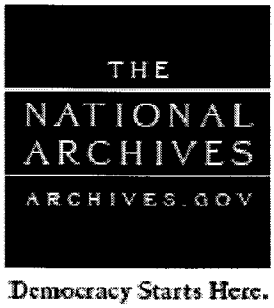
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA)



Report on the 2008 Review of NARA's Compliance with Section 522 of the Consolidated Appropriations Act, 2005.

(Policies, Procedures & Practices for Protection of Personally Identifiable Information)

Clifton Gunderson LLP

September 24, 2008

TABLE OF CONTENTS

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Paul Brachfeld
Inspector General
Office of the Inspector General
8601 Adelphi Road,
College Park, MD

Dear Mr. Brachfeld,

We are pleased to present our report on the National Archives and Records Administration's (NARA) compliance with protection of personal data in an identifiable form. This review included assessing compliance with applicable federal security and privacy laws and regulations as well as assessing the privacy and data protection procedures used by NARA as they relate to the guidelines set forth in Section 522-d of the *Omnibus Spending Bill for Transportation, Treasury, Independent Agencies, and General Government Appropriations Act of 2005.* The objective of our review was to determine whether: (1) the necessity of using personally identifiable information for processing was properly evaluated; (2) the Archives had established adequate procedures governing the collection, use and security of personally identifiable information; and (3) the Archives had properly complied with the prescribed procedures to prevent unauthorized access to and unintended use of personally identifiable information.

We interviewed key personnel involved in identifying and protecting personally identifiable information and reviewed documentation supporting NARA's efforts to comply with federal privacy and security laws and regulations.

This performance audit was conducted from July 2008 to August 2008 at the NARA Headquarters in College Park, Maryland and Archives I in Washington, District of Columbia and was conducted in accordance with *Generally Accepted Government Auditing Standards.*

We appreciate the opportunity to have served you once more and are grateful for the courtesy and hospitality extended to us by NARA personnel. Please do not hesitate to call me at (301) 931-2050 or email at george.fallon@cliftoncpa.com if you have questions.

We have incorporated NARA management's response to this report as an appendix.

Sincerely,

Clifton Gunderson LLP

CLIFTON GUNDERSON LLP
Calverton, Maryland
September 24, 2008

11710 Beltsville Drive
Suite 300
Calverton, MD 20705-3106
tel: 301-931-2050
fax: 301-931-1710

EXECUTIVE SUMMARY

The NARA Privacy Office or the Office of General Counsel has been proactive in carrying out its statutory responsibilities and its related role in ensuring compliance with Section 522 of the General Government Appropriations Act of 2005. Specifically, the Privacy Office has established a framework for identifying information systems containing or processing personally identifiable information (PII), securing data contained in these systems, conducting Privacy Impact Assessments (PIA) and reporting Systems of Records Notices (SORNs), all required by the Act.

Based on our review, NARA has (a) evaluated the necessity of using PII for data processing; and (b) established procedures for the collection and use of PII. However more work remains to be accomplished. Specifically, we noted the following:

The NARA Privacy Office (OGC) and the Office of Information Services (NH) has made significant effort in carrying out its statutory responsibilities and its related role in ensuring compliance with Section 522 of the General Government Appropriations Act. However, we noted policies and procedures as required by Office of Management and Budget (OMB) Memorandum 06-16 have not been developed.

- No formalized policies and procedures are in place for Personally Identifiable Information which: (1) explicitly identify the rules for determining whether physical removal is allowed; (2) require the information be encrypted and that appropriate procedures, training and accountability measures are in place to ensure that remote use of this encrypted information does not result in bypassing the protections provided by the encryption; (3) explicitly identify the rules for determining whether remote access is allowed for personally identifiable information that can be removed; (4) require that the remote access be accomplished via a virtual private network (VPN) connection established using agency issued authentication certificate (s) or hardware token, when remote access is allowed; (5) identify the rules for determining whether download or remote storage of the information is allowed, when remote access is allowed.

NARA technical controls related to the protection of personally identifiable information need to be strengthened.

- Encryption mechanisms are not in place on portable devices containing privacy data such as laptops, portable digital assistants (PDAs) or thumb drives leaving the NARA premises.
- Two factor authentication is not in place for remote access login.
- Risk assessments for Badging and Access System (B&A) and Automated Collection Management Database (IO/ACMD) is outdated and has not been updated at least every three years as required by federal mandates.

BACKGROUND

The Privacy Act of 1974 requires agencies to "establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom the information is maintained," 5 U.S.C. § 552a (e) (10). The Privacy Act limits agencies to "maintaining only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or Executive order of the President," 5 U.S.C. § 552a (e) (1).

The E-Government Act of 2002 strives to enhance protection of personal information in government information systems, by requiring the agencies to conduct PIAs. A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system.

Section 522 of the 2005 Consolidated Appropriations Act for Transportation and Treasury, Public Law 108-447, Division H, provides privacy requirements for NARA, including the implementation of privacy policies and procedures for public and employee data. OMB Memorandum-05-08 also requires each agency to designate a Senior Agency Official for Privacy. For NARA, the General Counsel also serves as the Senior Agency Official for Privacy.

