published in the Standard Navy Distribution List that is available at *http://doni.daps.dla.mil/sndl.aspx*.

NOTIFICATION PROCEDURE:

Individuals seeking to determine whether this system of records contains information about themselves should address written inquiries to the Commanding Officer or head of the activity where assigned. Official mailing addresses are published in the Standard Navy Distribution List that is available at *http://doni.daps.dla.mil/sndl.aspx*.

Written requests should contain the individual's full name, Social Security Number (SSN), and the request must be signed.

RECORD ACCESS PROCEDURES:

Individuals seeking access to records about themselves should address written inquiries to the Commanding Officer or head of the activity where assigned. Official mailing addresses are published in the Standard Navy Distribution List that is available at *http://doni.daps.dla.mil/sndl.aspx*.

Written requests should contain the individual's full name, Social Security Number (SSN), and the request must be signed.

CONTESTING RECORD PROCEDURES:

The Navy's rules for accessing records, and for contesting contents and appealing initial agency determinations are published in Secretary of the Navy Instruction 5211.5; 32 CFR part 701; or may be obtained from the system manager.

RECORD SOURCE CATEGORIES:

Individual concerned, driving record, insurance papers, activity correspondence, investigators reports, and witness statements.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[FR Doc. E8–7615 Filed 4–9–08; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Department of the Navy

[USN–2008–0027]

Privacy Act of 1974; System of Records

AGENCY: Department of the Navy, DoD.

ACTION: Notice to Alter a System of Records.

SUMMARY: The Department of the Navy proposes to alter a system of records notice in its existing inventory of records systems subject to the Privacy Act of 1974, (5 U.S.C. 552a), as amended. The alteration consists of redefining the purpose and routine uses for the system.

DATES: This proposed action will be effective without further notice on May 12, 2008 unless comments are received which 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. Doris Lama at (202) 685–325–6545.

SUPPLEMENTARY INFORMATION: The Department of the Navy's 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 reports, as required by 5 U.S.C. 552a(r), of the Privacy Act of 1974, as amended, was submitted on March 28, 2008, 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: April 4, 2008.

L.M. Bynum,

Alternate, OSD Federal Register Liaison Officer, Department of Defense.

N05520–4

SYSTEM NAME:

NCIS Investigative Files System (June 30, 1998, 63 FR 35575).

CHANGES:

* * * * *

SYSTEM LOCATION:

Delete para 2 and replace with ''Decentralized Segments—Located at the Naval Criminal Investigative Service (NCIS) Field Offices (FO), Resident Agencies (RA), and Polygraph sites worldwide. Law Enforcement Information Exchange (LInX) secure remote computer server sites. Naval Criminal Investigative Service Regional Offices retain copies of certain portions of some investigative files and related documentation. The number and location of these Naval Criminal Investigative Service Field Offices, Naval Criminal Investigative Service Resident Agencies, and Polygraph sites are subject to change in order to meet the requirements of the Department of the Navy.''

Delete para 3.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Delete para 2 and replace with ''Active, reserve, and inactive members of the naval service; civilians, to include applicants for employment with NCIS; both citizen and alien employees located in both the U.S. and in overseas areas and including temporary, part-time, and advisory personnel employed by the Department of the Navy; industrial and contractor personnel; civilian personnel being considered for sensitive positions, boards, conferences, etc. Civilian personnel who worked or resided overseas, e.g., Red Cross personnel. Civilian and military personnel accused, suspected, a witness to, or victims of felonious type offenses, or lesser offenses impacting on the good order, discipline, morale or security of the Department of the Navy; civilian personnel seeking access to or seeking to conduct or operate any business or other function aboard a Department of the Navy installation, facility or ship; civilians and civilian or military personnel who are subjects, co-subjects, witnesses, and victims in law enforcement and investigative cases in which law enforcement and investigative authorities (Federal, state, local, tribal, and foreign) have requested laboratory analysis of submitted evidence for law enforcement purposes; civilian or military personnel involved in the loss, compromise, or unauthorized disclosure of classified material/information; civilian and military personnel who were/are of counterintelligence interest to the Department of the Navy. Persons under investigation and parties to the communications whose communications have been intercepted during wire, electronic or oral surveillance operations conducted by or on behalf of NCIS.''

CATEGORIES OF RECORDS IN THE SYSTEM:

Delete and replace with ''Official investigative reports prepared by NCIS, DON, Department of Defense (DoD), or other Federal, state, local, tribal, or foreign law enforcement or investigative bodies.

Biographic data, intelligence/counterintelligence debriefing reports, information concerning U.S. personnel who are missing, captured, or detained by a hostile entity. The information may be of criminal, counterintelligence, or general investigative interest.

Preliminary Investigation Reports (PIR) document receipt of information that at the initial stage indicates an incident occurred involving one or more criminal offenses, however it was subsequently determined that no criminal offense occurred or that the incident and offenses did not fall within NCIS' jurisdiction and or responsibility to investigate.

Polygraph Data.

A listing of persons who submitted to polygraph examination by NCIS examiners. The data includes the examinee's name, location and results of the examination and the identity of the examiner. Also, copies of examination records created in support of criminal investigations. This data includes statistical and technical data sheets, questions sheets, charts, numerical evaluation forms, subject statements, consent forms, medical waivers, interview logs, personal data sheets, and related documents.

Case Control and Management documents which serve as the basis for recording, conducting, controlling, and guiding the investigative activity. Records identifying confidential sources and contacts with them. Index to persons reported by 'Name Only.'

Forensic Laboratory Report Records. Records reporting and documenting laboratory analysis of submitted evidence. Fingerprint Card Files. Fingerprint card and related correspondence obtained by DON designated law enforcement officials and submitted to NCIS Headquarters for quality review and forwarding to the Federal Bureau of Investigations in support of criminal investigations.

