DATES caption to read: March 15, 2005 from 0900 to 1700 and March 16, 2005 from 0800 to 1525.

Dated: February 28, 2005.

Jeannette Owings-Ballard,

OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 05–4371 Filed 3–4–05; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

National Reconnaissance Office; Privacy Act of 1974; System of Records.

AGENCY: National Reconnaissance Office.

ACTION: Notice to alter a system of records.

SUMMARY: The National Reconnaissance Office is altering a system of records notice in its existing inventory of record systems subject to the Privacy Act of 1974, (5 U.S.C. 552a), as amended.

DATES: This proposed action will be effective without further notice April 6, 2005, unless comments are received which result in a contrary determination.

ADDRESSES: Send comments to the FOIA/Privacy Official, National Reconnaissance Office, Information Access and Release, 14675 Lee Road, Chantilly, VA 20151–1715.

FOR FURTHER INFORMATION CONTACT: Contact the FOIA/NRO Privacy Official at (703) 227–9128.

SUPPLEMENTARY INFORMATION: The National Reconnaissance Office systems of records notices 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 above.

The proposed system report, as required by 5 U.S.C. 552a(r) of the Privacy Act of 1974, as amended, was submitted on February 1, 2005, to the House Committee on 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: February 25, 2005.

Jeannette Owings-Ballard,

OSD Federal Register Liaison Officer, Department of Defense.

QNRO–21

SYSTEM NAME:

Personnel Security Files (January 14, 2002, 67 FR 1741).

CHANGES:

* * * * *

CATEGORIES OF RECORDS IN THE SYSTEM:

Add to end of entry 'and security incident records, such as the security file number, user id, date resolved, case id, case manager, government point of contact, incident report date, incident report type, date notified, reporter's name, affiliation, employer, officer, information systems security officer name and phone number, manager name and phone number, program security officer name and phone number, date of incident, location where incident occurred, incident type and description, names of personnel involved with incident along with their social security number, office, affiliation, employer, and phone number, incident category, classification of data, name of person who classified it, including identification number, title, position, organization, phone number, person who verified classification level of data, their title, position, organization, phone number and source used to verify classification, data owner name, their title, position, organization, phone number, date notified, date classification confirmed, number of individuals and organizations with unauthorized access to information and their clearance level, organization that caused the unauthorized disclosure, nature of unauthorized disclosure, where file originated, how data was introduced into computer system, file name, size, type and whether action warrants notification of the Director of Central Intelligence.'

* * * * *

PURPOSE(S):

Add a new paragraph to entry 'The system will provide a centrally managed security incident database for NRO security managers. The user will be the primary reporter of the information. This will also be a tool to ensure incidents are identified, documented, tracked, investigated, responded to, adjudicated, and corrected, in a standard and timely manner.'

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

Add a new paragraph 'To the Intelligence Community to review the records, in the form of statistics only, for the purpose of providing trend analysis, disseminating threat information, providing reports of IT threats, any issues affecting mission critical networks, informing them of unauthorized disclosures or any compromise of intelligence information in accordance with applicable law.'

RETRIEVABILITY:

Add to entry 'type of incident, Case ID, Case Manager, and responsibility Program Security Officer.'

RETENTION AND DISPOSAL:

Delete entry and replace with 'Security case records are temporary, retained for 15 years after inactivation; noteworthy files are retained for 25 years after inactivation. Security incident records are temporary, retained for 5 years after inactivation. Audio and videotapes of polygraph examinations and interviews are temporary and are re-used or destroyed when superseded, obsolete, or no longer needed.'

* * * * *

SYSTEM MANAGER(S) AND ADDRESS:

Add to entry 'Deputy Director of Administration, Office of Security, Chief of Security Policy Staff.'

* * * * *

QNRO–21

SYSTEM NAME:

Personnel Security Files.

SYSTEM LOCATION:

Office of Security, Personnel Security Division, National Reconnaissance Office, 14675 Lee Road, Chantilly, VA 20151–1715.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

National REconnaissance Office (NRO) civilian, military and contractor personnel who have been nominated or investigated for security clearances and program accesses.

