DEPARTMENT OF DEFENSE

Department of the Navy

Notice of Availability of Record of Decision for the Final Environmental Impact Statement for the Keyport Range Complex Extension

AGENCY: Department of the Navy, DoD.

ACTION: Notice.

SUMMARY: The Department of the Navy (Navy), after carefully weighing the environmental consequences of the proposed action as presented in the Final Environmental Impact Statement (FEIS), announces its decision to extend the operational areas of the Naval Sea Systems Command Naval Undersea Warfare Center Keyport Range Complex and increase the number of days of activities and the number of activities per day, in furtherance of the Navy’s statutory obligations under Title 10 of the United States Code governing the roles and responsibilities of the Navy. In its decision, the Navy considered applicable laws and executive orders, including an analysis of the effects of its actions in compliance with the Endangered Species Act, the Coastal Zone Management Act, and the National Historic Preservation Act, and the requirements of Executive Order (EO) 12898, Federal Actions to Address Environmental Justice in Minority Populations and Low Income Populations and EO 13045, Protection of Children from Environmental Health Risks and Safety Risks.

Implementation of the proposed action could begin immediately.

SUPPLEMENTARY INFORMATION: The complete text of the Navy’s Record of Decision (ROD) is available for public viewing on the project Web site at: http://www.navsea.navy.mil/nwu委书记port/Environmental/EIS.aspx along with copies of the FEIS and supporting documents. Single copies of the ROD will be made available upon request by contacting the FEIS Project Manager, Ms. Kimberly Kler, 360–396–0927.

Dated: July 13, 2011.

L.M. Senay,

Lieutenant, Judge Advocate General’s Corps, U.S. Navy, Federal Register Liaison Officer.

[FR Doc. 2011–18232 Filed 7–19–11; 8:45 am]

BILLING CODE 3810–FF–P

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Privacy Act; System of Records

AGENCY: Defense Nuclear Facilities Safety Board.

ACTION: Notice of systems of records.

SUMMARY: Each Federal agency is required by the Privacy Act of 1974, 5 U.S.C. 552a, to publish a description of the systems of records containing personal information as defined by the Privacy Act. In this notice, the Defense Nuclear Facilities Safety Board (DNFSB) updates the descriptions of the eight systems it currently maintains, and announces the creation of a ninth system.


SUPPLEMENTARY INFORMATION: The Board has previously maintained eight systems of records under the Privacy Act. The Board has created a new system, DNFSB–9, Occupational Beryllium Exposure Records, but the creation of this new system does not involve the collection of additional information or changes in the use or storage of records. Instead, it is only a minor records management reorganization for streamlining purposes. The records now to be found in DNFSB–9 were originally maintained in DNFSB–5, which is now limited to Occupational Radiation Exposure Records.

DNFSB–1

SYSTEM NAME: Personnel Security Files.

SECURITY CLASSIFICATION: Unclassified.


CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: DNFSB employees, applicants for employment with DNFSB, DNFSB contractors and consultants, and other
individuals requiring access to classified materials and facilities.

CATEGORIES OF RECORDS IN THE SYSTEM:

Personnel security folders and requests for security clearances (Forms SF 86, 86A, 87, and 312) and Department of Energy (DOE) Forms 5631.18, 5631.20, 5631.21, and 5631.29. In addition, records including the following information:

1. Security clearance request information;
2. Security education and foreign travel lectures;
3. Security infractions;
4. Names of individuals visiting DNFSB offices; and
5. Personal identity verification documents (e.g., photographs, fingerprint cards, and proofs of identity) maintained for Federal identification badge and access purposes.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

42 U.S.C. 2286.

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

DNFSB—to determine which individuals should have access to classified material; to be able to transfer clearances to other facilities for visitor control purposes; and to verify the identity of its employees and contractors.

DOE—to determine eligibility for security clearances.

Other Federal and State agencies—to determine eligibility for security clearances.

DNFSB will disclose information to appropriate agencies, entities, and persons when DNFSB: (1) Suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) determines that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DNFSB or another agency or entity) that rely upon the compromised information; and (3) deems the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DNFSB’s efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

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

STORAGE:

Paper records and electronic files.