Personnel Security and Suitability Investigations. Requests for and results of investigations or inquiries conducted by U.S. Navy or other DoD, Federal, state, or local investigative agency. Record includes: Personal history statements; fingerprint cards; personnel security questionnaire; medical and/or educational records and waivers for release; requests for and National Agency checks; local agency checks; military records; birth records; employment records; credit records and waivers for release; interviews of education, employment, and credit references; interviews of listed and developed character references; interviews of neighbors; and other similar records.''

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Delete entry and replace with ''10 U.S.C. 5013, Secretary of the Navy; 18 U.S.C. 2510–2520 and 3504; 47 U.S.C. 605; DoD Directive 5210.48, Polygraph and Credibility Assessment Program; DoD Regulation 5240.1–R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons; DoD Directive 5505.9, Interception of Wire, Electronic, and Oral Communications for Law Enforcement; Secretary of the Navy Instruction 5430.107, Mission and Functions of the Naval Criminal Investigative Service; Secretary of the Navy M–5510.30, Department of the Navy Personnel Security Program; Secretary of the Navy M–5510.36, Department of the Navy Information Security Program; OPNAVINST 5530.14, Navy Physical Security and Law Enforcement; MCO 558.2, Law Enforcement Manual; E.O. 9397 (SSN); E.O. 10450, Security Requirements for Government Employees, in particular sections 2, 3, 4, 5, 6, 7, 8, 9, and 14; and E.O. 12333, United States Intelligence Activities.''

PURPOSE(S):

Delete para 2 and replace with ''The records in this system are used for the following purposes: suitability for access or continued access to classified information; suitability for promotion, employment, or assignment; suitability for access to military installations or industrial firms engaged in government projects/contracts; suitability for awards or similar benefits; use in current law enforcement investigation or program of any type including applicants; use in judicial or adjudicative proceedings including litigation or in accordance with a court order; to assist Federal, state, and local agencies that perform law enforcement or quasi-law enforcement functions; to assist Federal, state, and local agencies that perform victim/witness assistance services, child protection services or family support or sailor services; insurance claims including workmen's compensation; provide protective operations under the DoD Distinguished Visitor Protection Program and to assist the U.S. Secret Service in meeting its responsibilities; assist local law enforcement agencies in meeting their responsibilities for complying with Congressionally mandated records checks such as Brady Handgun Violence Prevention Act checks; used for public affairs or publicity purposes such as wanted persons announcements, etc.; referral of matters under their cognizance to Federal, state or local law enforcement authorities including criminal prosecution, civil court action or regulatory order; advising higher authorities and naval commands of the important developments impacting on security, good order or discipline; reporting of statistical data to naval commands and higher authority; input into the Defense Security Service managed Defense Clearance Index of Investigations (DCII) database under system notice V5–02. Wire, Electronic, and Oral Interceptions Index is maintained to enable NCIS to quickly locate records of intercept activities in response to motions for discovery and inquiries.''

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, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

(1) To any criminal, civil, or regulatory law enforcement authority (whether Federal, state, local, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.

(2) To a governmental entity lawfully engaged in collecting criminal law enforcement, criminal law enforcement intelligence, or national security intelligence information for law enforcement or intelligence purposes.

(3) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records.

(4) In an appropriate proceeding before a court, or administrative or adjudicative body, when NCIS determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

(5) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings.

(6) To a former employee of NCIS for purposes of: Responding to an official inquiry by a Federal, state, or local government entity or professional licensing authority, in accordance with applicable NCIS regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where NCIS requires information and/or consultation assistance from the former employee

regarding a matter within that person's former area of responsibility.

(7) To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

(8) To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim.

(9) To commercial insurance companies in those instances in which they have a legitimate interest in the results of the investigation, but only to that extent and provided an unwarranted invasion of privacy is not involved.

(10) To the White House for the purpose of personnel actions requiring approval of the President of the United States as provided for in DoD Instruction 1320.4.

(11) To any person or entity if deemed by NCIS to be necessary in order to elicit information or cooperation from the recipient for use by NCIS in the performance of an authorized law enforcement activity.

(12) To any individual, organization, or governmental entity in order to notify them of a serious terrorist threat for the purpose of guarding against or responding to such a threat.

The DoD Blanket Routine Uses that appear at the beginning of the Navy's compilation of systems notices also apply to this system.''

* * * * *

RETRIEVABILITY:

Delete entry and replace with ''NCIS closed case paper files are filed by numeric sequential number, alphabetic by company and topical title, and geographic location; microfilm files are filed by dossier number and location; and electronic/optically imaged files by case or control number, name, and Social Security Number (SSN).

In order to locate the file it is necessary to query the Defense Clearance Index of Investigations. Open case files may also be retrieved from NCIS automated systems by a case number assigned at the time the investigation was initiated.

Copies of the files in the Naval Criminal Investigative Service Field Offices, Naval Criminal Investigative Service Resident Agencies, and Polygraph sites are retrieved by name. Polygraph sites can also retrieve copies of the file by polygraph approval number. Wire, Electronic, and Oral Intercept Index records are retrieved by a combination of name, address, Social Security Number, telephone number/radio call sign, or case designation.''

SAFEGUARDS:

Delete entry and replace with ''Buildings employ alarms, security guards, and or rooms with security controlled areas accessible only to authorized persons. Classified and highly sensitive paper records are maintained in General Service Administrative approved security containers. Paper and microform records in NCIS records office are stored on open shelves and in filing cabinets in security controlled areas accessible only to authorized persons. Electronically, digital, and optically stored records are maintained in 'fail-safe' system software with password protected access. Records are accessible only to authorized persons with a need-to-know who are properly screened, cleared and trained. Noncurrent hardcopy and master copy of microfilmed files are retired to the Washington National Records Center where retrieval is restricted to authorized NCIS personnel.

