



This document is scheduled to be published in the Federal Register on 10/21/2015 and available online at <http://federalregister.gov/a/2015-26738>, and on FDsys.gov

Billing Code: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2015-OS-0100]

Privacy Act of 1974; System of Records

AGENCY: National Security Agency/Central Security Service, DoD.

ACTION: Notice to alter a System of Records.

SUMMARY: The National Security Agency/Central Security Service proposes to alter a system of records notice GNSA 18, entitled "Operations Records." This system is used to maintain records on foreign intelligence, counterintelligence, and information assurance/cybersecurity matters relating to the missions of the National Security Agency. The National Security Agency does not collect such records for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging individuals based on their ethnicity, race, gender, sexual orientation, or religion.

DATES: Comments will be accepted on or before [**INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER**]. This proposed action will be effective on the date following the end of the comment period unless comments are received which result in a contrary determination.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

* Federal Rulemaking Portal: <http://www.regulations.gov>.

Follow the instructions for submitting comments.

* Mail: Department of Defense, Office of the Deputy Chief Management Officer, Directorate of Oversight and Compliance, Regulatory and Audit Matters Office, 9010 Defense Pentagon, Washington, DC 20301-9010.

Instructions: All submissions received must include the agency name and docket number for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at <http://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Director, Civil Liberties and Privacy, Rebecca Richards, National Security Agency/Central Security Service, Civil Liberties and Privacy Office, Suite 6310, 9800 Savage Road, Ft. Meade, Maryland, 20755.

SUPPLEMENTARY INFORMATION: The Office of the Secretary of Defense notices for systems of records subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, have been published in the Federal Register and are available from the address in the

FOR FURTHER INFORMATION CONTACT or from the Defense Privacy and Civil Liberties Division website at <http://dpclld.defense.gov/>. The proposed systems reports, as required by 5 U.S.C. 552a(r) of the Privacy Act, as amended, were submitted on October 15, 2015 to the House Committee on Oversight and Government Reform, the Senate Committee on Homeland Security and Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to paragraph 4c of Appendix I to OMB Circular No. A-130, "Federal Agency Responsibilities for Maintaining Records About Individuals," dated February 8, 1996, (February 20, 1996, 61 FR 6427).

Dated: October 16, 2015.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

GNSA 18

System name:

Operations Records (November 30, 2010, 75 FR 74019)

Changes:

* * * * *

Categories of individuals covered by the system:

Delete entry and replace with "Individuals identified in foreign intelligence, counterintelligence, or information assurance/cybersecurity reports and supportive materials, including individuals involved in matters of foreign intelligence interest, information assurance/cybersecurity interest, the compromise of classified information, or terrorism."

Categories of records in the system:

Delete entry and replace with "Records may consist of any type of information acquired or maintained about an individual as NSA pursues its lawfully authorized missions, including but not limited to: an individual's name; Social Security Number (SSN); employee identification number; administrative information; biographic information when associated with an individual, such as phone number and email address; intelligence requirements; foreign intelligence, counterintelligence, and information assurance/cybersecurity analysis and reporting; operational records; articles, public-source data, and other published information on individuals and events of interest to NSA/CSS;

actual or purported compromises of classified intelligence; countermeasures in connection therewith; and identification of classified source documents and distribution thereof."

Authority for maintenance of the system:

Delete entry and replace with "National Security Agency Act of 1959, as amended (Pub. L. 86-36) (codified at 50 U.S.C. 3601 et seq.); the Foreign Intelligence Surveillance Act (FISA), as amended (Pub. L. 95-511) (codified at 50 U.S.C. 1801 et seq.); 44 U.S.C. 3541-3549, Federal Information Security Management (FISMA); E.O. 12333, as amended, United States intelligence activities; E.O. 13526, Classified National Security Information; National Security Directive 42, National Policy for the Security of National Security Telecommunications and Information Systems; and E.O. 9397 (SSN), as amended."

Purposes:

Delete entry and replace with "To maintain records on foreign intelligence, counterintelligence, and information assurance/cybersecurity matters relating to the missions of the National Security Agency.

The National Security Agency does not collect such records for the purpose of suppressing or burdening criticism or dissent, or

for disadvantaging individuals based on their ethnicity, race, gender, sexual orientation, or religion.”

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

Delete entry and replace with “In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended these records contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b) (3) as follows:

To U.S. Government agencies, including state and local agencies, and in some circumstances, foreign government agencies or their representatives, and private entities to provide, and in order to obtain, foreign intelligence, counterintelligence, information assurance/cybersecurity information, and other information, in accordance with applicable law and policy. The National Security Agency does not collect or provide such records to afford a competitive advantage to U.S. companies or U.S. business sectors commercially.

To U.S. Government officials regarding compromises of classified information including the document(s) apparently compromised,

implications of disclosure of intelligence sources and methods, investigative data on compromises, and statistical and substantive analysis of the data.

