Privacy Impact Assessment

Defense Nuclear Facilities Safety Board
GSS LAN

July 2015

Defense Nuclear Facilities Safety Board
625 Indiana Avenue NW, Suite 700, Washington, DC 20004

Executive Summary

The Defense Nuclear Facilities Safety Board (Board) uses the General Support System (GSS LAN) to provide IT services to its workforce. The Board conducted this privacy impact assessment (PIA) to demonstrate that an adequate level of protection has been afforded to privacy information collected, transmitted and stored by the applications and systems operating within the GSS LAN. Since the GSS LAN is used to support all Board business operations, certain authorized users have a legitimate need to access personally identifiable information (PII) during the conduct of official Board business.

Background

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed.

The PIA is an analysis of how information is handled to:

i. ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
ii. determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and
iii. examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the Board's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the Board's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

i. Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;
ii. Accountability for privacy issues;
iii. Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and
iv. Providing documentation on the flow of personal information and information requirements within the Board's systems.

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Board activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

[1] Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

Overview of the Board's General Support System

Congress created the Defense Nuclear Facilities Safety Board (Board) as an independent agency within the Executive Branch (42 U.S.C. § 2286, et seq.) to identify the nature and consequences of potential threats to public health and safety at the Department of Energy's (DOE's) defense nuclear facilities, to elevate such issues to the highest levels of authority, and to inform the public. Since DOE is a self-regulating entity, the Board constitutes the only independent technical oversight of operations at the Nation's defense nuclear facilities. Under its legislative mandate, the Board plays a key role in maintaining the future viability of the Nation's nuclear deterrent capability by:

i. Ensuring that the health and safety of the public and the workers at DOE's defense nuclear facilities located throughout the United States are adequately protected, as DOE maintains the readiness of the nuclear arsenal, dismantles surplus weapons, disposes of excess radioactive materials, cleans up surplus defense nuclear facilities, and constructs new defense nuclear facilities;

ii. Enhancing the safety and security at our Nation's most sensitive defense nuclear facilities when hazardous nuclear materials and components are placed in more secure and stable storage; and

iii. Providing for the early identification of health and safety vulnerabilities, allowing the Secretary of Energy to address issues before they become major problems.

The Congress established the Board in September 1988 in response to growing concerns about the level of health and safety protection that DOE was providing the public and workers at defense nuclear facilities. In so doing, Congress sought to provide the general public with added assurance that DOE's defense nuclear facilities are being safely designed, constructed, operated, and decommissioned.

Business operations are conducted using the Board's General Support System (GSS LAN) under the direct management of the Division of Information Technology and Security under the Office of the General Manager (OGM). The GSS LAN includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. All Board IT services are provided by the GSS LAN and no other security authorization boundaries exist within the Board network environment. The GSS LAN does interface with numerous external IT systems and services that process information on behalf of the Board but are not under the Board's direct management.

Information processed consists of all staff work products and administrative information that support the mission of the agency, which by its nature also includes the handling and transmission of PII. All of the Board's organizations (Office of the General Counsel (OGC), OGM, Office of the Technical Director (OTD), as well as the Board itself are users of the system. Users include both employees and contractors. The current number of GSS LAN users is approximately 150, though access to PII is limited to only those with a legitimate business need.

The majority of GSS LAN users reside at the main office location at 625 Indiana Avenue NW in Washington DC. Additional system users are located at the DOE Defense Nuclear facility site offices throughout the Continental United States including Hanford Site (Washington), Oak Ridge National Laboratory (Tennessee), Pantex Plant (Texas), Savannah River Site (Georgia), and Los Alamos National Laboratory (New Mexico). All site offices are considered part of the GSS LAN and are connected via dedicated IPsec VPN connections implemented by the HQ and site office firewalls.

What PII the GSS LAN Collects

The Board collects some PII from members of the public, such as resumes related to potential hiring actions and information in FOIA requests. The PII data contained in the Board's Privacy Act systems of records is limited to current and potential employees, former Board employees who left the agency, and independent contractors. The Board does not collect or retain personal information when visitors access the Board's official website. Personal information freely provided to the Board, as in an e-mail inquiry or by transmitting an electronic employment application, is used solely to respond to the information request or for employment consideration, and is protected accordingly. Personal information freely provided to the Board, as in an e-mail comment from the Board's "Contact Us" web page regarding a Board Recommendation or DOE's response to a Board Recommendation is included with the hardcopy file and posted on that Recommendation's web page. Since the Board is a small agency in terms of the total number of employees and contractors, PII data maintained by the Board for current/former employees and for independent contractors is minimal.