NCIS employees authorized to work offsite will safeguard government/agency records from unauthorized disclosure or damage by transporting only unclassified records in approved locked briefcases, satchels, or boxes. When not in use by the offsite employee, all records or case-related material is stored in a locked file cabinet or desk in the areas designated that is accessible only to authorized persons. Some documents will be prepared on government computers by NCIS employees at designated offsite locations. When offsite, computers may be connected securely to the Navy networks using approved virtual private network (VPN) software, and data and documents on government computers are protected using encryption. No data is authorized to be transferred to or stored on any employee's personal computer. Documents prepared at designated offsite locations and or temporarily held for the purposes of offsite work will not be printed at any unauthorized offsite location.''

RETENTION AND DISPOSAL:

Delete entry and replace with ''Counterintelligence (CI)/Counterterrorism (CT) Records: CI records are retained in the active file until the case is closed, then retired to the NCIS records office; then destroyed 25 years after the date of last action. Major CI/CT investigations are retired to the NCIS records office upon case closure; then transferred to the National Archives when 50 years old.

Copies may be retained at NCIS Field Offices for one year after case closure unless extended retention is authorized. Source records are retained in the active file until the operation is complete; then destroyed 75 years after the date of the last action.

Reciprocal CI/CT investigative files regarding individuals or organizations under investigative jurisdiction of the requesting agency are disposed of as prescribed above for CI/CT investigative records; except when the request is for CI/CT personnel security matters; then the file is destroyed after one year.

CI defensive briefings are retained until case closure, retired to the NCIS records office; then destroyed after 15 years. Foreign national marriage and visa applicant investigations are retired to the NCIS records office upon case closure; then destroyed after one year except when the investigation surfaces significant derogatory material. These files are destroyed after five years.

Records pertaining to CI polygraph examinations conducted in support of CI activities are filed with the case file and disposed of in accordance with the guidance for the associated file.

CI Security Polygraph Program (CSP) records are maintained in the active file until no longer needed; then disposed of after the final quality control review as follows: (1) CSP cases favorably resolved are destroyed after the final quality assurance review, except at NCIS Polygraph Units which retain the CSP investigative reports only; destroying it when no longer needed or after one year (2) CSP cases other than favorably resolved are destroyed 25 years after completion of the final quality assurance review, except when an existing criminal investigation exists.

In such cases the CSP Package is incorporated into the investigative file and disposed of in accordance with the disposition guidance for the dossier (3) audio tape recordings of routine CSP examinations with no significant responses are erased when no longer needed or after 90 days. Recordings referred for further investigation are incorporated into the investigative case file and disposed of in accordance with the disposition guidance for the dossier.

Personnel investigations: Completed NCIS investigative files on Personnel Security Investigations (PSI's) are destroyed after 15 years unless significant incidents or adverse information is developed, in which case they are destroyed after 25 years. PSI files on persons considered for affiliation with DoD will be destroyed within one year if the affiliation is not consummated. Special Agent applicant records are retained for one year if the

applicant declines offer of employment and five years if the applicant is rejected for employment. Non-DoD-affiliated applicant records are destroyed when no longer needed or after 90 days. Records for applicants who are accepted are retired to NCIS records office upon case closure; then destroyed 10 years after release, separation, transfer, retirement, or resignation. Internal personnel inquiries records are retired to NCIS records office after case closure; then destroyed 15 years after case closure.

Limited inquiries records are retired to NCIS records office at inquiry closure; then destroyed after 5 years.

Support applicant records are retired to NCIS records office at case closure; then destroyed after 15 years.

Law Enforcement Records: Criminal investigative files are destroyed after 25 years, except (1) controlled death and criminal sex investigations and investigations created on or after January 1, 1988 and where DoDI 5505.11 requires submission of offender criminal history data to the FBI are destroyed 50 years after date of case closure (2) files of cases determined to be of historical value are transferred to NARA 50 years after the date of the last action, except Grand Jury material which is destroyed at the time of transfer. Copies may be retained at NCIS Field Offices for one year after case closure unless extended retention is authorized.

Incident Reports (IR) received from Navy Law Enforcement and Marine Corps Military Police offices pertaining to categories of investigations/reports under the jurisdiction of NCIS and created prior to 1 January 1988 are destroyed when 25 years old. Cases created on or after 1 January 1988 are destroyed when 50 years old. Cases referred but determined not under NCIS jurisdiction are destroyed when no longer needed. Copies may be retained at the submitting office for two years after case closure unless extended retention is authorized.

Criminal Initiative Operations files are retired to NCIS records office upon closure; then destroyed 15 years after closure for Group 1 records and five years for Group 2.

Protective Operations files involving protective details of distinguished persons are destroyed when five years old, except records where a threat or attempted threat materialized are destroyed when 25 years old.

Law enforcement source records are retired to NCIS records office after case closure and destroyed 15 years after the date of last action.

Preliminary Investigation Reports (PIR) Records are used to document the receipt of information that at the initial stage indicated an incident occurred involving one or more criminal offenses, however, it was subsequently determined that no criminal offense occurred or that the incident and offenses did not fall within NCIS' jurisdiction and or responsibility to investigate. These records are destroyed/deleted 5 years after case closure.

Reciprocal investigative files regarding requests for investigative assistance from other Federal, state and local law enforcement agencies are disposed of as prescribed for the criminal investigative reports and IRs, as appropriate. Polygraph examinations conducted for criminal investigations are quality assured and filed in the associated criminal investigation. Disposition is in accordance with the guidance for the investigative case file.