RETRIEVABILITY:

By name, social security number, and numeric code.

SAFEGUARDS:

Access is limited to authorized DNFSB employees only. Paper records are stored in locked offices and locked file cabinets, and electronic records are maintained on a password-protected desktop personal computer (PC). The Security Management Officer’s office remains locked when not in use.

RETENTION AND DISPOSAL:

Records retention and disposal requirements are contained in the “General Records Schedules” published by the National Archives and Records Administration, Washington, DC. Paper records are shredded before disposal and electronic files are destroyed by secure, permanent methods.

SYSTEM MANAGER AND ADDRESS:


NOTIFICATION PROCEDURE:

Requests made by individuals to determine if DNFSB–1 records include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2091. Required proof of identification: complete name, social security number, and date of birth.

RECORD ACCESS PROCEDURES:

Individuals requesting permission to access DNFSB–1 records that include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2091. Required proof of identification before viewing records: complete name, social security number, date of birth, and individual must show official photo identification (e.g., driver’s license, passport, or government identification).

CONTESTING RECORD PROCEDURES:

Individuals contesting any DNFSB–1 records that include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2091. Required proof of identification before viewing records: complete name, social security number, date of birth, and individual must show official photo identification (e.g., driver’s license, passport, or government identification).

RECORD SOURCE CATEGORIES:

Subject individuals, Questionnaire for Sensitive Positions (SF 86), agency files, official visitor logs, contractors, and DOE Personnel Security Branch.

SYSTEM EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

DNFSB–2

SYSTEM NAME:

Time and Attendance Records.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:


CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

DNFSB employees.

CATEGORIES OF RECORDS IN THE SYSTEM:

Time and attendance records to include names, addresses, social security numbers, service computation dates, leave usage data with corresponding balances, and authorizations for overtime and compensatory time.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

42 U.S.C. 2286.

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

DNFSB—to enter and maintain payroll, time, and attendance data for DNFSB employees.

Federal Deposit Insurance Corporation—to compute and maintain payroll, time, and attendance data for Federal employees.

Internal Revenue Service—to process state and local income taxes.

Savings Institutions—to credit accounts for savings made through payroll deductions.

State and Local Governments—to process state and local income taxes.

Health Insurance Carriers—to process insurance claims.

DNFSB will disclose information to appropriate agencies, entities, and persons when DNFSB: (1) Suspects or
has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) determines that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DNFSB or another agency or entity) that rely upon the compromised information; and (3) deems the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DNFSB’s efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

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

STORAGE:

Paper records and electronic files.

RETRIEVABILITY:

By name, social security number, and alphanumeric code.

SAFEGUARDS:

Access is limited to authorized DNFSB employees only. Paper records are stored in locked file cabinets and electronic records are maintained on a password-protected desktop PC.

RETENTION AND DISPOSAL:

Records retention and disposal requirements are contained in the “General Records Schedules” published by the National Archives and Records Administration, Washington, DC. Paper records are shredded before disposal and electronic files are destroyed by secure, permanent methods.

SYSTEM MANAGER AND ADDRESS:


NOTIFICATION PROCEDURE:

Requests made by individuals to determine if DNFSB–2 records include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification before viewing records: complete name, social security number, date of birth, and individual must show official photo identification (e.g., driver’s license, passport, or government identification).

CONTESTING RECORD PROCEDURES:

Individuals contesting any DNFSB–2 records that include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification before viewing records: complete name, social security number, date of birth, and individual must show official photo identification (e.g., driver’s license, passport, or government identification).

RECORD SOURCE CATEGORIES:

Subject individuals, timekeepers, supervisors, the Bureau of the Public Debt for payroll records, and the Internal Revenue Service and State officials for withholding and tax information.

SYSTEM EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

DNFSB–3

SYSTEM NAME:

Drug Testing Program Records.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Division of Human Resources, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Duplicate systems may exist, in whole or in part, at contractor testing laboratories and collection/evaluation facilities.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

DNFSB employees and applicants for employment with DNFSB.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records including the following information:

1. Pre-employment drug test requests or results, random tests, confirmatory tests, and follow-up tests;
2. Information supplied by employees or applicants contesting positive test results;
3. Information supplied by individuals concerning alleged drug abuse by DNFSB employees or applicants; and
4. Written statements or medical evaluations of attending physicians or information regarding prescription or nonprescription drugs.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:


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

Information in these records may be used by a Medical Review Officer (MRO) and DNFSB management:

1. To identify substance abusers within the agency;
2. To initiate counseling and rehabilitation programs;
3. To take personnel actions;
4. To take personnel security actions; and
5. For statistical purposes.