In light of the above, the PII that is collected is done so via certain GSS LAN applications. In most cases, the GSS LAN itself does not directly collect PII. However, since the GSS LAN houses all Board hardware (excluding hosted services) PII may occasionally be transmitted, processed and/or stored on GSS LAN devices (e.g., file servers, local work stations) or GSS LAN produced output (e.g., printed hardcopy materials).

The Board maintains nine confidential systems of records. The confidential systems are Privacy Act Systems of Records and are represented in the table below:

System of Record	Applications Used	Data Types Collected
DNFSB-1 Personnel Security Files	Board Workstation, File Server, and Printer General Services Administration (HSPD-12 MSO System) Office of Personnel Management (e-QIP)	Personnel security folders and requests for security clearances including: Security clearance request information; Security education and foreign travel lectures; Security infractions; Names of individuals visiting Board offices; and Personal identity verification documents (e.g., photographs, fingerprint cards, and proofs of identity) maintained for Federal identification badge and access purposes.
DNFSB-2 Time and Attendance Records	Department of Treasury's Bureau of Fiscal Services (Web TA)	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.
DNFSB-3 Drug Testing Program Records	Paper copies of testing results "Random Employee Selection Automation System" application installed locally	Pre-employment drug test requests or results, random tests, confirmatory tests, and follow-up tests; Information supplied by employees or applicants contesting positive test results; Information supplied by individuals concerning alleged drug abuse by Board employees or applicants; and Written statements or medical evaluations of attending physicians or information regarding prescription or nonprescription drugs.
DNFSB-4 Personnel	Bureau of Fiscal Services	Name, social security number, sex, date of birth, home address, grade level, family information, and occupational code; Federal

System of Record	Applications Used	Data Types Collected
Files	(Web TA) Office of Personnel Management (eOPF, EHRI) Board Workstation, File Server, and Printer	employment application materials; Assigned Position Description; Telework Agreement (if applicable); Records on suggestions, awards, and bonuses; Training requests, authorization data, and training course evaluations; Employee appraisals, appeals, grievances, and complaints; Employee disciplinary actions; Employee retirement records; Employment transfers; Promotions, payroll changes, and benefits elections; and Proof of identity documents.
DNFSB-5 Occupational Radiation Exposure Records	Board Workstation and Printer	Occupational radiation exposure information
DNFSB-6 Board Staff Resume Book	Board Workstation, File Server, and Printer	A summary of each Board technical and legal employee's educational background and work experience with emphasis on areas relevant to the individual's work at the Board.
DNFSB-7 Supervisory Files	Board Workstation, File Server, and Printer	Information used to write annual or mid-year performance appraisals, proposed awards, or proposed honors; Documented written correspondence, employee's work samples, hard-copy of electronic communications, confidential supervisor notations, and employee performance records; and Information used to contact personnel during non-duty hours, such as personal cell phone numbers and home phone numbers.
DNFSB-8 Travel, Procurement, and Administrative Files	Board Workstation, File Server, and Printer United States Department of Agriculture (USDA) (Concur Travel System)	Official travel documents including names, addresses, social security numbers, dates of birth, passport numbers, relocation records, and travel credit card numbers; Purchase credit card numbers, invoices, and payment records; Employee credit evaluations, credit check information, and travel/purchase card histories; Parking permit records; Public transit subsidy applications and issuance records; Contracts/purchase orders; and Miscellaneous reimbursements.
DNFSB-9 Occupational Beryllium Exposure Records	Board Workstation and Printer	Occupational beryllium exposure information

The information is collected by Board personnel directly from the subjects above using a variety of forms and other collection methods into the GSS LAN.

Why the GSS LAN Collects PII Information and How it is Used

The Board GSS LAN collects PII during the conduct of everyday business. Specific rationale for the collection of each system of record is noted in the table below.

