doi.gov. For classified reporting, the DOI OLES CI Unit can be reached by secure phone (vIPer or STE) at: (202) 208-6353/6124 or via classified email DOI_Counterintelligence@dhs.sgov.gov (HSDN/SIPRNet); counterintelligence@doi.csp.ic.gov (JWICS/ICEMail). The DOI OIG can be reached via the DOI OIG Hotline at 1-800-424-5081.