To any U.S. Government or foreign government organization in order to facilitate any security, employment, detail, liaison, or contractual decision by any U.S. Government organization.

To the President's Foreign Intelligence Advisory Board, the Intelligence Oversight Board, and the Privacy and Civil Liberties Oversight Board, and any successor organizations, when requested by those entities, or when NSA/CSS determines that disclosure will assist in oversight functions.

Records may further be disclosed to agencies involved in the protection of intelligence sources and methods to facilitate such protection and to support intelligence analysis and reporting.

The DoD Blanket Routine Uses set forth at the beginning of the NSA/CSS compilation of systems of records notices may apply to this system. The complete list of DoD blanket routine uses can be found online at:

<http://dpcl.d.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses>
s"

* * * * *

Retrievability:

Delete entry and replace with "Information may be retrieved by any unique identifier or other criteria, to include an individual's name, Social Security Number (SSN), and/or employee identification number."

Safeguards:

Delete entry and replace with "Buildings are secured by a series of guarded pedestrian gates and checkpoints. Access to facilities is limited to security-cleared personnel and escorted visitors only. Within the facilities themselves, access to paper records and computer printouts are controlled by limited-access facilities and lockable containers. Access to electronic records is controlled by computer password protection and those who are cleared on a need to know basis in the performance of their duties."

Retention and disposal:

Delete entry and replace with "SIGINT Operational Data: Temporary, review annually for destruction.

SIGINT Collection Records: Temporary, close inactive files annually and transfer to the NSA/CSS Records Center. Review every 5 years for destruction.

SIGINT Analysis Information and Records: Permanent, transfer to the NSA/CSS Records Center when 5 years old, transfer to the NSA/CSS Archives after 20 years, and transfer to the National Archives and Records Administration when 25 years old.

SIGINT Product: Permanent, transfer to NSA/CSS Records Center when 5 years old, transfer to the NSA/CSS Archives after 20 years, and transfer to the National Archives and Records Administration when 50 years old.

Counterintelligence Records: Permanent, transfer to the NSA/CSS Records Center when 3 years old, transfer to the NSA/CSS Archives when 20 years old, and transfer to the National Archives and Records Administration when 25 years old.

Information Assurance and Communication Security data: Temporary, review every year for destruction.

Information Assurance and Communications Security Monitoring Reports: Permanent, transfer to the NSA/CSS Records Center when 5 years old, transfer to the NSA/CSS Archives when 20 years old, and transfer to the National Archives and Records Administration when 25 years old."

* * * * *

Record source categories:

Delete entry and replace with "Individuals themselves; U.S. agencies and organizations; media, including periodicals, newspapers, and broadcast transcripts; public and classified sources; intelligence source documents; investigative reports; and correspondence."

Exemptions claimed for the system:

Delete entry and replace with "Information specifically authorized to be classified under E.O. 13526, as implemented by DoDM 5200.1, may be exempt pursuant to 5 U.S.C. 552a(k)(1).

Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2).

However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identity of a confidential source. NOTE: When

claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

An exemption rule for this record system has been promulgated according to the requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c) and (e) and published in 32 CFR part 322. For additional information contact the system manager."

GNSA 18

System name:

Operations Records.

System location:

National Security Agency/Central Security Service, Ft. George G. Meade, MD 20755-6000.

Categories of individuals covered by the system:

Individuals identified in foreign intelligence, counterintelligence, or information assurance/cybersecurity reports and supportive materials, including individuals involved in matters of foreign intelligence interest, information assurance/cybersecurity interest, the compromise of classified information, or terrorism.

Categories of records in the system:

Records may consist of any type of information acquired or maintained about an individual as NSA pursues its lawfully authorized missions, including but not limited to: an individual's name; Social Security Number (SSN); employee identification number; administrative information; biographic information when associated with an individual, such as phone

number and email address; intelligence requirements; foreign intelligence, counterintelligence, and information assurance/cybersecurity analysis and reporting; operational records; articles, public-source data, and other published information on individuals and events of interest to NSA/CSS; actual or purported compromises of classified intelligence; countermeasures in connection therewith; and identification of classified source documents and distribution thereof.

Authority for maintenance of the system:

National Security Agency Act of 1959, as amended (Pub. L. 86-36) (codified at 50 U.S.C. 3601 et seq.); the Foreign Intelligence Surveillance Act (FISA), as amended (Pub. L. 95-511) (codified at 50 U.S.C. 1801 et seq.); 44 U.S.C. 3541-3549, Federal Information Security Management (FISMA); E.O. 12333, as amended, United States intelligence activities; E.O. 13526, Classified National Security Information; National Security Directive 42, National Policy for the Security of National Security Telecommunications and Information Systems; and E.O. 9397 (SSN), as amended.

Purpose(s):

To maintain records on foreign intelligence, counterintelligence, and information assurance/cybersecurity

matters relating to the missions of the National Security Agency.