System of Record	**Why Data is Collected and How it is Used**
DNFSB-1 Personnel Security Files	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.
DNFSB-2 Time and Attendance Records	To enter and maintain payroll, time, and attendance data for Board employees.
DNFSB-3 Drug Testing Program Records	Information in these records may be used by a Medical Review Officer (MRO) and Board 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-4 Personnel Files	To maintain personnel files on Board employees to facilitate processing of personnel actions.
DNFSB-5 Occupational Radiation Exposure Records	To monitor employees' occupational radiation exposures during their employment with the Board.
DNFSB-6 **Board** Staff Resume Book	To provide the Board Members and staff an understanding of the technical and legal qualifications of the Board's employees to facilitate work assignments and for work planning purposes.
DNFSB -7 Supervisory Files	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-8 Travel, Procurement, and Administrative Files	To process travel- and procurement-related documents.
DNFSB-9	To assist Board employees and contractors who may have been exposed to beryllium and

System of Record	Why Data is Collected and How it is Used
Occupational Beryllium Exposure Records	wish to be informed of any applicable DOE beryllium disease screening and prevention programs.

How the GSS LAN Shares Information

The majority of system users accessing PII reside with the majority of GSS LAN components at the main office location at 625 Indiana Avenue NW in Washington DC. Additional system users are located at the DOE Defense Nuclear facility site offices throughout the Continental United States including Hanford Site (Washington), Oak Ridge National Laboratory (Tennessee), Pantex Plant (Texas), Savannah River Site (Georgia), and Los Alamos National Laboratory (New Mexico). However, all site offices are considered part of the GSS LAN and are connected via dedicated IPsec VPN connections implemented by the HQ and site office firewalls.

All users of the GSS LAN are Board employees or their contractors and the system's program manager must approve access. Other than the use of PII information by Board employees and/contractors with a legitimate business need to support operations, and employees/contractors of the Nuclear Regulatory Commission (NRC) Office of the Inspector General (the NRC Inspector General (IG) is assigned to serve as the Board's IG),the following table lists external parties with whom the PII may be shared:

System of Record	Information is Shared with the Following External Parties
DNFSB -1 Personnel Security Files	DOE – to determine eligibility for security clearances. Other Federal and State agencies – to determine eligibility for security clearances.
DNFSB-2 Time and Attendance Records	Bureau of Fiscal Services – to process and maintain payroll, time, and attendance data for Board employees. Treasury Department – to collect withholding taxes and issue savings bonds. Internal Revenue Service – to process Federal income taxes. State and Local Governments – to process state and local income taxes. Savings Institutions – to credit accounts for savings made through payroll deductions. Health Insurance Carriers – to process insurance claims.
DNFSB-3 Drug Testing Program Records	None – see note below
DNFSB-4 Personnel Files	Bureau of of Fiscal Services – to maintain Official Personnel Folders for the Board. Office of Personnel Management – to maintain transfer and retirement records for the calculation of benefits and collection of anonymous statistical reports and to enter personnel

System of Record	Information is Shared with the Following External Parties
	record information into the eOPF system Federal Retirement Thrift Investment Board – to invest employee contributions in selected funds, track financial performance of employee investments, and provide performance reports. Social Security Administration – to maintain Social Security records for the calculation of benefits. Department of Labor – to process Workmen's Compensation claims. Department of Defense Military Retired Pay Offices – to adjust military retirement. Veterans Administration – to evaluate veteran's benefits to which the individual may be entitled. States' Departments of Employment Security – to determine entitlement to unemployment compensation or other state benefits. Federal, State, or Local government agencies – to investigate individuals in connection with security clearances, and administrative or judicial proceedings. Private Organizations – to verify employees' employment status with the Board.
DNFSB-5 Occupational Radiation Exposure Records	DOE – to monitor radiation exposure of visitors, including Board employees, to the various DOE facilities in the United States. Other Federal and State Health Institutions – to monitor occupational radiation exposure of Board personnel.
DNFSB-6 Board Staff Resume Book	None – see note below
DNFSB-7 Supervisory Files	None – see note below
DNFSB-8 Travel, Procurement, and Administrative Files	USDA – to reimburse Board employees, applicants for employment, and consultants for travel-related expenses and miscellaneous reimbursements, and to reimburse contractors for services rendered. Travel Agencies – to process travel itineraries.
DNFSB-9 Occupational Beryllium Exposure Records	DOE – to assist DOE in identifying Board employees and contractors who may have been exposed to beryllium while visiting or working at various DOE defense nuclear facilities throughout the United States.