CATEGORIES OF RECORDS IN THE SYSTEM:

'Name, Social Security Number, agency identification number, employee's geographic work location, employer, work telephone number, date and place of birth, home address and home telephone number, dependents' names, individual's background investigation and polygraph data, interview and adjudication information, all other information such as that found

on standard government forms SF 86 and 1879, appeal and referral data, program access status, classification number, the security file location, and administrative and investigatory comments and security incident records, such as the security file number, user id, date resolved, case id, case manager, government point of contact, incident report date, incident report type, date notified, reporter's name, affiliation, employer, officer, information systems security officer name and phone number, manager name and phone number, program security officer name and phone number, date of incident, location where incident occurred, incident type and description, names of personnel involved with incident along with their social security number, office, affiliation, employer, and phone number, incident category, classification of data, name of person who classified it, including identification number, title, position, organization, phone number, person who verified classification level of data, their title, position, organization, phone number and source used to verify classification, data owner name, their title, position, organization, phone number, date notified, date classification confirmed, number of individuals and organizations with unauthorized access to information and their clearance level, organization that caused the unauthorized disclosure, nature of unauthorized disclosure, where file originated, how data was introduced into computer system, file name, size, type and whether action warrants notification of the Director of Central Intelligence.'

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

National Security Act of 1947, as amended, 50 U.S.C. 401 *et seq.;* 5 U.S.C. 301 Departmental Regulations; E.O. 12333; E.O. 12958; E.O. 12968; and E.O. 9397 (SSN).

PURPOSE(S):

The information is used for grant in security program accesses to NRO personnel; to maintain, support, and track personnel security administrative processing; to provide data for day-to-day security functions; and to conduct security investigations. The system also provides a centrally managed security incident database for NRO security managers. The user will be the primary reporter of the information to enable an accurate overall view of incident response activities. This will also be a tool to ensure incidents are identified, documented, tracked, investigated, responded to, adjudicated, and corrected, in a standard and timely manner.

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, these records or information contained therein may specifically be disclosed outside the NRO as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: To contractors and other Federal agencies for purposes of protecting the security of NRO installations, activities, property, and employees; to facilitate and verify an individual's eligibility to access classified information; and to protect the interests of National Security. The NRO Director of Security or his/her designee must approve disclosure in writing.

To the Intelligence Community to review the records, in the form of statistics only, for the purpose of providing trend analysis, disseminating threat information, providing reports of IT threats, any issues affecting mission critical networks, informing them of unauthorized disclosures or any compromise of intelligence information in accordance with applicable law.

The DoD 'Blanket Routines Uses' published at the beginning of the NRO 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 files and automated information system, maintained in computers and computer output products.

RETRIEVABILITY:

Name, Social Security Number, agency identification number, employer, employee's geographic work location, date and place of birth, administrative comments, type of incident, Case ID, Case Manager, and responsibility Program Security Officer.

SAFEGUARDS:

Records are stored in a secure, gated facility, guard, badge, and password access protected. Access to and use of these records are limited to security staff whose official duties require such access.

RETENTION AND DISPOSAL:

Security case records are temporary, retained for 15 years after inactivation; noteworthy files are retained for 25 years after inactivation. Security incident records are temporary, retained for 5 years after inactivation. Audio and videotapes of polygraph examinations and interviews are temporary and are reused or destroyed when superseded, obsolete, or no longer needed.

SYSTEM MANAGER(S) AND ADDRESS:

Chief, Personnel Security Division, Office of Security, National Reconnaissance Office, 14675 Lee Road, Chantilly, VA 20151–1715.

Chief, Security Policy Staff, Office of Security, Deputy Director of Administration, National Reconnaissance Office, 14675 Lee Road, Chantilly, VA 20151–1715.

NOTIFICATION PROCEDURE:

Individuals seeking to determine whether this system of records contains information about themselves should address written inquiries to the National Reconnaissance Office, Information Access and Release Center, 14675 Lee Road, Chantilly, VA 20151–1715.

Request should include full name and any aliases or nicknames, address, Social Security Number, current citizenship status, and date and place of birth, and other information identifiable from the record.

In addition, the requester must provide a notarized statement or an unsworn declaration in accordance with 28 U.S.C. 1746, in the following format:

If executed without the United States: I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).

If executed within the United States, its territories, possessions, or commonwealths: I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).

RECORD ACCESS PROCEDURES:

Individuals seeking to access information about themselves contained in this system should address written inquiries to the National Reconnaissance Office, Information Access and Release Center, 14675 Lee Road, Chantilly, VA 20151–1715.

Request should include full name and any aliases or nicknames, address, Social Security Number, current citizenship status, and date and place of birth, and other information identifiable from the record.