DNFSB will disclose information to appropriate agencies, entities, and persons when DNFSB: (1) Suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) determines that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DNFSB or another agency or entity) that rely upon the compromised information; and (3) deems the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DNFSB’s efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

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

STORAGE:

Test records are maintained on paper in file folders. Records used for initiating a random drug test are maintained on the Random Employee Selection Automation System. This is a password-protected, stand-alone system that resides on a desktop computer.

RETRIEVABILITY:

Records maintained in file folders are indexed and accessed by name and social security number. Random drug testing records are accessed via a computer database that includes
employees’ names, social security numbers, and job titles.

SAFEGUARDS:

Access usage rights are limited to authorized DNFSB employees only. The Division of Human Resources records are stored in a locked file cabinet. Records in laboratory collection and evaluation facilities are stored under appropriate security measures so that access is limited and controlled.

RECORD NOTIFICATION PROCEDURE:

Requests made by individuals to determine if DNFSB–3 records include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification: complete name, social security number, and date of birth.

RECORD ACCESS PROCEDURES:

Individuals requesting permission to access DNFSB–3 records that include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification before viewing records: complete name, social security number, date of birth, and individual must show official photo identification (e.g., driver’s license, passport, or government identification).

CONTESTING RECORD PROCEDURES:

Individuals contesting any DNFSB–3 records that include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification before viewing records: complete name, social security number, date of birth, and individual must show official photo identification (e.g., driver’s license, passport, or government identification).

RECORD SOURCE CATEGORIES:

DNFSB employees and applicants who have been identified for drug testing, who have been tested, or who have admitted abusing drugs prior to being tested; physicians’ statements regarding medical evaluations or authorized prescriptions for drugs; individuals providing information through a pre-employment drug use questionnaire; individuals providing information concerning alleged drug abuse by DNFSB employees or applicants, including but not limited to: specimen collection, laboratories for analysis, and medical evaluations; and DNFSB staff administering the drug testing program to ensure the achievement of a drug-free workplace.

RECORD NOTIFICATION PROCEDURE:

Requests made by individuals to determine if DNFSB–3 records include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification: complete name, social security number, and date of birth.

RECORD ACCESS PROCEDURES:

Individuals requesting permission to access DNFSB–3 records that include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification before viewing records: complete name, social security number, date of birth, and individual must show official photo identification (e.g., driver’s license, passport, or government identification).

CONTESTING RECORD PROCEDURES:

Individuals contesting any DNFSB–3 records that include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification before viewing records: complete name, social security number, date of birth, and individual must show official photo identification (e.g., driver’s license, passport, or government identification).

RECORD SOURCE CATEGORIES:

DNFSB employees and applicants who have been identified for drug testing, who have been tested, or who have admitted abusing drugs prior to being tested; physicians’ statements regarding medical evaluations or authorized prescriptions for drugs; individuals providing information through a pre-employment drug use questionnaire; individuals providing information concerning alleged drug abuse by DNFSB employees or applicants, including but not limited to: specimen collection, laboratories for analysis, and medical evaluations; and DNFSB staff administering the drug testing program to ensure the achievement of a drug-free workplace.

SYSTEM EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

Pursuant to 5 U.S.C. 552a(k)(5), DNFSB has exempted portions of this System of Records from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), (I), and (f). The exemption is invoked for the following reasons: 1. The information is neither public nor required to be maintained in a form which identifies any individual. 2. The information is not used for any purpose other than the proper performance of the protective functions of the system. 3. Records in the System of Records are not maintained for a period longer than is necessary to accomplish the purpose for which they are maintained. 4. The records are never disclosed to any except the gov...
DNFSB’s efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

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

**STORAGE:**
- Paper records and electronic files.

**RETRIEVABILITY:**
- By name and social security number.

**SAFEGUARDS:**
- Access is limited to authorized DNFSB employees only. Paper records are stored in locked file cabinets and electronic files are password-protected.