Note: The Board will disclose information to appropriate agencies, entities, and persons when the Board:

i. suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

ii. 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 the Board or another agency or entity) that rely upon the compromised information; and

iii. deems the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Board's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

How the GSS LAN Ensures Data Accuracy

Information is collected via several forms and direct online user entry depending on the PII collected. The PII data is assumed to be accurate since the information is collected directly from the subject and the individual is given the opportunity at that time to verify the accuracy of their information. Within the GSS LAN system components, automated data checks are in place to ensure data entered conforms to the expected values and formats.

How Long the GSS LAN Retains PII

Records retention and disposal requirements are contained in the ``General Records Schedules'' published by the National Archives and Records Administration (NARA), Washington, DC.

The Board performs daily, weekly and monthly backups of all electronic records on the servers utilizing both full and differential backup techniques. Backup tapes are also kept and the current backup strategy is under review to ensure retention of electronic records are compliant with relevant retention schedules. Paper records are shredded before disposal and electronic files are destroyed by secure, permanent methods.

The table below specifies the retention schedule for each system of record:

System of Record	**How Long Information is Retained**
DNFSB-1 Personnel Security Files	General Records Schedule 18 Personnel Security Clearance Files • Investigative reports and related documents furnished to agencies by investigative organizations for use in making security/suitability determinations o Destroy in accordance with the investigating agency instructions. • Index to the Personnel Security Case Files o Destroy with related case file. Security Violations Files • Files relating to alleged violations of a sufficiently serious nature o Destroy 5 years after close of case. • All other files, exclusive of documents placed in official personnel folders o Destroy 2 years after completion of final action. Classified Information Nondisclosure Agreements • If maintained separately from the individual's official personnel folder o Destroy when 70 years old.

System of Record	How Long Information is Retained
	• If maintained in the individual's official personnel folder o Apply the disposition for the official personnel folder.
DNFSB-2 Time and Attendance Records	General Records Schedule 2 Leave Application Files • If employee initials time card or equivalent o Destroy at end of following pay period. • If employee has not initialed time card or equivalent o Destroy after GAO audit or when 3 years old, whichever is sooner. Time and Attendance Source Records and Input Records • Destroy after GAO audit or when 6 years old, whichever is sooner.
DNFSB-3 Drug Testing Program Records	General Records Schedule 1 Federal Workplace Drug Testing Program Files • Drug test plans and procedures o Destroy when 3 years old or when superseded or obsolete. • Employee acknowledgment of notice forms o Destroy when employee separates from testing-designated position. • Selection/scheduling records o Destroy when 3 years old. • Records relating to the collection and handling of specimens "Record Books" o Destroy 3 years after date of last entry. Chain of custody records o Destroy when 3 years old. • Test results Positive results for employees o Destroy when employee leaves the agency or when 3 years old, whichever is later. Positive results for applicants not accepted for employment o Destroy when 3 years old. Negative results o Destroy when 3 years old.
DNFSB-4 Personnel Files	General Records Schedule 1 Official Personnel Folders (OPFs) • Transferred employees. o See Chapter 7 of The Guide to Personnel Recordkeeping for instructions relating to folders of employees transferred to another agency. • Separated employees. o Transfer folder to National Personnel Records Center (NPRC), St. Louis, MO, 30 days after latest separation. Offers of Employment Files • Accepted offers.

System of Record	How Long Information is Retained
	o Destroy when appointment is effective. • Declined offers: (1) When name is received from certificate of eligible – return to OPM with reply and application. (2) Temporary or excepted appointment – file with application (3) All others – destroy immediately <u>Certificate of Eligibles Files</u> • Destroy when 2 years old. <u>Employee Record Cards</u> • Destroy on separation or transfer of employee. <u>Interview Records</u> • Destroy 6 months after transfer or separation of employee. <u>Notifications of Personnel Actions</u> • Chronological file copies, including fact sheets, maintained in personnel offices. o Destroy when 2 years old. • All other copies maintained in personnel offices. o Destroy when 1 year old. <u>Correspondence and Forms Files</u> • Correspondence and forms relating to pending personnel actions. o Destroy when action is completed. • Retention registers and related records. (1) Registers and related records used to effect reduction-in-force actions. o Destroy when 2 years old. (2) Registers from which no reduction-in-force actions have been taken and related records. o Destroy when superseded or obsolete. • All other correspondence and forms. o Destroy when 6 months old.
DNFSB-5 Occupational Radiation Exposure Records	Retention and Disposition Schedule currently in the Board's internal Draft/Approval process and will be submitted to the National Archives and Records Administration (NARA) for approval. • Proposed Disposition. o Transfer folder to Washington National Records Center (WNRC) when 2 years old. Destroy when 75 years old.
DNFSB-6 Board Staff Resume Book	The Resume Book will be periodically updated, and out-of-date copies will be destroyed when updated copies are printed.
DNFSB-7 Supervisory Files	<u>General Records Schedule 1</u> <u>Supervisors' Personnel Files and Duplicate OPF Documentation</u> • Supervisors' Personnel Files.

