

SYSTEM NAME: Insider Threat Program Records (ODNI– 22)

SECURITY CLASSIFICATION: The classification of records in this system can range from UNCLASSIFIED to TOP SECRET.

SYSTEM LOCATION: Office of the Director of National Intelligence (ODNI), Washington, DC 20511.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Present and former U.S. Government civilian employees, military members, contractor employees, experts, consultants, licensees, grantees or any other category of person who holds or has held a security clearance; who serves or has served in a sensitive position.

CATEGORIES OF RECORDS IN THE SYSTEM: Records, including reports and analyses, pertaining to matters, behaviors, or conduct arising in the Counterintelligence, Personnel Security, Physical Security, IT Systems Security, Information Assurance, Human Resources, Law Enforcement, or Background/Suitability contexts that are consistent with the possible existence of a counterintelligence or security threat or that bear on the individual's eligibility to hold a security clearance or serve in a sensitive position.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: The National Security Act of 1947, as amended, 50 U.S.C. 3341, et seq.; 5 U.S.C. 9101; Executive Order 12968, as amended (73 FR 38103); Executive Order 9397, as amended (73 FR 70239); Executive Order 10450, as amended (44 FR 1055); Executive Order 10865, as amended (68 FR 4075); Executive Order 12333, as amended (73 FR 45325); Executive Order 13526, as amended (75 FR 707); Executive Order 13467 (73 FR 38103); Executive Order 13587 (76 FR 63811); Presidential Memorandum, November 21, 2012, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.

PURPOSE(S): To enhance awareness of potential national security vulnerabilities arising from: Inadvertent as well as intentional misuse of authorizations and accesses; violation of established protocols and codes of conduct; disregard for law, regulation, or policy; or from encounters, relationships, or exchanges with persons who may pose a counterintelligence or security risk.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: See General Routine Uses Applicable to More Than One ODNI Privacy Act System of Records, Subpart C of the ODNI's Privacy Act Regulation published at 32 CFR part 1701 (73 FR 16531, 16541) and incorporated by reference (see also <http://www.dni.gov>).

DISCLOSURE TO CONSUMER REPORTING AGENCIES: None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE: Electronic records are stored in secure file-servers located within secure government facilities. Paper records are stored in secured areas within the control of the ODNI.

RETRIEVABILITY: By name, social security number, or other unique employee identifier; other key terms, including the names of individuals with whom covered individuals have interacted.

SAFEGUARDS: Information in this system is safeguarded in accordance with recommended and/or prescribed administrative, physical, and technical safeguards. Records are maintained in a secure government facility with access to the facility limited to authorized personnel only, and authorized and escorted visitors. Physical security protections include guards and locked facilities requiring badges and passwords for access. Records are accessed only by authorized personnel holding appropriate security clearances and whose official duties require access to the records. Communications are encrypted where required and other safeguards are in place to monitor and audit access, and to detect intrusions. System backup is maintained separately.

RETENTION AND DISPOSAL: Pursuant to 44 U.S.C. 3303a(d) and 36 CFR chapter 12, subchapter B, part 1228—Disposition of Federal Records, records will not be disposed of until such time as the National Archives and Records Administration (NARA) approves an applicable ODNI Records Control Schedule.

SYSTEM MANAGER(S) AND ADDRESS: Director, Mission Support Directorate/ Counterintelligence, c/o Director, Information Management Division, Office of the Director of National Intelligence, Washington, DC 20511.

NOTIFICATION PROCEDURE: As specified below, records in this system are exempt from certain notification, access, and amendment procedures. Individuals seeking to learn whether this system contains nonexempt information about them should address inquiries to the ODNI at the address and according to the requirements set forth below under the heading “Record Access Procedures.”

RECORD ACCESS PROCEDURES: As specified below, records in this system have been exempted from certain notification, access, and amendment procedures. A request for access to non-exempt records shall be made in writing with the envelope and letter clearly marked “Privacy Act Request.” Each request must provide the requester’s full name and complete address. The requester must sign the request and have it verified by a notary public. Alternatively, the request may be submitted under 28 U.S.C. 1746, certifying the

requester's identity and acknowledging that obtaining records under false pretenses constitutes a criminal offense. Requests for access to information must be addressed to the Director, Information Management Division, Office of the Director of National Intelligence, Washington, DC 20511. Regulations governing access to one's records or for appealing an initial determination concerning access to records are contained in the ODN I regulation implementing the Privacy Act, 73 FR 16531 (March 28, 2008).

CONTESTING RECORD PROCEDURES: As specified below, records in this system are exempt from certain notification, access, and amendment procedures. Individuals seeking to correct or amend non-exempt records should address their requests to the ODN I at the address and according to the requirements set forth above under the heading "Record Access Procedures." Regulations governing access to and amendment of one's records or for appealing an initial determination concerning access or amendment of records are contained in the ODN I regulation implementing the Privacy Act, 73 FR 16531 (March 28, 2008).

RECORD SOURCE CATEGORIES: Records are obtained from self reports, third party reports, systems activity monitoring activities, and electronic notifications triggered by interrelated U.S. Government systems, which may contain information from U.S. Government, public, and commercial data sources.

EXEMPTIONS CLAIMED FOR THE SYSTEM: Records contained in this System of Records may be exempted from the requirements of subsections (c)(3); (d)(1), (2), (3), (4); (e)(1) and (e)(4)(G), (H), (I); and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1), (k)(2) and (k)(5). Records may be exempted from these subsections or additionally, from the requirements of subsections (c)(4); (e)(2), (3), (5), (8), (12); and (g) of the Privacy Act consistent with any exemptions claimed under 5 U.S.C. 552a(j) or (k) by the originator of the record, provided the reason for the exemption remains valid and necessary.