**RETENTION AND DISPOSAL:**
- Records retention and disposal requirements are contained in the “General Records Schedules” published by the National Archives and Records Administration, Washington, DC. Paper records within DNFSB are shredded before disposal and electronic files are destroyed by secure, permanent methods.

**SYSTEM MANAGER AND ADDRESS:**
- Director, Division of Human Resources, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901.

**NOTIFICATION PROCEDURE:**
- Requests made by individuals to determine if DNFSB–4 records include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification: complete name, social security number, and date of birth.

**RECORD ACCESS PROCEDURES:**
- Individuals requesting permission to access DNFSB–4 records that include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification before viewing records: complete name, social security number, date of birth, and individual must show official photo identification (e.g., driver’s license, passport, or government identification).

**RECORDS SOURCES CATEGORIES:**
- Individual employees, official personnel records, Office of Personnel Management, State employment agencies, educational institutions, and supervisors.

**SYSTEM EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:**
- None.

**DNFSB–5**

**SYSTEM NAME:**
- Occupational Radiation Exposure Records.

**SECURITY CLASSIFICATION:**
- Unclassified.

**SYSTEM LOCATION:**

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**
- DNFSB employees.

**CATEGORIES OF RECORDS IN THE SYSTEM:**
- Occupational radiation exposure information.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:**
- DNFSB—to monitor employees’ occupational radiation exposures during their employment with DNFSB.
- DOE—to monitor radiation exposure of visitors, including DNFSB employees, to the various DOE facilities in the United States.
- Other Federal and State Health Institutions—to monitor occupational radiation exposure of DNFSB personnel.
- DNFSB will disclose information to appropriate agencies, entities, and persons when DNFSB: (1) Suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) determines that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DNFSB or another agency or entity) that rely upon the compromised information; and (3) deems the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DNFSB’s efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

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

**STORAGE:**
- Paper records and electronic files.

**RETRIEVABILITY:**
- By name, social security number, and date of birth.

**SAFEGUARDS:**
- Access is limited to authorized DNFSB employees and contractors only. Paper records are stored in locked file cabinets with appropriate Privacy Act markings in a controlled-access area. Electronic files are password-protected or encrypted and stored on a dedicated computer.

**RETENTION AND DISPOSAL:**
- Records retention and disposal requirements are contained in the “General Records Schedules” published by the National Archives and Records Administration, Washington, DC. Paper records are shredded before disposal and electronic files are destroyed by secure, permanent methods.

**SYSTEM MANAGER AND ADDRESS:**
- Director, Division of Human Resources, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901.

**NOTIFICATION PROCEDURE:**
- Requests made by individuals to determine if DNFSB–5 include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification: complete name, social security number, and date of birth.

**RECORD ACCESS PROCEDURES:**
- Individuals requesting permission to access DNFSB–5 records that include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification before viewing records: complete name, social security number, date of birth, and individual...
must show official photo identification (e.g., driver’s license, passport, or government identification).

CONTESTING RECORD PROCEDURES:
Individuals contesting any DNFSB–5 records that include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification before viewing records: complete name, social security number, date of birth, and individual must show official photo identification (e.g., driver’s license, passport, or government identification).

RECORD SOURCE CATEGORIES:
Subject individuals, previous employee records, DOE occupational Radiation Exposure Monitoring System (REMS), whole body counts, bioassays, dosimeters, and film badges.

SYSTEM EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:
None.

DNFSB–6
SYSTEM NAME:
DNFSB Staff Resume Book.
SECURITY CLASSIFICATION:
Unclassified.
SYSTEM LOCATION:
CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:
DNFSB’s technical and legal employees.
CATEGORIES OF RECORDS IN THE SYSTEM:
A summary of each DNFSB technical and legal employee’s educational background and work experience with emphasis on areas relevant to the individual’s work at DNFSB.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
42 U.S.C. 2286.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:
DNFSB—to provide DNFSB Board Members and staff an understanding of the technical and legal qualifications of DNFSB’s employees to facilitate work assignments and for work planning purposes.
DNFSB will disclose information to appropriate agencies, entities, and persons when DNFSB: (1) Suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) determines that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DNFSB or another agency or entity) that rely upon the compromised information; and (3) deems the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DNFSB’s efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:
STORAGE:
Paper records and electronic files.
RETRIEVABILITY:
By name.