Wire, Electronic, Oral Interception Index computer entries are deleted upon destruction or transfer to NARA of the case file containing intercept information. Disposition of the case files is governed by the NARA approved retention period applied to the case dossier.

Hardcopy records used to create the index are destroyed upon verification that the indexing information has been fully and accurately entered into the automated index.

National Crime Information Center (NCIC) records that support Department of the Navy entries into the FBI's National Crime Information Center are destroyed after the related entry is deleted from the National Crime Information Center computer.

Microfiche copies are destroyed when all cases on the fiche are cleared from the National Crime Information Center.

Fingerprint card files are disposed of as follows:

(1) digital capture of one fingerprint card set is forwarded to the Federal Bureau of Investigation; and the card is destroyed when it is verified that the digitally copy was accurately captured and transferred

(2) second fingerprint card, indices, and related correspondence are destroyed when 5 years old.

Counterintelligence records retained solely for the purpose of determining whether the information may be permanently retained on persons not affiliated with DoD must be destroyed within 90 days, unless retention is required by law or specifically approved by the Secretary of the Navy.

Counterintelligence Security Polygraph packages forwarded to Naval Criminal Investigative Service headquarters is destroyed when 35 years old. Files retained in the Naval Criminal Investigative Service Field Offices and Naval Criminal Investigative Service Resident Agencies and Polygraph sites are temporary and are destroyed after 90 days or earlier if no longer needed.

Destruction of records will be by shredding, burning, or pulping for paper records; burning for microform records; and magnetic erasing for computerized records. Optical digital data and CD ROM records are destroyed as specified by Department of the Navy, Information Assurance Remanence Publication 5239–26.''

* * * * *

N05520–4

SYSTEM NAME:

NCIS Investigative Files System.

SYSTEM LOCATION:

Primary System: Director, Naval Criminal Investigative Service, Washington Navy Yard, Building 111, 716 Sicard Street, SE., Washington, DC 20388–5380.

Decentralized Segments—Located at the Naval Criminal Investigative Service (NCIS) Field Offices (FO), Resident Agencies (RA), and Polygraph sites worldwide. Law Enforcement Information Exchange (LInX) secure remote computer server sites. Naval Criminal Investigative Service Regional Offices retain copies of certain portions of some investigative files and related documentation. The number and location of these Naval Criminal Investigative Service Field Offices, Naval Criminal Investigative Service Resident Agencies, and Polygraph sites are subject to change in order to meet the requirements of the Department of the Navy.

Consolidated Evidence Facilities maintain evidence inventory records.

Current locations of NCIS decentralized segments may be obtained from the Director, Naval Criminal Investigative Service, Washington Navy Yard, Building 111, 716 Sicard Street, SE., Washington, DC 20388–5380.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Persons in the following categories who require access to classified defense information and others who are of criminal, counterintelligence, security or general investigative interest to NCIS:

Active, reserve, and inactive members of the naval service; civilians, to include applicants for employment with NCIS; both citizen and alien employees located in both the U.S. and in overseas areas and including temporary, part-

time, and advisory personnel employed by the Department of the Navy; industrial and contractor personnel; civilian personnel being considered for sensitive positions, boards, conferences, etc. Civilian personnel who worked or resided overseas, e.g., Red Cross personnel. Civilian and military personnel accused, suspected, a witness to, or victims of felonious type offenses, or lesser offenses impacting on the good order, discipline, morale or security of the Department of the Navy; civilian personnel seeking access to or seeking to conduct or operate any business or other function aboard a Department of the Navy installation, facility or ship; civilians and civilian or military personnel who are subjects, co-subjects, witnesses, and victims in law enforcement and investigative cases in which law enforcement and investigative authorities (Federal, state, local, tribal, and foreign) have requested laboratory analysis of submitted evidence for law enforcement purposes; civilian or military personnel involved in the loss, compromise, or unauthorized disclosure of classified material/information; civilian and military personnel who were/are of counterintelligence interest to the Department of the Navy. Persons under investigation and parties to the communications whose communications have been intercepted during wire, electronic or oral surveillance operations conducted by or on behalf of NCIS.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

10 U.S.C. 5013, Secretary of the Navy; 18 U.S.C. 2510–2520 and 3504; 47 U.S.C. 605; DoD Directive 5210.48, Polygraph and Credibility Assessment Program; DoD Regulation 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons; DoD Directive 5505.9, Interception of Wire, Electronic, and Oral Communications for Law Enforcement; Secretary of the Navy Instruction 5430.107, Mission and Functions of the Naval Criminal Investigative Service; Secretary of the Navy M–5510.30, Department of the Navy Personnel Security Program; Secretary of the Navy M–5510.36, Department of the Navy Information Security Program; OPNAVINST 5530.14, Navy Physical Security and Law Enforcement; MCO 558.2, Law Enforcement Manual; E.O. 10450, Security Requirements for Government Employees, in particular sections 2, 3, 4, 5, 6, 7, 8, 9, and 14; E.O. 12333, United States Intelligence Activities and E.O. 9397 (SSN).

PURPOSE(S):

The information in this system is (was) collected to meet the investigative, counterintelligence, and security responsibilities of the Department of the Navy. This includes personal, personnel security, internal security, criminal, and other law enforcement matters all of which are essential to the effective operation of the Department of the Navy.

