



9500-01

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Privacy Act of 1974; System of Records

AGENCY: Office of the Director of National Intelligence.

ACTION: Notice.

SUMMARY: The Office of the Director of National Intelligence (ODNI) provides notice that it is establishing two (2) new Privacy Act systems of records, updating and amending four (4) existing Privacy Act systems of records, and rescinding two (2) Privacy Act systems of records. This action is necessary to meet the requirements of the Privacy Act to publish in the Federal Register notice of the existence and character of records maintained by the agency (5 U.S.C. 552a(e)(4)).

DATES: This action will be effective on **[INSERT DATE 40 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, unless comments are received that result in a contrary determination.

ADDRESSES: You may submit comments, identified by [RIN number] by any of the following methods:

Federal eRulemaking Portal: <http://www.regulations.gov>

Email: Dni-FederalRegister@dni.gov

Mail: Director, Information Management Division, Office of the Director of National Intelligence, Washington, D.C. 20511.

FOR FURTHER INFORMATION CONTACT: Jennifer Hudson, Director, Information Management Division, 703-874-8085.

SUPPLEMENTARY INFORMATION: The ODNI was created by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. 108-458, 118 Stat. 3638 (Dec. 17, 2004). ODNI published its final Privacy Act Regulation on March 28, 2008 (73 FR 16531), codified at 32 CFR part 1701. It published twelve (12) Privacy Act systems of records notices on December 28, 2007 (72 FR 73887); fourteen (14) Privacy Act systems of records notices on April 2, 2010 (75 FR 16853) and seven (7) systems of records notices on July 19, 2011 (76 FR 42737). It now adds two (2) systems of records to its inventory of record systems subject to the Privacy Act of 1974 (5 U.S.C. 552a). These new systems of records are: Counterintelligence Trends Analyses Records (ODNI/NCSC-002) and Insider Threat Program Records (ODNI-22). To protect classified and sensitive personnel or law enforcement information contained in these systems, the Director of National Intelligence is proposing to exempt these systems of records from certain portions of the Privacy Act where necessary, as permitted by law.

As required by the Privacy Act, a proposed rule is being published concurrently with this notice seeking public comment regarding exemption of these systems. The ODNI has previously established a rule that it will preserve the exempt status of records it receives when the reason for the exemption remains valid. See 32 CFR part 1701.20 (a)(2) (73 FR at 16537). The two new systems of records are subject to the General Routine Uses Applicable to More than One ODNI Privacy Act System of Records, subpart C of ODNI's Privacy Act Regulation published at 32 CFR part 1701 (73 FR 16531, 16541). ODNI/NCSC-002 articulates an additional routine use permitting disclosure of records in that system to U.S. Government personnel engaged in covered counterintelligence trends analyses.

Several systems of records are being updated to reflect some combination of changes in the categories of record subjects, categories of records maintained, purposes for which the records are used, title, records control schedule, or technology/systems management. These systems of records are: Equal Employment Opportunity and Diversity Office (EEOD) Records (ODNI-10), originally published at 75 FR 16861 (April 2, 2010) and now renamed "Office of Intelligence Community Equal Employment Opportunity and Diversity Office (EEOD) Records;" Security Clearance Reform Research Records (ODNI-13), originally published at 75 FR 16865 (April 2, 2010) and now renamed "Security Clearance Reform Research and Oversight Records;" National Counterterrorism Center (NCTC) Online (ODNI/NCTC-005), originally published at 72 FR 73892 (December 28, 2007) and now renamed "NCTC Current."

In addition, Privacy Act system of records ODNI-19 (Information Technology Systems Activity and Access Records), originally published at 76 FR 42742 (July 19,

2011), is being amended to add subsection (k)(2) of the Privacy Act as an additional basis for exempting records in that system from those provisions of the Act enumerated at 5 U.S.C. 552a(k). A proposed rulemaking supporting this notice addresses ODNI's intention to amend the exemption language of ODNI-19. This is the sole amendment to ODNI-19.

Finally, the ODNI provides notice that it is rescinding two systems of records. The system of records entitled National Counterintelligence Center (NACIC) System of Records, published at 62 FR 8995-01 (February 27, 1997), is rescinded because the National Counterintelligence Center (NACIC) no longer exists as an independent agency, its functions having been transferred under section 1011 of the Intelligence Reform and Terrorism Prevention Act of 2004 to the Office of the National Counterintelligence Executive (now the National Counterintelligence and Security Center) within the ODNI (Pub. L. 108-458; 116 Stat. 3638). The system of records entitled Analytic Resources Catalog (ARC), published at 75 FR 16859 (April 2, 2010), is rescinded pursuant to termination of the activity and decommissioning of the electronic system.

In accordance with 5 U.S.C. 552(r), the ODNI has provided a report of these new and altered systems of records to the Office of Management and Budget and to Congress.

Dated: May 19, 2015.

Jennifer Hudson,

Director,

Information Management Division.