SAFEGUARDS:
The Resume Book is not accessible via the Internet or DNFSB’s Public Reading Room. Access to the Resume Book is limited to current DNFSB employees as determined by the Chairman. Paper records are stored in locked file cabinets or in locked desk drawers.

RETENTION AND DISPOSAL:
Records retention and disposal requirements are contained in the “General Records Schedules” published by the National Archives and Records Administration, Washington, DC. Out-of-date paper records are shredded before disposal and electronic files are destroyed by secure, permanent methods.

SYSTEM MANAGER AND ADDRESS:
Director, Division of Information Technology and Security, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901.

NOTIFICATION PROCEDURE:
Requests made by individuals to determine if DNFSB–6 records include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification: complete name, social security number, and date of birth.

RECORD ACCESS PROCEDURES:
Individuals requesting permission to access DNFSB–6 records that include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification before viewing records: complete name, social security number, date of birth, and individual must show official photo identification (e.g., driver’s license, passport, or government identification).

CONTESTING RECORD PROCEDURES:
Individuals contesting any DNFSB–6 records that include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification before viewing records: complete name, social security number, date of birth, and individual must show official photo identification (e.g., driver’s license, passport, or government identification).

RECORD SOURCE CATEGORIES:
Subject individuals.

SYSTEM EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:
None.

DNFSB–7
SYSTEM NAME:
Supervisor Files.
SECURITY CLASSIFICATION:
Unclassified.
SYSTEM LOCATION:
CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:
DNFSB’s technical, legal, and administrative employees.
CATEGORIES OF RECORDS IN THE SYSTEM:
Records including the following information:
1. Information used to write annual or mid-year performance appraisals, proposed awards, or proposed honors;
2. Documented written correspondence, employee’s work samples, hard-copy of electronic communications, confidential supervisor notations, and employee performance records; and
3. Information used to contact personnel during non-duty hours, such as personal cell phone numbers and home phone numbers.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
42 U.S.C. 2286.
ROUTINE USES OF RECORDS MAINTAINED IN THE
SYSTEM, INCLUDING CATEGORIES OF USERS AND
PURPOSES OF SUCH USES:

DNFSB—to be used by supervisors to write annual or mid-year performance appraisals for their employees or to propose awards or honors; to be used in connection with disciplinary or adverse actions.

DNFSB will disclose information to appropriate agencies, entities, and persons when DNFSB: (1) Suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) determines that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DNFSB or another agency or entity) that rely upon the compromised information; and (3) deems the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DNFSB’s efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

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

STORAGE:
Paper records and electronic files.

RETRIEVABILITY:
By name.

SAFEGUARDS:
Access is limited to the direct supervisor and administrative personnel who maintain the records. Paper records are stored in locked offices, locked file cabinets, or in locked desk drawers, and electronic files are password-protected.

RETENTION AND DISPOSAL:
Records retention and disposal requirements are contained in the “General Records Schedules” published by the National Archives and Records Administration, Washington, DC. Out-of-date paper records are shredded before disposal and electronic files are destroyed by secure, permanent methods.

SYSTEM MANAGER AND ADDRESS:
Director, Division of Information Technology and Security, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901.

NOTIFICATION PROCEDURE:
Requests made by individuals to determine if DNFSB–7 records include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification: complete name, social security number, and date of birth.

RECORD ACCESS PROCEDURES:
Individuals requesting permission to access DNFSB–7 records that include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification before viewing records: complete name, social security number, date of birth, and individual must show official photo identification (e.g., driver’s license, passport, or government identification).

CONTESTING RECORD PROCEDURES:
Individuals contesting any DNFSB–7 records that include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification before viewing records: complete name, social security number, date of birth, and individual must show official photo identification (e.g., driver’s license, passport, or government identification).

RECORD SOURCE CATEGORIES:
Subject individuals.