The records in this system are used for the following purposes: suitability for access or continued access to classified information; suitability for promotion, employment, or assignment; suitability for access to military installations or industrial firms engaged in government projects/contracts; suitability for awards or similar benefits; use in current law enforcement investigation or program of any type including applicants; use in judicial or adjudicative proceedings including litigation or in accordance with a court order; to assist Federal, state and local agencies that perform law enforcement or quasi-law enforcement functions; to assist Federal, state and local agencies that perform victim/witness assistance services, child protection services or family support or sailor services; insurance claims including workmen's compensation; provide protective operations under the DoD Distinguished Visitor Protection Program and to assist the U.S. Secret Service in meeting its responsibilities; assist local law enforcement agencies in meeting their responsibilities for complying with Congressionally mandated records checks such as Brady Handgun Violence Prevention Act checks; used for public affairs or publicity purposes such as wanted persons announcements, etc; referral of matters under their cognizance to Federal, state or local law enforcement authorities including criminal prosecution, civil court action or regulatory order; advising higher authorities and naval commands of the important developments impacting on security, good order or discipline; reporting of statistical data to naval commands and higher authority; input into the Defense Security Service managed Defense Clearance Index of Investigations (DCII) database under system notice V5–02. Wire, Electronic, and Oral Interceptions Index is maintained to enable NCIS to quickly locate records of intercept activities in response to motions for discovery and inquiries.

Users of the records in this system include NCIS employees who require access for operational, administrative, or supervisory purposes; DoD criminal investigative and intelligence units; DoD components making suitability determinations.

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 DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

(1) To any criminal, civil, or regulatory law enforcement authority (whether Federal, state, local, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.

(2) To a governmental entity lawfully engaged in collecting criminal law enforcement, criminal law enforcement intelligence, or national security intelligence information for law enforcement or intelligence purposes.

(3) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records.

(4) In an appropriate proceeding before a court, or administrative or adjudicative body, when NCIS determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

(5) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings.

(6) To a former employee of NCIS for purposes of: responding to an official inquiry by a Federal, state, or local government entity or professional licensing authority, in accordance with applicable NCIS regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where NCIS requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(7) To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

(8) To complainants and/or victims to the extent necessary to provide such persons with information and

explanations concerning the progress and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim.

(9) To commercial insurance companies in those instances in which they have a legitimate interest in the results of the investigation, but only to that extent and provided an unwarranted invasion of privacy is not involved.

(10) To the White House for the purpose of personnel actions requiring approval of the President of the United States as provided for in DoD Instruction 1320.4.

(11) To any person or entity if deemed by NCIS to be necessary in order to elicit information or cooperation from the recipient for use by NCIS in the performance of an authorized law enforcement activity.

(12) To any individual, organization, or governmental entity in order to notify them of a serious terrorist threat for the purpose of guarding against or responding to such a threat.

The DoD Blanket Routine Uses that appear at the beginning of the Navy's compilation of systems notices also apply to this system.

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

STORAGE:

Maintained on paper records in file folders, audio and audiovisual tapes, microimaging, electronic systems, magnetic tape, optical digital data disks, CD ROM, and computer output products. Some laboratory documents are stored in loose-leaf notebooks or bound record books.

RETRIEVABILITY:

NCIS closed case paper files are filed by numeric sequential number, alphabetic by company and topical title, and geographic location; microfilm files are filed by dossier number and location; and electronic/optically imaged files by case or control number, name, and Social Security Number (SSN).

In order to locate the file it is necessary to query the Defense Clearance Index of Investigations. Open case files may also be retrieved from NCIS automated systems by a case number assigned at the time the investigation was initiated.

Copies of the files in the Naval Criminal Investigative Service Field Offices, Naval Criminal Investigative Service Resident Agencies, and Polygraph sites are retrieved by name.

Polygraph sites can also retrieve copies of the file by polygraph approval number. Wire, Electronic, and Oral Intercept Index records are retrieved by a combination of name, address, Social Security Number, telephone number/radio call sign, or case designation.

SAFEGUARDS:

Buildings employ alarms, security guards, and or rooms with security controlled areas accessible only to authorized persons. Classified and highly sensitive paper records are maintained in General Service Administrative approved security containers. Paper and microform records in NCIS records office are stored on open shelves and in filing cabinets in security controlled areas accessible only to authorized persons. Electronically, digital, and optically stored records are maintained in 'fail-safe' system software with password protected access. Records are accessible only to authorized persons with a need-to-know who are properly screened, cleared and trained. Noncurrent hardcopy and master copy of microfilmed files are retired to the Washington National Records Center where retrieval is restricted to authorized NCIS personnel.

NCIS employees authorized to work offsite will safeguard government/agency records from unauthorized disclosure or damage by transporting only unclassified records in approved locked briefcases, satchels, or boxes. When not in use by the offsite employee, all records or case-related material is stored in a locked file cabinet or desk in the areas designated that is accessible only to authorized persons. Some documents will be prepared on government computers by NCIS employees at designated offsite locations. When offsite, computers may be connected securely to the Navy networks using approved virtual private network (VPN) software, and data and documents on government computers are protected using encryption. No data is authorized to be transferred to or stored on any employee's personal computer. Documents prepared at designated offsite locations and or temporarily held for the purposes of offsite work will not be printed at any unauthorized offsite location.

RETENTION AND DISPOSAL:

Counterintelligence (CI) Records:

CI records are retained in the active file until the case is closed; then destroyed 25 years after the date of last action. Major CI investigations are retired to the NCIS records office upon case closure; then transferred to the National Archives and Records Administration (NARA) when 25 years old.

Source records are retained in the active file until the operation is complete; then destroyed 75 years after the date of the last action.