SYSTEM NAME:

Counterintelligence Trends Analyses Records (ODNI/NCSC-002)

SECURITY CLASSIFICATION:

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

SYSTEM LOCATION:

National Counterintelligence and Security Center (NCSC), Office of the Director of National Intelligence (ODNI), Washington, D.C. 20505.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals convicted of or the subject of a criminal complaint, or indicted for espionage or other crime(s) relating to U.S. national security; individuals conspiring with or working on behalf of foreign criminal organizations and convicted of or charged with criminal activity including, but not limited to, corruption and theft of government records for the benefit of a foreign entity or activity; individuals linked to foreign or transnational criminal organizations, foreign intelligence organizations, or international terrorist organizations and subject to administrative processes or penalties for such activity or association; individuals interviewed by U.S. Government personnel or mentioned in such interviews who have been identified in connection with or who have provided relevant information in relation to espionage, crimes related to U.S. national security, foreign

criminal organizations, international terrorist organizations, or unauthorized disclosures of sensitive or classified information.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records include law enforcement records (e.g., convictions, subpoenas, rap sheets, investigatory or administrative files), court documents (e.g., indictments, criminal complaints, plea agreements), NCSC debriefings and interviews with record subjects or their associates and related damage assessments, intelligence or law enforcement reporting on above individuals; and biographical profiles of and personally identifiable information belonging to individuals covered by the system.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108–458, 118 Stat. 3638 (Dec. 17, 2004); the Counterintelligence Enhancement Act of 2002, as amended, 50 U.S.C. 3031, et seq.; the National Security Act of 1947, as amended, 50 U.S.C. 3001, et seq.; Executive Order 12333, 46 Fed. Reg. 59,941 (1981); Executive Order 13354, 69 Fed. Reg. 53,589 (2004).

PURPOSE:

To facilitate development of counterintelligence trend analyses that can be applied to: (1) improving U.S. Government personnel security, counterintelligence, and insider threat programs, policies, and procedures; (2) developing training and instruction to identify threats and mitigate associated risks; (3) promoting cooperative research and analyses

within and among U.S. Government elements on counterintelligence, insider threat, and personnel security issues that have policy implications; and (4) identifying best practices.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

Records in this system are shared with U.S. Government personnel conducting the analyses described herein. Records or findings may be disclosed as set forth in the General Routine Uses Applicable to More Than One ODNI Privacy Act System of Records, Subpart C of ODNI's Privacy Act Regulation published at [32 CFR part 1701](#) (73 FR 16531, 16541) and incorporated by reference.

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 within U.S. Government facilities. Paper and other hard copy records are stored in secured areas within the control of NCSC.

RETRIEVABILITY:

The records in this system are retrieved by name, personal identifier, or subject matter. Only authorized personnel may search this system.

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 only authorized personnel or authorized and escorted visitors. Physical security protections include guards and locked facilities requiring badges and passwords for access. Records are accessed only by authorized U.S. Government personnel and contractors holding an appropriate security clearance and who have a “need to know.” Software controls are in place to limit access, and other safeguards exist 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:

NCSC CI Trends System Manager, c/o Director, Information Management Division,
Office of the Director of National Intelligence, Washington D.C. 20511.

NOTIFICATION PROCEDURES:

As specified below, records in this system have been exempted from certain notification, access, and amendment procedures. Individuals seeking to learn if this system contains information about them should address inquiries to the NCSC at the system manager address above 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."

Pursuant to ODNI's Privacy Act Regulation at 32 CFR 1701.7(d), requesters shall provide their full name and complete address, date and place of birth, citizenship status, alien registration number (if applicable), and date that status was acquired. Additional or clarifying information may be sought to ascertain identity. Requesters also must provide sufficient details to facilitate locating the record. 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 understanding that obtaining a record 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, D.C. 20511. Regulations governing access to one's records or for appealing an initial determination concerning access to records are contained in the ODNI regulation implementing the Privacy Act, 73 FR 16531 (March 28, 2008).

CONTESTING RECORD PROCEDURES:

As specified below, records in this system have been exempted from certain notification, access, and amendment procedures. Individuals seeking to correct or amend non-exempt records should direct their requests to the NCSC at the system manager address and according to the requirements set forth above under the heading "Record Access Procedures." Regulations regarding requests to amend, for disputing the contents of one's record, or for appealing initial determinations concerning these matters are contained in the ODNI Privacy Act regulation, 73 FR 16531 (March 28, 2008).

RECORD SOURCE CATEGORIES:

Records derived from human and record sources consulted in the course of investigating disclosure of sensitive or classified information.

EXEMPTIONS:

Records contained within 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) and (k)(2). Records may be exempted from these subsections or, additionally, from the requirements of subsections (c)(4); (e)(2),(3),(5),(8) and (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 protecting the record from disclosure remains valid and necessary.