System of Record	How Long Information is Retained
	o Review annually and destroy superseded or obsolete documents, or destroy file relating to an employee within 1 year after separation or transfer. • Duplicate Documentation. o Destroy when 6 months old.
DNFSB-8 Travel, Procurement, and Administrative Files	General Records Schedule 3 Noncommercial, Reimbursable Travel Files • Travel administrative office files. o Destroy when 6 years old. • Obligation copies. o Destroy when funds are obligated. General Records Schedule 9 Federal Employee Transportation Subsidy Records • Destroy when 3 years old. General Records Schedule 11 Credentials Files. • Identification credentials and related papers. (1) Identification credentials including cards, badges, parking permits, photographs, agency permits to operate motor vehicles, and property, dining room and visitors passes, and other identification credentials. o Destroy credentials 3 months after return to issuing office. (2) Receipts, indexes, listings, and accountable records. o Destroy after all listed credentials are accounted for.
DNFSB-9 Occupational Beryllium Exposure Records	Retention and Disposition Schedule currently in the Board's internal Draft/Approval process and will be submitted to the National Archives and Records Administration (NARA) for approval. • Proposed Retention and Disposition. o Transfer folder to Washington National Records Center (WNRC) when 2 years old. Destroy when 75 years old.

How the GSS LAN Secures PII Information

The Board GSS LAN achieved a three-year Authority to Operate (ATO) on October 3, 2012, with an expiration date of October 3, 2015. The GSS LAN is categorized as a moderate-risk system in accordance with National Institutes of Science and Technology (NIST) Federal Information Processing Standards (FIPS) 199. This is appropriate to protect the PII stored electronically. Accordingly, access to the PII within the GSS LAN is only available to users on the internal network who have received authorization and granted access to specific GSS LAN applications, file shares and/or hard copy printed materials.

In addition, all board laptops include either self-encrypting drives or encryption software. The IT enterprise is independently audited annually as part of the annual financial statement and FISMA audits, and findings are included in the Board's FISMA report and Performance and Accountability Report. In addition, the Board's Senior Agency Official for Privacy conducts an annual privacy program assessment that is provided to the independent auditor. Any findings or negative remarks are fixed immediately.

The system of security controls employed by the Board to protect sensitive PII from inadvertent disclosure or compromise is based on a strict set of management, operational and technical controls to guard against the unauthorized access to the Board's Privacy Act systems of records and files containing PII, and to also minimize the potential harm that could result from the loss or compromise of PII data should a breach occur. Examples of the controls listed in the Board Privacy Act Operating Procedure (OP 231-2.1) include:

i. Strictly limiting the number of staff and contractors with access to PII to those with an authorized "need-to-know" in order to perform their official duties.
ii. Eliminating access to Privacy Act systems of records and PII data stored in electronic formats from outside the Board's protected network.
iii. Requiring the written approval of the Chairman or General Manager before encrypted or similarly protected PII in electronic formats or un-redacted PII in paper form can be removed from Board offices.
iv. Implementing NIST security technical controls to include enhanced password protection, access monitoring systems, encrypting password files, encrypting PII data, user warning messages, and notification of inclusion of PII data before allowing access.
v. Paper records are stored in locked offices and locked file cabinets. Offices containing locked file cabinets remain locked when not in use.

To minimize potential harm due to an inadvertent disclosure or breach, the Board has:

i. Reduced the amount of PII data under its control, such as eliminating the use of social security numbers whenever possible in systems of records for Federal employees and applicants for employment with the Board.
ii. Conducted initial and annual training programs for employees and contractors on the collection, maintenance, destruction, and protection of PII data.
iii. Developed procedures to quickly address any actual or potential breach of PII under the Board’s control.