In addition, the requester must provide a notarized statement or an unsworn declaration in accordance with 28 U.S.C. 1746, in the following format:

If executed without the United States: I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the

foregoing is true and correct. Executed on (date). (Signature).

If executed within the United States, its territories, possessions, or commonwealths: I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).

CONTESTING RECORD PROCEDURES:

The NRO rules for accessing records, for contesting contents and appealing initial agency determinations are published in NRO Directive 110–3A and NRO Instruction 110–5A; 32 CFR part 326 or may be obtained from the Privacy Act Coordinator, National Reconnaissance Office, 14675 Lee Road, Chantilly, VA 20151–1715.

RECORD SOURCE CATEGORIES:

Information is supplied by the individual, by persons other than the individual, and by documentation gathered in the background investigation, and other government agencies.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Investigatory material compiled for law enforcement purposes 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 such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source.

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 exemption has been promulgated in accordance with requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c) and (e) and published in 32 CFR part 326. For additional information contact the system manager.

[FR Doc. 05–4368 Filed 3–4–05; 8:45 am]

BILLING CODE 5001–06–M

DEPARTMENT OF DEFENSE

Department of the Army

Privacy Act of 1974; System of Records; correction

AGENCY: Department of the Army, DoD

ACTION: Notice to amend system of records; correction.

SUMMARY: The Department of Defense published a document in the **Federal Register** of February 25, 2005, the Department of the Army is proposing to amend the Preamble to its Compilation of Privacy Act systems of records notices by updating the telephone number of the *Point of Contact*. The point of contact and phone number is incorrect.

FOR FURTHER INFORMATION CONTACT: Ms. Janice Thornton at (703) 428–6497.

Correction

In the **Federal Register** of February 25, 2005, in FR Doc. 25fe05–61, on pages 9289, in the first column, correct the ''Point of Contact'' to read:

''*Point of Contact:* Ms. Janice Thornton at 703–428–6497; DSN: 328–6497.''

Dated: February 28, 2005.

Jeannette Owings-Ballard,

OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 05–4373 Filed 3–4–05; 8:45 am]

BILLING CODE 5001–06–M

DEPARTMENT OF DEFENSE

Department of the Navy

Privacy Act of 1974; System of Records

AGENCY: Department of the Navy, DoD.

ACTION: Notice to add systems of records.

SUMMARY: The Department of the Navy proposes to add a system of records notice to its inventory of record systems subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended.

DATES: This action will be effective on April 6, 2005, unless comments are received that would result in a contrary determination.

ADDRESSES: Send comments to the Department of the Navy, PA/FOIA Policy Branch, Chief of Naval Operations (DNS–36), 2000 Navy Pentagon, Washington, DC 20350–2000.

FOR FURTHER INFORMATION CONTACT: Mrs. Lama at 202–685–6545.

SUPPLEMENTARY INFORMATION: The Department of the Navy's record system notices for records systems, 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 above.

The proposed systems reports, as required by 5 U.S.C. 552a(r) of the Privacy Act, were submitted on January 26, 2005, to the House Committee on 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, (61 FR 6427, February 20, 1996).

Dated: February 28, 2005.

Jeannette Owings-Ballard,

OSD Federal Register Liaison Officer, Department of Defense.

NM05100–5

SYSTEM NAME:

Enterprise-wide Safety Applications Management System (ESAMS).

SYSTEM LOCATION:

HGW and Associates, LLCI, Suite A–100, 9000 Executive Park Drive, Knoxville, TN 37923–4685 and organizational elements of the Department of the Navy. Official mailing addresses are published in the Standard Navy Distribution List that is available at *http://ned.daps.dla.,mil/sndl.htm.*

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Department of the Navy military and civilian personnel, non-appropriated personnel, and foreign national civilian personnel.

CATEGORIES OF RECORDS IN THE SYSTEM:

Name, Social Security Number, date of birth, job title, rank/rate/grade, civilian/military indicator, unit identification code (UIC) , activity name, major command code, department, sex, job title, OSH training received, test scores, occupational medical stressors, medical physical dates and non-medically sensitive results, respirator usage and fit test results, chemical and/or environmental exposures, and occupational injuries/illnesses.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 4101–4118, the Government Employees Training Act of 1958; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5042, Commandant of the Marine Corps; E.O. 12196, Occupational Safety and Health Programs for Federal Employees; and DoD Instruction 6055.7, Accident Investigation, Reporting, and Record Keeping; and E.O. 9397 (SSN).

PURPOSE(S):

The Department of the Navy is proposing to establish a system of