SYSTEM NAME:

Revise system name as follows:

National Counterterrorism Center Current (ODNI/NCTC-005)

SECURITY CLASSIFICATION:

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

SYSTEM LOCATION:

National Counterterrorism Center (NCTC), Office of the Director of National Intelligence (ODNI), Washington, D.C. 20511.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals known or suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism or counterterrorism; and individuals who offer information pertaining to terrorism and counterterrorism. The system also contains information about individuals who have access to the system for counterterrorism purposes.

CATEGORIES OF RECORDS IN THE SYSTEM:

Classified and unclassified intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism; message traffic (cables); finished intelligence products and results of intelligence analysis, and reporting

(including law enforcement information); information gleaned through links to other systems, databases and collaborative features such as e-mail, communities of interest, and on-line chat rooms; information systems security analysis and reporting; publicly available information (including information contained in media reports and commercial databases); data concerning the providers of information; and information from other sources necessary to fulfill the mission of NCTC.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004); the National Security Act of 1947, as amended, 50 U.S.C. 401-442; Executive Order 13354, 69 Fed. Reg. 53,589 (2004); Executive Order 12333, as amended, 46 Fed. Reg. 59,941 (1981).

PURPOSE(S):

Revise current paragraph as follows:

National Counterterrorism Center Current is maintained for the purpose of compiling, assessing, analyzing, integrating, and disseminating information relating to terrorism and counterterrorism.

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 ODNI's Privacy Act Regulation published in 32 CFR part 1701 (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:

Electronic records are stored in secure files-servers located within secure facilities under the control of NCTC. Paper and other hard-copy records are stored in secured areas within the control of NCTC.

RETRIEVABILITY:

By name, social security number, or other identifier. Information may be retrieved from the System of Records by automated or hand searches based on existing indices and automated capabilities utilized in the normal course of business. Only authorized personnel with a need to know may search this system.

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 or contractor 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 government personnel and contractors holding appropriate security clearances and who have a valid business reason to access the records.

Communications are encrypted where required and other safeguards are in place to monitor and audit access and to detect intrusions. Backup tapes are maintained in a secure, off-site location.

RETENTION AND DISPOSAL:

Revise current paragraph as follows:

Pursuant to 44 U.S.C. 3303a(d) and 36 CFR Chapter 12, Subchapter B, Part 1228 – Disposition of Federal Records, records in this system will be dispositioned in accordance with records controls schedules N1-576-08-1; CT-4; and CT-5.

SYSTEM MANAGER(S) AND ADDRESS:

Revise current paragraph to read as follows:

NCTC Current System Manager, c/o Director, Information Management Division, Office of the Director of National Intelligence, Washington, D.C. 20511.

NOTIFICATION PROCEDURES:

As specified below, records in this system are exempt from certain notification, access, and amendment procedures. Individuals seeking to learn whether this system contains non-exempt 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:

Revise current paragraph as follows:

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."

Pursuant to ODNI's Privacy Act Regulation at 32 CFR 1701.7(d), requesters shall provide their full name and complete address, date and place of birth, citizenship status, alien registration number (if applicable), and date that status was acquired. Additional or clarifying information may be sought to ascertain identity. Requesters also must provide sufficient details to facilitate locating the record. The requester must sign the request and have it verified by a notary public. Alternately, the request may be submitted under 28 U.S.C. 1746, certifying the requester's identity and understanding that obtaining a record 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, D.C. 20511. Regulations governing access to one's records or for appealing an initial determination concerning access to records are contained in the ODNI regulation implementing the Privacy Act, 73 FR 16531 (March 28, 2008).

CONTESTING RECORD PROCEDURES:

Revise current paragraph to read as follows:

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 ODNI at the address and according to the requirements set forth above under the heading "Records Access Procedures."

Regulations governing access to and amendment of one's records or for appealing an initial determination concerning access to or amendment of records are contained in the ODNI regulation implementing the Privacy Act, 73 FR 16531 (March 28, 2008).

RECORD SOURCE CATEGORIES:

Information may be obtained from diplomatic, financial, military, homeland security, intelligence or law enforcement activities relating to counterterrorism or from any federal, state, or local government; foreign government information; private sector or public source material; information from other sources necessary to fulfill the mission of NCTC.

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) and (k)(2). 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.

SYSTEM NAME:

Analytic Resources Catalog (ARC) (ODNI-07)

SYSTEM CLASSIFICATION:

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

SYSTEM LOCATION:

Office of the Director of National Intelligence, Washington, DC 20511.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Current and former staff (employees, detailees, assignees and contractors) of the Intelligence Community (IC) elements, including military personnel and other federal employees with intelligence analysis duties.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records, including the Analyst Yellow Pages, reflecting the assignments, expertise, education, specialized foreign language and other skills, and experiences of federal government employees and contractors performing intelligence analysis duties; pre-set reports and other documentation about analytic resources at each IC element and across the IC.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The National Security Act of 1947, as amended, 50 USC 401-442; Executive Order 12333, as amended (73 FR 45325); and Executive Order 9397, as amended (73 FR 70239).