Training is an essential feature of the Board's Privacy program. Each Board employee and on-site contractor receives initial and annual refresher training to familiarize them with the information privacy laws and regulations, as well as the Board policies, rules of conduct, and the consequences of inappropriate access and disclosure of Privacy Act data or PII. Annual training is included in the Information Systems Security Awareness Training. All information technology personnel and staff directly involved with administering or maintaining personal information receive additional annual training on maintaining and safeguarding Privacy Act data or PII.

For externally hosted systems that contain PII of Board employees and its contractors (e.g., Bureau of Fiscal Services, USDA’s ConcurTravel System), the Board relies on the servicing organizations to properly protect the records, but reviews the appropriate security authorizations, and privacy impact assessments to determine they are using proper controls.

How the GSS LAN Provides Notice and Consent[2]

Notice to individuals concerning the collection of their PII is provided at the time of collection by the Board personnel and is provided in the form of an appropriate statement in accordance with Section (e)(3) of the Privacy Act, 5 U.S.C. Section 552a(e)(3). Individuals provide consent for the collection by submitting the information to the Board during the course of normal business operations. Additional notice is provided through this PIA and the Systems of Records Notices DNFSB-1 – DNFSB-9 available in the Federal Register dated July 20, 2011 (Volume 76, Number 139).

How the GSS LAN Provides Redress

Under the provisions of the Privacy Act, individuals may request searches of Board systems to determine if any records have been added that may pertain to them. This is accomplished by the following:

Notification procedure: Individuals wishing to know if their records appear in this system may inquire in person or in writing to:

Defense Nuclear Facilities Safety Board
Privacy Officer
625 Indiana Avenue NW, Suite 700
Washington, DC 20004-2901

Included in the request must be the following proof of identification:

- Complete Name,
- Social Security Number,
- Date of Birth,
- An individual must show official photo identification (e.g., driver's license, passport, or government identification).

Contesting record procedures: Individuals wanting to contest information about themselves that is contained in this system should make their requests in writing, detailing the reasons for why the records should be corrected to the following address:

Defense Nuclear Facilities Safety Board
Privacy Officer
625 Indiana Avenue NW, Suite 700
Washington, DC 20004-2901

GSS LAN Legal Authority for PII Information Collection

The PII maintained in GSS LAN is authorized under 10 CFR 1705 – Privacy Act.

GSS LAN System of Records Notice (SORN)

Given that the GSS LAN supports multiple applications with different PII collection, processing and storage objectives, the Board has issued the following SORNs which collectively cover the SORN requirements for the system:

[2] According to the Privacy Act of 1974, 5 U.S.C. § 552a(b), “No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains [subject to 12 exceptions listed under subsection (b)(1–12)]."

- DNFSB-1 Personnel Security Files
- DNFSB-2 Time and Attendance Records
- DNFSB-3 Drug Testing Program Records
- DNFSB-4 Personnel Files
- DNFSB-5 Occupational Radiation Exposure Records
- DNFSB-6 Board Staff Resume Book
- DNFSB-7 Supervisory Files
- DNFSB-8 Travel, Procurement, and Administrative Files
- DNFSB-9 Occupational Beryllium Exposure Records

All Board Privacy Act SORNs can be found in the Federal Register/Vol.76, No. 139/Wednesday, July 20, 2011/Notices, pages 43278-43286.
(http://www.dnfsb.gov/sites/default/files/Pages/About%20DNFSB's%20Systems%20of%20Records/072011%20Federal%20Register%20Volume%2076%20Number%20139%20System%20of%20Records%20Notice%20SORN_1.pdf)

For further information contact:

Defense Nuclear Facilities Safety Board
General Counsel
625 Indiana Avenue, NW, Suite 700
Washington, DC 20004-2901,
Phone: (202) 694-7000

Responsible Official

Board Privacy Officer
Andrew Thibadeau
Director, Division of Information Technology and Security
Phone: 202 694-7088
Email: AndrewT@dnfsb.gov

8/25/2015

Andrew Thibadeau Date

Senior Agency Official for Privacy
Mark Welch
General Manager
Phone: 202 694-7043
Email: MarkW@dnfsb.gov

M. Welch 8/25/15

Mark Welch Date