Reciprocal CI investigative files regarding individuals or organizations under investigative jurisdiction of the requesting agency are disposed of as prescribed above for CI investigative records; except when the request is for CI personnel security matters; then the file is destroyed after one year. CI defensive briefings are retained until case closure, retired to the NCIS records office; then destroyed after 15 years. Foreign national marriage and visa applicant investigations are retired to the NCIS records office upon case closure; then destroyed after one year except when the investigation surfaces significant derogatory material. These files are destroyed after five years.

Records pertaining to CI polygraph examinations conducted in support of CI activities are filed with the case file and disposed of in accordance with the guidance for the associated file. CI Security Polygraph Program (CSP) records are maintained in the active file until no longer needed; then disposed of after the final quality control review as follows: (1) CSP cases favorably resolved are destroyed after the final quality assurance review, except at NCIS Polygraph Units which retain the CSP investigative reports only; destroying it when no longer needed or after one year (2) CSP cases other than favorably resolved are destroyed 25 years after completion of the final quality assurance review, except when an existing criminal investigation exists. In such cases the CSP Package is incorporated into the investigative file and disposed of in accordance with the disposition guidance for the dossier (3) audio tape recordings of routine CSP examinations with no significant responses are erased when no longer needed or after 90 days. Recordings referred for further investigation are incorporated into the investigative case file and disposed of in accordance with the disposition guidance for the dossier.

PERSONNEL INVESTIGATIONS:

Completed NCIS investigative files on Personnel Security Investigations (PSI's) are destroyed after 15 years unless significant incidents or adverse information is developed, in which case they are destroyed after 25 years. PSI files on persons considered for affiliation with DoD will be destroyed within one year if the affiliation is not consummated. Special Agent applicant records are retained for one year if the

applicant declines offer of employment and five years if the applicant is rejected for employment. Non-DoD-affiliated applicant records are destroyed when no longer needed or after 90 days. Records for applicants who are accepted are retired to NCIS records office upon case closure; then destroyed 10 years after release, separation, transfer, retirement, or resignation. Internal personnel inquiries records are retired to NCIS records office after case closure; then destroyed 25 years after the date of last action or 10 years after termination of employment, whichever is later.

Limited inquiries records are retired to NCIS records office at inquiry closure; then destroyed after 5 years. Support applicant records are retired to NCIS records office at case closure; then destroyed after 15 years.

Law Enforcement Records:

Criminal investigative files are destroyed after 25 years, except (1) controlled death investigations which are destroyed 75 years after date of case closure (2) files of cases determined to be of historical value are transferred to NARA 25 years after the date of the last action, except Grand Jury material which is destroyed at the time of transfer. Incident Complaint Reports (ICR) received from Navy Shore Patrol and Marine Corps military police offices pertaining to categories of investigations/reports under the jurisdiction of NCIS are destroyed when 25 years old. Cases referred but determined not under NCIS jurisdiction are destroyed when no longer needed.

Criminal intelligence operations files are retired to NCIS records office upon closure; then destroyed 15 years after closure for Group 1 records and five years for Group 2. Protective operations files involving protective details of distinguished persons are destroyed when five years old, except records where a threat or attempted threat materialized are destroyed when 25 years old.

Law enforcement source (also called 'cooperating witness') records are retired to NCIS records office after case closure and destroyed 15 years after the date of last action. Information reports consisting of incidental information impacting on the security or discipline of commands or of interest to other law enforcement elements are destroyed when 25 years old.

Reciprocal investigative files regarding requests for investigative assistance from other Federal, state and local law enforcement agencies are disposed of as prescribed for the criminal investigative reports and ICRs, as appropriate.

Polygraph examinations conducted for criminal investigations are quality assured and filed in the associated criminal investigation. Disposition is in accordance with the guidance for the investigative case file.

Wire, Electronic, Oral Interception Index computer entries are deleted upon destruction or transfer to NARA of the case file containing intercept information. Disposition of the case files is governed by the NARA approved retention period applied to the case dossier. Hardcopy records used to create the index are destroyed upon verification that the indexing information has been fully and accurately entered into the automated index. National Crime Information Center (NCIC) records that support Department of the Navy entries into the FBI's National Crime Information Center are destroyed after the related entry is deleted from the National Crime Information Center computer. Microfiche copies are destroyed when all cases on the fiche are cleared from the National Crime Information Center.

Laboratory fingerprint card files are disposed of as follows:

(1) One fingerprint card set is forwarded to the Federal Bureau of Investigation; the other set is destroyed when 75 years old.

(2) Fingerprint card indices and related correspondence are destroyed when all administrative needs have expired.

Counterintelligence records on persons not affiliated with DoD must be destroyed within 90 days or one year under criteria set forth in DoD Directive 5200.27, unless retention is required by law or specifically approved by the Secretary of the Navy. Files retained in the Naval Criminal Investigative Service Field Offices and Naval Criminal Investigative Service Resident Agencies and Polygraph sites are temporary and are destroyed after 90 days or one year, as appropriate.

Destruction of records will be by shredding, burning, or pulping for paper records; burning for microform records; and magnetic erasing for computerized records. Optical digital data and CD ROM records are destroyed as specified by NAVSO P–5239–26, 'Remanence Security Guidebook' of September 1993.

Counterintelligence (CI)/Counterterrorism (CT) Records: CI records are retained in the active file until the case is closed, then retired to the NCIS records office; then destroyed 25 years after the date of last action. Major CI/CT investigations are retired to the NCIS records office upon case closure; then transferred to the National Archives when 50 years old.

Copies may be retained at NCIS Field Offices for one year after case closure unless extended retention is authorized. Source records are retained in the active file until the operation is complete; then destroyed 75 years after the date of the last action.

Reciprocal CI/CT investigative files regarding individuals or organizations under investigative jurisdiction of the requesting agency are disposed of as prescribed above for CI/CT investigative records; except when the request is for CI/CT personnel security matters; then the file is destroyed after one year.