PURPOSE:

Records in this system are used to: locate IC and other intelligence analysts for collaborative activities; identify analysts authorized to access on-line collaboration zones; obtain information about the expertise, skills and educational backgrounds of IC and other intelligence analysts; obtain aggregate information about the use of analytic resources across the IC; and assist in management and planning functions of each IC element and of the IC as a whole.

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 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>). In addition, as routine uses specific to this system, the ODNI may disclose relevant ARC records to the following persons or entities and under the circumstances or for the purposes described below:

(a) A record from this system of records may be disclosed, as a routine use, to appropriately cleared and authorized staff of the IC elements in order to identify and locate intelligence analysts possessing specific expertise, skills or experiences for the purpose of collaborative analytic endeavors.

(b) A record from this system of records may be disclosed, as a routine use, to appropriately cleared and authorized staff of the IC elements whose responsibility it is to assess the depth and strength of the IC's analytic skills, expertise and experience and for other workforce management, budgeting or planning purposes.

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 facilities under control of the ODNI.

RETRIEVABILITY:

Records about individual analysts can be searched and retrieved based on name or other key word (e.g., degrees held, foreign language ability, country or intelligence area of specialization) pertinent to analytic expertise.

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 only authorized personnel or authorized and escorted visitors. Physical security protections include guards and locked facilities requiring badges and passwords for access. Records are accessed only by authorized government personnel and contractors holding an appropriate security clearance 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:

ARC Program Manager, c/o Director, Information Management, Office of the Director of National Intelligence, Washington, DC 20511.

NOTIFICATION PROCEDURES:

As specified below, records in this system are exempt from certain notification, access, and amendment procedures. Individuals seeking to learn whether this system contains non-exempt information about them ("notification") 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."

Requesters shall provide their full name and complete address. The requester must sign the request and have it verified by a notary public. Alternately, the request may be submitted under 28 U.S.C. 1746, certifying the requester's identity and understanding that obtaining a record under false pretenses constitutes a criminal offense. Requests for access to information must be addressed to the Director, Information Management, Office of the Director of National Intelligence, Washington, D.C. 20511. Regulations governing access to one's records or for appealing an initial determination concerning access to records are contained in the ODNI regulation implementing the Privacy Act.

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 ODNI at the address and according to the requirements set forth above under the heading "Records Access Procedures."

Regulations governing access to and amendment of one's records or for appealing an initial determination concerning access to or amendment of records are contained in the ODNI regulation implementing the Privacy Act.

RECORDS SOURCE CATEGORIES:

Records in the system are obtained directly from individual analysts and from their employing agencies' human resource information systems.

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). 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.

SYSTEM NAME:

Revise current paragraph to read as follows:

Office of Intelligence Community Equal Employment Opportunity and Diversity (IC EEO) Records (ODNI-10)

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, D.C. 20511.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Revise current paragraph to read as follows:

Individuals covered by this system of records include Office of the Director of National Intelligence (ODNI) current and former staff and contract employees, personal services independent contractors, employees of industrial contractors, military or civilian personnel detailed or assigned to the ODNI, Intergovernmental Personnel Act personnel detailed to the ODNI, and applicants for employment with the ODNI who: 1) have consulted an Equal Employment Opportunity (EEO) Counselor and/or filed a formal complaint alleging discrimination or reprisal; 2) initiated a harassment allegation with an appropriate supervisor or an EEO Counselor; 3) are the responding management official or witness in a discrimination or harassment complaint; 4) have made requests for reasonable accommodation or retirement on the basis of a disability.

CATEGORIES OF RECORDS IN THE SYSTEM

Revise current paragraph to read as follows:

Records relating to the EEO complaints process as directed by 29 CFR Part 1614, including: 1) information collected by an EEO counselor or investigator relating to EEO inquiries, allegations of discrimination or reprisal, and records relating to alternative dispute resolution; 2) sworn affidavits or statements from relevant witnesses; 3) documents, electronic communications, statistical summaries, investigative reports, and similar records. Records collected for consideration by the ODNI, the U.S. Equal Employment Opportunity Commission, or federal courts in rendering decisions under relevant laws or Executive Orders. Records also may include: information and communications relating to compliance activities resulting from decisions, opinions, recommendations, and settlement agreements; agency administrative files, internal and external communications, case disposition records, and records relating to procedural and substantive case management; records related to a report of harassment and formal inquiry, including statements of witnesses, reports of interviews, written summary of the inquiry, findings, recommendations, decisions, corrective action taken, and related correspondence; records relating to requests made by individuals or offices for reasonable accommodations based on disability (including medical records), notes or records made during consideration of requests, the products or services provided in response to such requests, and/or information related to the decisions for the denial or approval of a reasonable accommodation request, and records made to implement or track decisions on requests; and records regarding individuals who apply for retirement on the basis of medical disabilities.