The National Security Agency does not collect such records for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging individuals based on their ethnicity, race, gender, sexual orientation, or religion.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended these records contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b) (3) as follows:

To U.S. Government agencies, including state and local agencies, and in some circumstances, foreign government agencies or their representatives, and private entities to provide, and in order to obtain, foreign intelligence, counterintelligence, information assurance/cybersecurity information, and other information, in accordance with applicable law and policy. The National Security Agency does not collect or provide such

records to afford a competitive advantage to U.S. companies or U.S. business sectors commercially.

To U.S. Government officials regarding compromises of classified information including the document(s) apparently compromised, implications of disclosure of intelligence sources and methods, investigative data on compromises, and statistical and substantive analysis of the data.

To any U.S. Government or foreign government organization in order to facilitate any security, employment, detail, liaison, or contractual decision by any U.S. Government organization.

To the President's Foreign Intelligence Advisory Board, the Intelligence Oversight Board, and the Privacy and Civil Liberties Oversight Board, and any successor organizations, when requested by those entities, or when NSA/CSS determines that disclosure will assist in oversight functions.

Records may further be disclosed to agencies involved in the protection of intelligence sources and methods to facilitate such protection and to support intelligence analysis and reporting.

The DoD 'Blanket Routine Uses' published at the beginning of the NSA/CSS' compilation of systems of records notices apply to this system.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Paper records in file folders and electronic storage media.

Retrievability:

Information may be retrieved by any unique identifier or other criteria, to include an individual's name, Social Security Number (SSN), and/or employee identification number.

Safeguards:

Buildings are secured by a series of guarded pedestrian gates and checkpoints. Access to facilities is limited to security-cleared personnel and escorted visitors only. Within the facilities themselves, access to paper records and computer printouts are controlled by limited-access facilities and lockable containers. Access to electronic records is controlled

by computer password protection and those who are cleared on a need to know basis in the performance of their duties.”

Retention and disposal:

SIGINT Operational Data: Temporary, review annually for destruction.

SIGINT Collection Records: Temporary, close inactive files annually and transfer to the NSA/CSS Records Center. Review every 5 years for destruction.

SIGINT Analysis Information and Records: Permanent, transfer to the NSA/CSS Records Center when 5 years old, transfer to the NSA/CSS Archives after 20 years, and transfer to the National Archives and Records Administration when 25 years old.

SIGINT Product: Permanent, transfer to NSA/CSS Records Center when 5 years old, transfer to the NSA/CSS Archives after 20 years, and transfer to the National Archives and Records Administration when 50 years old.

Counterintelligence Records: Permanent, transfer to the NSA/CSS Records Center when 3 years old, transfer to the NSA/CSS Archives when 20 years old, and transfer to the National Archives and Records Administration when 25 years old.

Information Assurance and Communication Security data:

Temporary, review every year for destruction.

Information Assurance and Communications Security Monitoring

Reports: Permanent, transfer to the NSA/CSS Records Center when 5 years old, transfer to the NSA/CSS Archives when 20 years old, and transfer to the National Archives and Records Administration when 25 years old.

System manager(s) and address:

Director, National Security Agency/Central Security Service, Ft. George G. Meade, MD 20755-6000.

Notification procedure:

Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to the National Security Agency/Central Security Service, Freedom of Information Act/Privacy Act Office, 9800 Savage Road, Suite 6248, Ft. George G. Meade, MD 20755-6248.

Written inquiries should contain the individual's full name, address and telephone number.

Record access procedures:

Individuals seeking access to information about themselves contained in this system should address written inquiries to the National Security Agency/Central Security Service, Freedom of Information Act/Privacy Act Office, 9800 Savage Road, Suite 6248, Ft. George G. Meade, MD 20755-6248.

Written inquiries should contain the individual's full name, address and telephone number.

Contesting record procedures:

The NSA/CSS rules for contesting contents and appealing initial determinations are published at 32 CFR part 322 or may be obtained by written request addressed to the National Security Agency/Central Security Service, Freedom of Information Act/Privacy Act Office, 9800 Savage Road, Suite 6248, Ft. George G. Meade, MD 20755-6248.

Record source categories:

Individuals themselves; U.S. agencies and organizations; media, including periodicals, newspapers, and broadcast transcripts; public and classified sources; intelligence source documents; investigative reports; and correspondence.

Exemptions claimed for the system:

Information specifically authorized to be classified under E.O. 13526, as implemented by DoDM 5200.1, may be exempt pursuant to 5 U.S.C. 552a(k)(1).

Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identity of a confidential source. NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

An exemption rule for this record system has been promulgated according to the requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c) and (e) and published in 32 CFR part 322. For additional information contact the system manager.

[FR Doc. 2015-26738 Filed: 10/20/2015 08:45 am; Publication Date: 10/21/2015]