CI defensive briefings are retained until case closure, retired to the NCIS records office; then destroyed after 15 years. Foreign national marriage and visa applicant investigations are retired to the NCIS records office upon case closure; then destroyed after one year except when the investigation surfaces significant derogatory material. These files are destroyed after five years.

Records pertaining to CI polygraph examinations conducted in support of CI activities are filed with the case file and disposed of in accordance with the guidance for the associated file.

CI Security Polygraph Program (CSP) records are maintained in the active file until no longer needed; then disposed of after the final quality control review as follows: (1) CSP cases favorably resolved are destroyed after the final quality assurance review, except at NCIS Polygraph Units which retain the CSP investigative reports only; destroying it when no longer needed or after one year (2) CSP cases other than favorably resolved are destroyed 25 years after completion of the final quality assurance review, except when an existing criminal investigation exists.

In such cases the CSP Package is incorporated into the investigative file and disposed of in accordance with the disposition guidance for the dossier (3) audio tape recordings of routine CSP examinations with no significant responses are erased when no longer needed or after 90 days. Recordings referred for further investigation are incorporated into the investigative case file and disposed of in accordance with the disposition guidance for the dossier.

Personnel investigations: Completed NCIS investigative files on Personnel Security Investigations (PSI's) are destroyed after 15 years unless significant incidents or adverse information is developed, in which case they are destroyed after 25 years. PSI files on persons considered for affiliation with DoD will be destroyed within one year if the affiliation is not consummated. Special Agent applicant records are retained for one year if the

applicant declines offer of employment and five years if the applicant is rejected for employment. Non-DoD-affiliated applicant records are destroyed when no longer needed or after 90 days. Records for applicants who are accepted are retired to NCIS records office upon case closure; then destroyed 10 years after release, separation, transfer, retirement, or resignation. Internal personnel inquiries records are retired to NCIS records office after case closure; then destroyed 15 years after case closure.

Limited inquiries records are retired to NCIS records office at inquiry closure; then destroyed after 5 years.

Support applicant records are retired to NCIS records office at case closure; then destroyed after 15 years.

Law Enforcement Records: Criminal investigative files are destroyed after 25 years, except (1) controlled death and criminal sex investigations and investigations created on or after January 1, 1988 and where DoDI 5505.11 requires submission of offender criminal history data to the FBI are destroyed 50 years after date of case closure (2) files of cases determined to be of historical value are transferred to NARA 50 years after the date of the last action, except Grand Jury material which is destroyed at the time of transfer. Copies may be retained at NCIS Field Offices for one year after case closure unless extended retention is authorized.

Incident Reports (IR) received from Navy Law Enforcement and Marine Corps Military Police offices pertaining to categories of investigations/reports under the jurisdiction of NCIS and created prior to 1 January 1988 are destroyed when 25 years old. Cases created on or after 1 January 1988 are destroyed when 50 years old. Cases referred but determined not under NCIS jurisdiction are destroyed when no longer needed. Copies may be retained at the submitting office for two years after case closure unless extended retention is authorized.

Criminal Initiative Operations files are retired to NCIS records office upon closure; then destroyed 15 years after closure for Group 1 records and five years for Group 2.

Protective Operations files involving protective details of distinguished persons are destroyed when five years old, except records where a threat or attempted threat materialized are destroyed when 25 years old.

Law enforcement source records are retired to NCIS records office after case closure and destroyed 15 years after the date of last action.

Preliminary Investigation Reports (PIR) Records are used to document the receipt of information that at the initial stage indicated an incident occurred involving one or more criminal offenses, however, it was subsequently determined that no criminal offense occurred or that the incident and offenses did not fall within NCIS' jurisdiction and or responsibility to investigate. These records are destroyed/deleted 5 years after case closure.

Reciprocal investigative files regarding requests for investigative assistance from other Federal, state and local law enforcement agencies are disposed of as prescribed for the criminal investigative reports and IRs, as appropriate.

Polygraph examinations conducted for criminal investigations are quality assured and filed in the associated criminal investigation. Disposition is in accordance with the guidance for the investigative case file.

Wire, Electronic, Oral Interception Index computer entries are deleted upon destruction or transfer to NARA of the case file containing intercept information. Disposition of the case files is governed by the NARA approved retention period applied to the case dossier.

Hardcopy records used to create the index are destroyed upon verification that the indexing information has been fully and accurately entered into the automated index.

National Crime Information Center (NCIC) records that support Department of the Navy entries into the FBI's National Crime Information Center are destroyed after the related entry is deleted from the National Crime Information Center computer.

Microfiche copies are destroyed when all cases on the fiche are cleared from the National Crime Information Center.

Fingerprint card files are disposed of as follows:

(1) Digital capture of one fingerprint card set is forwarded to the Federal Bureau of Investigation; and the card is destroyed when it is verified that the digitally copy was accurately captured and transferred

(2) Second fingerprint card, indices, and related correspondence are destroyed when 5 years old.

Counterintelligence records retained solely for the purpose of determining whether the information may be permanently retained on persons not affiliated with DoD must be destroyed within 90 days, unless retention is required by law or specifically approved by the Secretary of the Navy.

Counterintelligence Security Polygraph packages forwarded to Naval Criminal Investigative Service headquarters is destroyed when 35 years old. Files retained in the Naval Criminal Investigative Service Field Offices and Naval Criminal Investigative Service Resident Agencies and Polygraph sites are temporary and are destroyed after 90 days or earlier if no longer needed.