In addition, information and records may be collected and retained for analysis, reporting, and review to comply with Executive and Legislative Branch requirements, or

as authorized by Intelligence Community Directives and Instructions as necessary to execute the duties of IC EEOD.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Revise current paragraph to read as follows:

The National Security Act of 1947, as amended, 50 USC 3002-3231; Title VII of the Civil Rights Act of 1964, as amended; the Equal Pay Act of 1963 (EPA), as amended; the Age Discrimination in Employment Act of 1967 (ADEA), as amended; the Rehabilitation Act of 1973, as amended; the Americans with Disabilities Act (ADA), as amended; the Genetic Information Non-Discrimination Act of 2008 (GINA); the Architectural Barriers Act of 1968, as amended; the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR Act); the Federal Records Act of 1950, as amended; U.S. Equal Employment Opportunity Commission Management Directives 110 and 715; 29 CFR Parts 1614, 1630 and 1635; 44 U.S.C. 3101 et. seq; Executive Order 12333, as amended (73 FR 45325); Executive Order 13526, as amended (75 FR 707); Executive Order 12968, as amended (73 FR 38103); Executive Order 13164 (65 FR 46565); Executive Order 11478 (34 FR 12985), as amended by Executive Order 13087 (63 FR 30097) and Executive Order 13152 (65 FR 26115); and Equal Employment Opportunity Commission's Policy Guidance on Executive Order 13164: Establishing Procedures to Facilitate the Provision of Reasonable Accommodation, Directives Transmittal Number 915.002, October 20, 2000.

PURPOSE(S):

Revise current paragraph to read as follows:

Records in this system enable the DNI to carry out lawful and authorized responsibilities under myriad statutes, regulations, and guidance governing equal employment opportunity. These records are maintained for the purpose of counseling, investigating, and adjudicating complaints of employment discrimination or reprisal; providing information for review by the Equal Employment Opportunity Commission, providing information for federal court review; conducting internal investigations into allegations of harassment and taking appropriate action; considering, deciding, implementing, and tracking requests for and action taken in response to requests for provision of reasonable accommodations based on medical disability, and processing Agency certification of reassignment and accommodations efforts to support Disability Retirement Packages.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

Revise current paragraph to read as follows:

See General Routine Uses Applicable to More Than One ODNI Privacy Act System of Records, Subpart C of 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:

Revise current paragraph to read as follows:

Paper records are stored in secured areas within the ODNI. Electronic records are stored in file servers located at secure government facilities.

RETRIEVABILITY:

Revise current paragraph to read as follows:

By name, and/or case number of the aggrieved person. By name of alleged discriminator or harasser. By name of the individual requesting reasonable accommodation or medical disability retirement. Information may be retrieved from this system of records by automated or hand search based on indices and automated capabilities utilized in the normal course of business. All searches of this system of records will be performed in ODNI offices by authorized personnel.

SAFEGUARDS:

Revise current paragraph to read as follows:

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 government personnel and contractors holding appropriate security clearances, and whose official duties require access to the records. The required use of password protection identification features and other system protection methods also restricts access to electronic information. Communications are encrypted where required and other safeguards are in place to monitor and audit access, and to detect intrusions. Backup tapes are maintained in a secure, off-site location.

RETENTION AND DISPOSAL:

Revise current paragraph to read as follows:

EEOD records covered by the National Archives and Records Control (NARA) General Records Schedule 1-24 through 1-27 will be retained and disposed according to those provisions, EEOC Management Directive 110, and EEOC's Policy Guidance on Executive Order 13164: Establishing Procedures to Facilitate the Provision of Reasonable Accommodation, Directives Transmittal Number 915.002, October 20, 2000. Any other EEOD records will be disposed of in accordance with NARA Control Schedule N1-576-11-9.

SYSTEM MANAGER(S) AND ADDRESS:

Revise current paragraph to read as follows:

Chief, Office of Intelligence Community Equal Employment Opportunity and Diversity,
Office of the Director of National Intelligence, Washington, D.C. 20511.

NOTIFICATION PROCEDURES:

As specified below, records in this system are exempt from certain notification, access, and amendment procedures. Individuals seeking to learn whether this system contains non-exempt 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:

Revise current paragraph to read as follows:

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."

Pursuant to the ODNI's Privacy Act Regulation at 32 CFR 1701.7(d), requesters shall provide their full name and complete address, date and place of birth, citizenship status, alien registration number (if applicable), and date that status was acquired. Additional or clarifying information may be sought to ascertain identity. Requesters also must provide sufficient details to facilitate locating the record. 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 understanding that obtaining a record 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, D.C. 20511. Regulations governing access to one's records or for appealing an initial determination concerning access to

records are contained in the ODNI regulation implementing the Privacy Act, 73 FR 16531 (March 28, 2008).

CONTESTING RECORD PROCEDURES:

Revise current paragraph to read as follows:

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 ODNI at the address and according to the requirements set forth above under the heading "Records Access Procedures."

