

A.J. Eggenberger, Chairman
John E. Mansfield, Vice Chairman
Joseph F. Bader
Larry W. Brown
Peter S. Winokur

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

625 Indiana Avenue, NW, Suite 700 Washington, D.C. 20004-2901
(202) 694-7000



October 1, 2008

The Honorable Jim Nussle
Director
Office of Management and Budget
Washington, DC 20503

Dear Mr. Nussle:

The FY 2008 Federal Information Security Management Act (FISMA) Report for the Defense Nuclear Facilities Safety Board (Board) is enclosed. During FY 2008, the Board continued to improve the controls protecting the Board's information, and to make progress towards achieving a fully FISMA-compliant information security program. This work is being done deliberately and comprehensively, consistent with the Board's limited resources and mission needs.

The findings of the Board's Chief Information Officer (CIO) and the Board's Inspector General designate regarding the Board's information security posture and contents of the FISMA micro-agency template are in agreement.

The Board completed a significant milestone in FY 2008 and authorized its internal general support system (GSS) to operate. By accrediting this system, which contains the security controls for all of the Board's internal applications, the Board has significantly increased its confidence in the effectiveness of the security controls used to protect agency information stored within its GSS. The Board also continued to verify that external systems used to process Board information, such as those operated by other Federal agencies as service providers, were also authorized to operate and had their security controls tested. By ensuring that both internal and external systems used to process Board information have been accredited, management now has a much better understanding of the risks facing the Board.

The Board has also made significant improvements in protecting Board information and has taken the following actions:¹

- All new laptop computers deployed by the Board are equipped with full disk encryption software to protect sensitive data in case of loss or theft.

- Secure USB drives have been purchased and issued to Board staff, and Board policy requires their use for the transportation of all sensitive information outside of the Board's physical space.
- The Board has deployed handheld devices for remote access to e-mail that encrypt all e-mail communications to protect communications from being intercepted.
- The Board continues to use IPsec and SSL technologies to secure all remote access connections to Board information systems

The Board has taken other steps to continue to improve its overall security posture, including:

- The Board has replaced all of its desktop and laptop computers in FY 2008 and configured them to comply with the Federal Desktop Core Configuration (FDCC) settings as set forth in OMB Memorandum M-07-18.
- The Board continues to issue personal identity verification (PIV) credentials in compliance with HSPD-12. As of September 30, 2008, the Board has sponsored 107 out of 113 employees and on-site contractors for PIV credentials and 93 credentials have been activated and are in use.
- The Board installed a new physical access system, allowing the use of PIV credentials to control physical access to the Board's headquarters facility.

In conclusion, the Board continues to improve and update its information security program's policies, procedures, and practices to achieve a fully FISMA-compliant information security program. This is being done in a manner consistent with its limited resources to balance mission requirements and the need to adequately and effectively protect the confidentiality, integrity, and availability of the Board's information.

Sincerely,



A. J. Eggenberger
Chairman

Enclosure: As stated

¹ All of the items above utilize FIPS-140 validated cryptographic modules

Microagency Reporting Template for FY 2008 FISMA and Information Privacy Management

Agency Name: Defense Nuclear Facilities Safety Board

Agency Point of Contact: Jeremy N. Bingham

Microagencies are defined as agencies employing 100 or fewer Full Time Equivalent positions (FTEs). Microagencies must report to OMB annually on FISMA and Information Privacy Management. While quarterly reports/updates are not required, microagencies should be prepared to provide information or to begin submitting quarterly reports to OMB upon request.

1. Information Systems Security

a. Total Number of agency and contractor systems	5
b. Number of agency and contractor systems certified and accredited	5
c. Number of agency and contractor systems for which security controls have been tested and reviewed in the past year	5
d. Was an independent assessment conducted in the last year?	Yes
e. Number of employees	95
f. Number of contractors	18
g. Number of employees and contractors who received IT security awareness training in the last year	107

2. Information Privacy

Breach Notification

- a. Agencies are required by OMB memorandum (M-07-16) of May 22, 2007, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" to develop and implement a breach notification policy within 120 days.

Please certify whether your agency has completed the requirements of M-07-16 by answering "Yes" or "No" to questions (1) through (4) in the table below.

I certify the agency has completed:

1.	A breach notification policy (Attachment 3 of M-07-16)	Yes
2.	An implementation plan to eliminate unnecessary use of Social Security Numbers (SSN) (Attachment 1 of M-07-16)	Yes
3.	An implementation plan and progress update on review and reduction of holdings of personally identifiable information (PII) (Attachment 1 of M-07-16)	Yes
4.	Policy outlining rules of behavior and identifying consequences and corrective actions available for failure to follow these rules (Attachment 4 of M-07-16)	Yes

Note: Micro agencies must maintain all documentation supporting this certification, and make it available in a timely manner upon request by OMB or other oversight authorities. **Micro Agencies are not required to provide the actual documentation with the annual report.**

Microagency Reporting Template for FY 2008 FISMA and Information Privacy Management

Agency Name: Defense Nuclear Facilities Safety Board

Agency Point of Contact: Jeremy N. Bingham

Privacy Impact Assessments (PIAs) and Systems of Record Notices (SORNs)

- b.** Please provide the URL to a centrally located web page on the agency web site on which the agency lists working links to all of its PIAs and working links to all of its SORNs published in the Federal Register. Agencies must maintain all documentation supporting this certification and make it available in a timely manner upon request by OMB or other oversight authorities. By submitting the template the agency certifies that to the best of agency's knowledge the quarterly report accounts for all of the agency's systems to which the privacy requirements of the E-Government Act and Privacy Act are applicable. If the agency does not have any PIAs or SORNs, enter "NA."