Destruction of records will be by shredding, burning, or pulping for paper records; burning for microform records; and magnetic erasing for computerized records. Optical digital data and CD ROM records are destroyed as specified by Department of the Navy, Information Assurance Remanence Publication 5239–26.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Naval Criminal Investigative Service, Washington Navy Yard, Building 111, 716 Sicard Street, SE., Washington, DC 20388–5380.

NOTIFICATION PROCEDURE:

Individuals seeking to determine whether this system of records contains information about themselves should address written inquiries to the Director, Naval Criminal Investigative Service, Washington Navy Yard, Building 111, Code 00JF, 716 Sicard Street, SE., Washington, DC 20388–5380.

Requests must contain the full name of the individual and at least one additional personal identifier such as date and place of birth, or Social Security Number (SSN). Persons submitting written requests must properly establish their identity to the satisfaction of the Naval Criminal Investigative Service. 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 outside 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).

Attorneys or other persons acting on behalf of an individual must provide written authorization from that individual for their representative to act on their behalf.

RECORD ACCESS PROCEDURES:

Individuals seeking access to records about themselves contained in this

system of records should address written inquiries to the Director, Naval Criminal Investigative Service, Washington Navy Yard, Building 111, Code 00JF, 716 Sicard Street, SE., Washington, DC 20388–5380.

Requests must contain the full name of the individual and at least one additional personal identifier such as date and place of birth and Social Security Number (SSN). Persons submitting written requests must properly establish their identity to the satisfaction of the Naval Criminal Investigative Service. 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 outside 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).

Attorneys or other persons acting on behalf of an individual must provide written authorization from that individual for their representative to act on their behalf.

CONTESTING RECORD PROCEDURES:

The Navy's rules for accessing records, and for contesting contents and appealing initial agency determinations are published in Secretary of the Navy Instruction 5211.5; 32 CFR part 701; or may be obtained from the system manager.

RECORD SOURCE CATEGORIES:

From individual, DoD and Military Department records; Federal Agency records; foreign law enforcement agencies, security, intelligence, investigatory, or administrative authorities; state, county, and municipal records; employment records of public schools, colleges, universities, technical and trade schools; hospital records; real estate agencies; credit bureaus; financial institutions which maintain credit information on individuals such as loan and mortgage companies, credit unions, banks, etc.; transportation companies (airlines, railroad, etc.); other private records sources deemed necessary in order to complete an investigation; miscellaneous records such as: telephone directories, city directories; Who's Who in America; Who's Who in Commerce and Industry; Who Knows What, a listing of experts in various fields; American Medical Directory; Martindale-Hubbell Law Directory; U.S. Postal Guide; Insurance Directory; Dunn and Bradstreet; and the U.S. Navy BIDEX (Biographical Index); any other type of miscellaneous records deemed necessary to complete the investigation or inquiry; the interview of individuals who have knowledge of the subject's background and activities; the interview of witnesses, victims, confidential sources, and or other individuals deemed necessary to complete the investigation.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Parts of this system may be exempt pursuant to 5 U.S.C. 552a(j)(2), since the information is compiled and maintained by the Naval Criminal Investigative Command, which performs as its principle function the enforcement of criminal laws.

Information specifically authorized to be classified under E.O. 12958, as implemented by DoD 5200.1–R, may be exempt pursuant to 5 U.S.C. 552a(k)(1).

Records maintained in connection with providing protective services to the President and other individuals under 18 U.S.C. 3506, may be exempt pursuant to 5 U.S.C. 552a(k)(3).

Records maintained solely for statistical research or program evaluation purposes and which are not used to make decisions on the rights, benefits, or entitlement of an individual except for census records which may be disclosed under 13 U.S.C. 8, may be exempt pursuant to 5 U.S.C. 552a(k)(4).

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.

Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service may be exempt pursuant to 5 U.S.C. 552a(k)(6), if the disclosure would compromise the objectivity or fairness of the test or examination process.

An exemption rule for this system 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 701, subpart G. For additional information, contact the system manager.

[FR Doc. E8–7617 Filed 4–9–08; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF EDUCATION

Submission for OMB Review; Comment Request

AGENCY: Department of Education.

SUMMARY: The IC Clearance Official, Regulatory Information Management Services, Office of Management invites comments on the submission for OMB review as required by the Paperwork Reduction Act of 1995.

DATES: Interested persons are invited to submit comments on or before May 12, 2008.

ADDRESSES: Written comments should be addressed to the Office of Information and Regulatory Affairs, Attention: Education Desk Officer, Office of Management and Budget, 725 17th Street, NW., Room 10222, Washington, DC 20503. Commenters are encouraged to submit responses electronically by email to *oira_submission@omb.eop.gov* or via fax to (202) 395–6974. Commenters should include the following subject line in their response ''Comment: [insert OMB number], [insert abbreviated collection name, e.g., ''Upward Bound Evaluation'']. Persons submitting comments electronically should not submit paper copies.

SUPPLEMENTARY INFORMATION: Section 3506 of the Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35) requires that the Office of Management and Budget (OMB) provide interested Federal agencies and the public an early opportunity to comment on information collection requests. OMB may amend or waive the requirement for public consultation to the extent that public participation in the approval process would defeat the purpose of the information collection, violate State or Federal law, or substantially interfere with any agency's ability to perform its statutory obligations. The IC Clearance Official, Regulatory Information Management Services, Office of Management, publishes that notice containing proposed information collection requests prior to submission of these requests to OMB. Each proposed information collection, grouped by office, contains the following: (1) Type of review requested, e.g. new, revision, extension, existing or reinstatement; (2) Title; (3) Summary of the collection; (4) Description of the need for, and proposed use of, the information; (5) Respondents and frequency of collection; and (6) Reporting and/or Recordkeeping burden. OMB invites public comment.