Regulations governing access to and amendment of one's records or for appealing an initial determination concerning access to or amendment of records are contained in the ODNI regulation implementing the Privacy Act, 73 FR 16531 (March 28, 2008).

RECORD SOURCE CATEGORIES:

Revise current paragraph to read as follows:

Individuals covered by this system; individuals who provide information during the counseling/investigation of EEO complaints or during harassment inquiries; EEO Counselors; EEO investigators; Human Resource Officers; the EEOC, federal courts, and ODNI decision makers (e.g., supervisors); medical and psychiatric professionals; and the Office of Personnel Management.

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.

SYSTEM NAME:

Revise current system name to read as follows: Security Clearance Reform Research and Oversight Records (ODNI-13).

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, D.C. 20511.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Revise current paragraph to read as follows:

Present and former U.S. Government civilian employees, military members, contractor employees, experts, consultants, licensees, grantees, and applicants to any of the foregoing roles, or any other category of person who possesses or has sought eligibility

for a security clearance, or eligibility for a sensitive position; individuals whose names, exclusive of other information, are captured in publicly available data sets (including those obtained through subscription or fee).

CATEGORIES OF RECORDS IN THE SYSTEM:

Revise current paragraph to read as follows:

Investigation packages including but not limited to completed Standard Forms 85, 85P, 86, and 86C, or their successor forms, and associated authorization and consent forms; position designation records; financial disclosure forms; records of polygraph examinations (including reports, charts, tapes, and polygraph interviews notes); name-data sets obtained from publicly available sources, including those obtained for fee or by subscription; records from credit, criminal history, and any other records from databases and sources checked in the conduct of suitability determinations, or background investigations, reinvestigations, and continuous evaluations of persons under consideration for or retention in sensitive national security positions, including positions requiring eligibility for access to classified information under Executive Order 12968 or any successor order; background investigation reports and responses from personnel security-related interviews and questionnaires; non-disclosure agreements; adjudicative records including but not limited to adjudicative decisions, summaries of adjudicative decisions, supporting information, and adjudicative processes.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The National Security Act of 1947, as amended, 50 U.S.C. 3002, 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).

PURPOSE (S):

Revise current paragraph to read as follows:

To conduct oversight, research, development, and analyses for: (1) evaluating and improving U.S. Government personnel security programs, policies, and procedures; (2) assisting in providing training, instruction, and advice on personnel security vetting of subjects for U.S. Government elements; (3) encouraging cooperative research within and among U.S. Government elements on personnel security issues that have broad programmatic or policy implications and sharing best practices identified through these cooperative personnel security research initiatives; (4) identifying efficiencies, best practices, and cost saving opportunities for the conduct of personnel security programs across the Government; (5) evaluating the uniformity, quality, and efficiency of the conduct of personnel security investigations and adjudications, including analyses of reciprocal acceptance of such determinations; and (6) conducting pilot test projects regarding personnel security and related research in support of the mission of the Security Executive Agent.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND 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: Paper and other hard-copy records (computer output products, disks, etc.) are stored in secured areas maintained by the ODNI. Electronic records are stored in secure file servers located within secure facilities under the control of the ODNI.

RETRIEVABILITY:

Records are retrieved by name, social security number, or other unique identifier.

Information may be retrieved from this system of records by automated or hand search.

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 or contractor 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 when 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:

Revise current paragraph to read as follows:

Security Research or Oversight Program Manager, or their successor titles, c/o Director,
Information Management Division, Office of the Director of National Intelligence,
Washington, D.C. 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
non-exempt 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:

Revise current paragraph to read as follows:

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, D.C.

20511. Regulations governing access to one’s records or for appealing an initial determination concerning access to records are contained in the ODNI regulation implementing the Privacy Act, 73 FR 16531 (March 28, 2008).

CONTESTING RECORD PROCEDURES:

Revise current paragraph to read as follows:

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 ODNI 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 ODNI regulation implementing the Privacy Act, 73 FR 16531 (March 28, 2008).

RECORD SOURCE CATEGORIES:

Revise current paragraph to read as follows:

Records are obtained from the human resources, insider threat, and personnel security records of the departments and agencies of the Federal Government performing personnel security investigations or adjudications of persons under consideration for, or retention in, sensitive national security positions, including positions requiring eligibility for access to classified information under Executive Order 12968; other government data sources and publicly available commercial data sets; interviews with and questionnaires completed by covered individuals, references, and developed references; and information publicly available on the World Wide Web.

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.

SYSTEM NAME:

Office of the Director of National Intelligence (ODNI) Information Technology Systems Activity and Access Records (ODNI-19)

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, Washington, D.C. 20511.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who are authorized to use ODNI and Intelligence Community (IC) enterprise information technology resources.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records in this system include data on the use and attempted use of enterprise information technology resources by all individuals with access to these resources to include full content of audited events.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The National Security Act of 1947, as amended, 50 USC 401-442; the Counterintelligence Enhancement Act of 2002, as amended, 50 USC 402b; the Federal Records Act of 1950, as amended, 44 USC 3101 et seq.; the Computer Security Act of 1987, 40 USC 1441 note; Executive Order 12333, as amended (73 FR 45325); Executive Order 12968, as amended (73 FR 38103); and Executive Order 13526 (75 FR 707).