- b.1.** Provide the URL of the centrally located page on the agency web site listing working links to agency PIAs:
(Hyperlink not required)

NA

- b.2.** Provide the URL of the centrally located page on the agency web site listing working links to the published SORNs:
(Hyperlink not required)

http://www.dnfsb.gov/pub_docs/dnfsb/fr_20050715.pdf

= Data Entry Cells

October 1, 2008

Mr. Mark Welch
Contracting Officer
Defense Nuclear Facilities Safety Board
625 Indiana Ave NW, Suite 700
Washington, DC 20004-2901

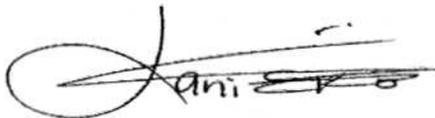
Dear Mr. Welch:

The Defense Nuclear Facilities Safety Board engaged Lani Eko & Company to perform an independent evaluation of its FY 2008 submission in compliance with the Federal Information Security Management Act (FISMA) and Agency Privacy Management, Title III of the E-Government Act of 2002. The Board is a small agency and, as such, does not have an Inspector General. At the request of the Board, we conducted an independent review of the FISMA compliance and reporting processes. Because the Board employs fewer than 100 full-time federal employees, we reviewed the Office of Management and Budget (OMB) 2008 reporting template for micro-agencies and resolved any discrepancies.

We completed this evaluation in accordance with Standards for Consulting Services established by the American Institute of Certified Public Accountants. Accordingly, we provide no opinion, attestation, or other form of assurance with respect to the work or the information upon which the work is based. The procedures we performed do not constitute an examination or a review in accordance with generally accepted auditing standards or attestation standards. The evaluation technique consisted mainly of interviews and documentation review. We evaluated the Board's information systems and security program against standards and requirements for federal agencies, such as those provided through FISMA, National Institute of Standards and Technology Special Publications, and OMB memorandums.

Please do not hesitate to contact us if you have any questions.

Very truly yours,

A handwritten signature in black ink, appearing to read "Lani Eko", with a large, stylized flourish on the left side.

Lani Eko, CPA,CGFM

Defense Nuclear Facilities Safety Board
FY 2008 Financial Statements Audit
09/30/08

DNFSB FISMA Microagency Template Reporting



DNFSB FY 2008
Annual FISMA Submis

1a. Total number of agency systems: 1

- DNFSB General Support System (GSS)

Total number of contractor systems: 4

- E2 (GSA travel system)
- Pegasys (GSA accounting system)
- USAccess (GSA HSPD-12 system)
- WebTA (BPD T&A system)

The DNFSB has defined all of its systems for Certification and Accreditation (C&A) purposes based on the Guide for the Security Certification and Accreditation of Federal Information Systems (NIST SP800-37).

1b: Number of agency and contractor systems certified and accredited: 5

The DNFSB has completed C&A for the GSS system managed by the Board's systems owners. For contractor systems, the certification and accreditation was completed by the agency service provider. DNFSB has confirmed the accreditation status by obtaining the accreditation letters for the service provider systems.

Due to the fact that the DNFSB C&A Security Test and Evaluation (ST&E) work by an independent contractor was ongoing through the month of September 2008, Lani Eko & Company did not have chance to review the controls testing performed on the GSS.

1c. Number of systems for which security controls have been tested and reviewed in the past year: 5

- GSS – in September 2008
- Pegasys (GSA service provider) – SAS 70 completed in 2008, but not assessed on NIST SP800-53 controls
- Web T&A (BPD service provider) – SAS 70 completed in 2008, but not assessed on NIST SP800-53 controls
- E2 (GSA service provider) – SAS 70 completed in 2008, but not assessed on NIST SP800-53 controls
- USAccess (GSA service provider) – SAS 70 completed in 2008, but not assessed on NIST SP800-53 controls

1d. Was an independent assessment conducted in the last year: Yes

Defense Nuclear Facilities Safety Board
FY 2008 Financial Statements Audit
09/30/08

The independent assessment was completed in September 2008.

1e. Number of employees and contractors: 113

- FTE: 95
- Contractors: 18

1f. Number of employees and contractors who received IT security awareness training in the last year: 107

Our audit testing confirms this number.

2a (1-4): Breach Notification Policy: Yes

DNFSB management has released the memorandum titled *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.

2b1. URL for PIAs: NA

Concur.

2b2. URL for SORNS: http://www.dnfsb.gov/pub_docs/dnfsb/fr_20050715.pdf

Concur.