SYSTEM EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:
None.

DNFSB–8
SYSTEM NAME:
Travel, Procurement, and Administrative Files.

SECURITY CLASSIFICATION:
Unclassified.

SYSTEM LOCATION:

CATEGORIES OF INDIVIDUALS COVERED BY THE
SYSTEM: DNFSB EMPLOYEES, APPLICANTS FOR
EMPLOYMENT WITH DNFSB, AND DNFSB
CONTRACTORS AND CONSULTANTS.

CATEGORIES OF RECORDS IN THE SYSTEM:
1. Official travel documents including names, addresses, social security numbers, dates of birth, passport numbers, relocation records, and travel credit card numbers;
2. Purchase credit card numbers, invoices, and payment records;
3. Employee credit evaluations, credit check information, and travel/purchase card histories;
4. Parking permit records;
5. Public transit subsidy applications and issuance records;
6. Contracts/purchase orders; and
7. Miscellaneous reimbursements.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
42 U.S.C. 2286.

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

DNFSB—to process travel- and procurement-related documents.

General Services Administration—to reimburse DNFSB employees, applicants for employment, and consultants for travel-related expenses and miscellaneous reimbursements, and to reimburse contractors for services rendered.

General Accounting Office and Auditors—to verify accuracy and legality of disbursements.

Travel Agencies—to process travel itineraries.

DNFSB will disclose information to appropriate agencies, entities, and persons when DNFSB: (1) Suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) determines that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DNFSB or another agency or entity) that rely upon the compromised information; and (3) deems the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DNFSB’s efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

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

STORAGE:
Paper records and electronic files.

RETRIEVABILITY:
By name, social security number, travel dates, relocation dates, and alphanumeric code.

SAFEGUARDS:
Access is limited to authorized DNFSB employees only. Paper records are stored in locked file cabinets and electronic records are maintained on a password-protected desktop PC.
RETENTION AND DISPOSAL:
Records retention and disposal requirements are contained in the “General Records Schedules” published by the National Archives and Records Administration, Washington, DC. Paper records are shredded before disposal and electronic files are destroyed by secure, permanent methods.

SYSTEM MANAGER AND ADDRESS:
Director, Division of Administration for official accounting identification).

SYSTEM NAME:
Occupational Beryllium Exposure Records.

SECURITY CLASSIFICATION:
Unclassified.

SYSTEM LOCATION:

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:
DNFSB employees and contractors.

CATEGORIES OF RECORDS IN THE SYSTEM:
Occupational beryllium exposure information.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
42 U.S.C. 2286.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:
DNFSB—to assist DNFSB employees and contractors who may have been exposed to beryllium and wish to be informed of any applicable DOE beryllium disease screening and prevention programs.

DOE—to assist DOE in identifying DNFSB employees and contractors who may have been exposed to beryllium while working at various DOE defense nuclear facilities throughout the United States.

DNFSB will disclose information to appropriate agencies, entities, and persons when DNFSB: (1) Suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) determines that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DNFSB or another agency or entity) that rely upon the compromised information; and (3) deems the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DNFSB’s efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

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

STORAGE:
Paper records and electronic files.

RETRIEVABILITY:
By name.

SAFEGUARDS:
Access is limited to authorized DNFSB employees and contractors only. Paper records are stored in locked file cabinets with appropriate Privacy Act markings in a controlled-access area. Electronic files are password-protected or encrypted and are stored on a dedicated computer.

RETENTION AND DISPOSAL:
Records retention and disposal requirements are contained in the “General Records Schedules” published by the National Archives and Records Administration, Washington, DC. Paper records within DNFSB are shredded before disposal and electronic files are destroyed by secure, permanent methods.

SYSTEM MANAGER AND ADDRESS:
Director, Division of Human Resources, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901.

NOTIFICATION PROCEDURE:
Requests made by individuals to determine if DNFSB–9 records include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification: complete name, social security number, and date of birth.

RECORD ACCESS PROCEDURES:
Individuals requesting permission to access DNFSB–9 records that include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification before viewing records: complete name, social security number, date of birth, and individual must show official photo identification (e.g., driver’s license, passport, or government identification).