PURPOSE(S):

Data in this system will be used for evaluating the operational status, security, and performance of the information environment in support of business analytics, information security, counterintelligence, and law enforcement requirements (to include civil, criminal, and administrative investigative requirements).

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 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>). In addition, records from this system of records may be disclosed to Executive Branch departments or agencies for the purpose of evaluating usage trends, capabilities, misuse of, or threats to the ODNI and IC enterprise information resources.

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 the ODNI's facilities.

Paper records and other media are stored in secured areas within such facilities.

RETRIEVABILITY:

By name, user ID, e-mail address, or other unique identifying search term.

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 government personnel and contractors 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 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, or when applicable, GRS 24 and 27.

SYSTEM MANAGER(S) AND ADDRESS:

Revise current paragraph to read as follows:

Assistant Director of National Intelligence and IC Chief Information Officer; and
Director of Information Technology, Mission Support Directorate; c/o Director,
Information Management Division, Office of the Director of National Intelligence,
Washington, D.C. 20511.

NOTIFICATION PROCEDURES:

As specified below, records in this system are exempt from certain notification, access, and amendment procedures. Individuals seeking to learn whether this system contains non-exempt 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:

Revise current paragraph as follows:

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."

Pursuant to ODNI's Privacy Act Regulation at 32 CFR 1701.7(d), requesters shall provide their full name and complete address, date and place of birth, citizenship status, alien registration number (if applicable), and date that status was acquired. Additional or clarifying information may be sought to ascertain identity. Requesters also must provide sufficient details to facilitate locating the record. 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 understanding that obtaining a record 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, D.C. 20511. Regulations governing access to one's records or for appealing an initial determination concerning access to records are contained in the ODNI regulation implementing the Privacy Act, 73 FR 16531 (March 28, 2008).

CONTESTING RECORD PROCEDURES:

Revise current paragraph to read as follows;

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 ODNI 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 ODNI regulation implementing the Privacy Act, 73 FR 16531 (March 28, 2008).

RECORD SOURCE CATEGORIES:

ODNI and IC enterprise audit data.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Revise current paragraph as follows:

Records contained in this System of Records may be exempted from the requirements of subsections (c)(3); (d)(1),(2),(3),(4); (e)(1); (e)(4)(G),(H),(I); (f) and (h) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1), (k)(2) and (k)(5). Additionally, records may be exempted 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.

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, D.C. 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. 3303](#)(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, D.C. 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 non-exempt 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, D.C. 20511.

Regulations governing access to one's records or for appealing an initial determination concerning access to records are contained in the ODNI 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 ODNI 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 ODNI 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.

SYSTEM NAME:

National Counterintelligence System of Records

SYSTEM LOCATION:

National Counterintelligence Center, 3 WO1 NHB, Washington, D.C. 20505

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

- A. Individuals who are of foreign intelligence or foreign counterintelligence interest and relate in any manner to foreign intelligence threats to US national and economic security.
- B. Applicants for, and current and former personnel of NACIC.
- C. Individuals associated with NACIC administrative operations or services including pertinent functions such as training, contractors and pertinent persons related thereto.

CATEGORIES OF RECORDS IN THE SYSTEM:

1. Director's Correspondence: Correspondence whose contents relates to NACIC's mission, policies, or programs; and correspondence whose contents relates to routine, administrative, or facilitative matters.
2. NACIC Chronological Files: Copies of outgoing correspondence, memoranda, and other records signed by the Director, the Deputy

Director, and NACIC Office Chiefs. 3. Public Relations Files: Speeches or public statements made by the Director and Deputy Director. 4. NACIC Staff Meeting Records, agendas, minutes, and staff meeting highlights. 5. Progress Reports: six month progress reports submitted to the National Counterintelligence Policy Board outlining activities and accomplishments of the NACIC. 6. Compromised Names Database. The purpose of the database is to notify US intelligence community personnel whose names were potentially compromised as a result of espionage or other foreign intelligence collection activity. NACIC reviews pertinent reports to determine documents that were possibly passed in a particular case and then reviews those documents for names. The database contains the names of persons potentially compromised, date of the memo sent to the person or their employer informing them, the document number of where the person's name came from, document title, and document date. 7. Chronological Files of the PIO: Copies of correspondence, memoranda, and other records generated by PIO and its branches in assessing the effectiveness of CI operations, maintained for reference purposes. 8. Publications, Training Materials and Regional Seminars Records Maintained by PIO's Community Training Branch: Letters of acceptance, enrollment forms, thank you letters, list of attendees, list of speakers, notes, case studies, syllabus, training packet, magazine or newspaper articles, and other records used either for course development purposes or to facilitate the presentation of seminars. 9. Personnel Files: Individual personnel folders of staff employees, consultants and contract employee files consisting of papers documenting personnel actions; performance appraisals; correspondence; training documents; travel documents; contracts; justifications; memoranda; and administrative material. (Many of these files are maintained on a

temporary basis while the individuals are detailed to the NACIC. Upon their return to their home agency, their file is returned with them.) 10. Freedom of Information Act (FOIA)/Privacy Act (PA) Requests and Legal Fields: Files created in response for information under the FOIA/PA, consisting of the original request, a copy of the reply thereto, and all related supporting files which may include the official file copy of requested record or copy thereof; files created in response to administrative appeals for release of information denied by the NACIC, consisting of the appellant's letter, a copy of related supporting documents; FOIA/PA Control Files and Report Files; Files relating to an individual's request to amend a record pertaining to the individual as provided for under 5 U.S.C. 552a(d)(2), 552a(d)(3), and to any civil action brought by the individual against NACIC as provided under 5 U.S.C. 552a(g); Privacy Act Report files of recurring reports and one-time information requirements relating to agency implementation including biennial reports to the Office of Management and Budget, and Report on New Systems.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The Federal Records Act of 1950 Title 44, United States Code, Chapter 31, Section 3101; and Title 36, Code of Federal Regulations, Chapter XII, require Federal agencies to insure that adequate and proper records are made and preserved to document the organization, functions, policies, decisions, procedures and transactions and to protect the legal and financial rights of the Federal Government.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

(See Statement of General Routing Uses)

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

STORAGE:

Files are maintained in computerized form and hard copy form. Computerized form may be stored in memory, on disk storage, on computer tape, or on a computer printed listing.

RETRIEVABILITY:

Names are retrievable by automated word or hand search. NACIC will not permit any organization, public or private, outside the NACIC to have direct access to NACIC files. All searches on the NACIC data base and hard files will be performed on site, within NACIC space, by NACIC personnel.

SAFEGUARDS:

Records and databases are maintained in a restricted area within NACIC and are accessed only by NACIC personnel. All employees are checked to insure they have recent background investigations prior to being assigned to NACIC and are cautioned about divulging confidential information or any information contained in NACIC files. Failure to abide by these provisions may violate certain statutes providing maximum severe

penalties of a ten thousand-dollar fine or 10 years imprisonment, or both. Employees who resign or retire are also cautioned about divulging information acquired in their jobs. Registered mail is used to transmit routine hard copy records. Highly classified records are hand carried by employee personnel. Highly classified or sensitive privacy information, which is electronically transmitted between NACIC and other offices, is transmitted in encrypted form to prevent interception.

RETENTION AND DISPOSAL:

Records evaluated as historical and permanent will be transferred to the National Archives after established retention periods and administrative needs of the NACIC have elapsed.

SYSTEM MANAGER(S) AND ADDRESS:

Information and Privacy Coordinator, Executive Secretariat Office, National Counterintelligence Center, 3W01 NHB, Washington, D.C. 20505.

RECORD ACCESS PROCEDURES:

A request for access to a record from the system shall be made in writing with the envelope and the letter clearly marked "Privacy Access Request". Include in the request your full name, complete address, date of birth, place of birth, notarized signature, and other identifying data you may wish to furnish to assist in making a proper search of NACIC records. A request for access to records must describe the records sought in sufficient detail to enable NACIC personnel to locate the system of records containing

the record with a reasonable amount of effort. Whenever possible, a request for access should describe the nature of the record sought, and the date of the record or the period in which the record was compiled. The requester will also provide a return address for transmitting the information. Requests for access must be addressed to the Information and Privacy Coordinator, Executive Secretariat Office, National Counterintelligence Center, 3W01 NHB, Washington, D.C. 20505.

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend information maintained in the system should also direct their request to the Information and Privacy Coordinator, Executive Secretariat Office, National Counterintelligence Center, 3W01 NHB, Washington, DC. 20505.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Notice is hereby given that NACIC intends to exempt, from certain provisions of the Act, those systems of records which are (A) specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy and (B) are in fact, properly classified pursuant to such Executive Order. (5 U.S.C. 552(b)(1), as amended by Public Law 93-502) In addition, pursuant to authority granted in section (j) of the Privacy Act (5 U.S.C. 552a (j)) the Director of NACIC has determined (C) to exempt from notification under subsections (e)(4)(G) and (f)(1) those portions of each and all systems of records which have been exempted from individual access under subsection (j), in those cases where the Information and Privacy Coordinator, determines after advice by responsible components, that confirmation of the

existence of a record may jeopardize intelligence sources and methods. In such cases the NACIC may choose to neither confirm nor deny the existence of the record and may advise the individual that there is no record which is available to him pursuant to the Privacy Act of 1974.

[FR Doc. 2015-12764 Filed: 5/26/2015 08:45 am; Publication Date: 5/27/2015]