CONTESTING RECORD PROCEDURES:
Individuals contesting any DNFSB–9 records that include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification before viewing records: complete name, social security number, date of birth, and individual must show official photo identification (e.g., driver’s license, passport, or government identification).

CONTESTING RECORD PROCEDURES:
Individuals contesting any DNFSB–9 records that include their personal information should be directed to the Privacy Act Officer, Defense Nuclear Facilities Safety Board, 625 Indiana Avenue, NW., Suite 700, Washington, DC 20004–2901. Required proof of identification before viewing records: complete name, social security number, date of birth, and individual must show official photo identification (e.g., driver’s license, passport, or government identification).
DEPARTMENT OF EDUCATION

National Assessment Governing Board; Meeting


ACTION: Notice of open meeting and partially closed sessions.

SUMMARY: This notice sets forth the schedule and proposed agenda of a forthcoming meeting of the National Assessment Governing Board (Board) and also describes the functions of the Board. Notice of this meeting is required under Section 10(a)(2) of the Federal Advisory Committee Act. This notice is intended to notify members of the general public of their opportunity to attend. Individuals who will need special accommodations in order to attend the meeting (e.g., interpreting services, assistive listening devices, materials in alternative format) should notify Munira Mwalimu at 202–357–6938 or at Munira.Mwalimu@ed.gov no later than July 22, 2011. We will attempt to meet requests after this date, but cannot guarantee availability of the requested accommodation. The meeting site is accessible to individuals with disabilities.

Dates: August 4–6, 2011.

Times:
Ad Hoc Committee: Open Session: 9:30 a.m.–11:00 a.m.
Assessment Development Committee: Closed Session: 11:30 a.m.–4:15 p.m.
Executive Committee: Open Session: 4:30 p.m.–5:30 p.m.; Closed Session: 5:30 p.m.–6:00 p.m.

Closed Session: 12:00 p.m.–12:30 p.m.
Reporting and Dissemination Committee: Open Session: 10:15 a.m.–12:30 p.m.
August 6:
Nominations Committee: Closed Session: 7:30 a.m.–8:15 a.m.
Full Board: Open Session: 8:30 a.m.–10:30 a.m.
Location: The Ritz-Carlton Hotel, 1150 22nd Street, NW., Washington, DC.

FOR FURTHER INFORMATION CONTACT:

SUPPLEMENTARY INFORMATION: The National Assessment Governing Board (Board) is established under section 412 of the National Education Statistics Act of 1994, as amended. The Board is established to formulate policy guidelines for the National Assessment of Educational Progress (NAEP). The Board’s responsibilities include the following: selecting subject areas to be assessed, developing assessment frameworks and specifications, developing appropriate student achievement levels for each grade and subject tested, developing standards and procedures for interstate and national comparisons, developing guidelines for reporting and disseminating results, and releasing initial NAEP results to the public.

On August 4, from 9:30 a.m. to 11:00 a.m., the Ad Hoc Committee on Parent Engagement will meet in open session. From 11:30 a.m. to 4:15 p.m. the Assessment Development Committee will meet in closed session to review secure test items for the 2012 Economics assessment at grade 12 and the 2013 Pilot Writing computer-based assessment at grade 4. The Assessment Development Committee will also review secure task outlines for the 2013 Pilot of the Technology and Engineering Literacy assessment at grade 8. The Board will be provided with specific test materials/questions for review that cannot be discussed/disclosed in an open meeting. Premature disclosure of these secure test items and materials would significantly impede implementation of the NAEP assessments, and is therefore protected by exemption 9(B) of section 552b(c) of Title 5 of the United States Code.

On August 5, from 10:15 a.m. to 12:30 p.m. The Assessment Development Committee (ADC) will meet in closed session from 10:15 a.m. to 12:30 p.m. During the closed meeting the ADC will complete their review of secure NAEP test items for the 2012 Economics assessment at grade 12 and the 2013 Pilot Writing computer-based assessment at grade 4 which the Committee began to review on Thursday, August 4 in closed session. In addition, the ADC will receive a closed session briefing on embargoed data from cognitive lab studies of 4th grade students in preparation for the 2012 computer-based Writing assessment. Following that writing briefing, the ADC will receive an update.