NARA's use of personally identifiable information and related policies and procedures

NARA is an independent agency within the executive branch of the Federal Government responsible for preserving, protecting and providing access to the records of our Government. NARA also creates and receives a wide range of PII in the course of functioning as an executive branch with 3,229 employees. NARA also collects information on its contractors, volunteers and researchers who use the facilities and make requests for archival records as well as individuals who donate historical records or make financial contributions.

The NARA Privacy Program is housed within NARA's Office of General Counsel (OGC), located in Archives headquarters. The goal of the NARA Privacy Program is the protection of PII. The program provides leadership and assistance to NARA's divisions, nine regional archives and twelve Presidential libraries around the country on issues related to the Privacy Act of 1974, E-Government Act of 2002 and related OMB privacy guidance.

The NARA Privacy Program has an on-going initiative to grow the skills, knowledge and capabilities of the division heads and system owners.

In conformity with the 2005 Consolidated Appropriations Act, NARA's Senior Privacy Official published a Report of Senior Agency Official for Privacy on September 2006. This report was sent to the NARA OIG and to Congress. This report outlines the following areas:

- *Process of Conducting Privacy Review:* Includes an overview of NARA's privacy management program and determination of systems containing PII.
- *NARA Use of PII, Privacy and Data Protection Policies and Procedures:* Includes an overview of efforts used to track PII, NARA privacy officer's compliance efforts, NARA-wide policies and procedures developed or drafted to date in compliance with various privacy laws, regulations and OMB guidance, and other key privacy initiatives.

NARA's mission is to safeguard and preserve records of the US Government. In doing so, NARA is required to collect and use a significant amount of personal information from employees and the public for both administrative and operational initiatives. Also, presidential records and other archival records which are classified as PII are preserved within the Archives. To ensure information collected and maintained is secure, NARA has appointed an agency wide privacy officer located within the OGC. In addition to providing leadership on NARA-wide policies and procedures, the NARA Privacy Program works collaboratively with NH to guide and support their privacy awareness and compliance efforts. The methodology is based upon the following:

- Establish the priority, authority, and responsibility,
- Assess current privacy environment,
- Organize resources necessary for the project's goals,
- Develop policies, procedures and practices,
- Implement policies, practices and procedures,
- Maintain the policies, practices and procedures,
- Manage the exceptions and/or problems with the policies, practices and procedures.

In compliance with this requirement, NARA undertook a review of the use of PII and privacy policies and procedures at the agency wide level.

The NARA privacy officer in conjunction with the NH maintains an inventory of all information technology systems that collect, use, and share PII. As of the date of this report, there are 19 such systems.

Given the significant amount of sensitive PII data handled by the NARA, the NARA Privacy Officer continually works to track PII use and identify weaknesses that may require corrective action at the program or system level. A critical part of this process involves the review of PIAs and SORNs (if applicable) that are prepared by each PII system owner. In some cases, however, a PII system may be exempt from the requirement to perform a PIA if this system was created or implemented prior to the enactment of the E-Government Act of 2002. The NARA Privacy Office maintains a list of all PII systems that have completed a PIA or SORN and is responsible for posting all final PIAs and SORNs on the NARA Privacy Program web page.

SCOPE AND METHODOLOGY

NARA's OIG contracted with Clifton Gunderson LLP to conduct an audit of NARA's privacy and data protection policies and procedures in compliance with Section 522. The objective of this review was to assess the progress of NARA's Privacy Office in carrying out its responsibilities under federal law, more specifically, to determine whether: (1) the necessity of using personally identifiable information for processing was properly evaluated; (2) NARA had established adequate procedures governing the collection, use and security of personally identifiable information; and (3) NARA properly complied with the prescribed procedures to prevent unauthorized access to and unintended use of personally identifiable information.

To address this objective, we reviewed federal statutes including the Privacy Act of 1974 and Section 208 of the E-Government Act, to identify responsibilities of NARA's Privacy Office. We reviewed and analyzed privacy policies, guidance, and reports, and interviewed with officials from the Privacy Office. The personnel interviewed included the Senior Privacy Officer and the Privacy

Act Officer to identify privacy office's plans, priorities, and processes for implementing its responsibilities using available resources.

We further evaluated the Privacy Office policies, guidance, and processes for ensuring compliance with the Privacy Act, and the E-Government Act. We analyzed the SORNs and PIA development processes and assessed the progress of the office in implementing these processes. This analysis included analyzing the Privacy Office's overview of PIAs developed and assessing the overall quality of published PIAs.

Perform an assessment of NARA's privacy policies

We reviewed NARA information management practices for protection of PII, as they relate to the guidelines set forth in Section 522-d of the 2005 Government Appropriations Act. Public Law 107-347, the E-Government Act of 2002, defines "identifiable form" as *any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.* We performed procedures to assist the OIG in evaluating NARA's information management practices in order to:

A. Determine the accuracy of the descriptions of the use of information in identifiable form[1] while accounting for current technologies and processing methods;
B. Determine the effectiveness of privacy and data protection procedures by measuring actual practices against established procedural guidelines;
C. Determine compliance with the stated privacy and data protection policies of NARA and applicable laws and regulations;
D. Determine whether all technologies used to collect, use, store, and disclose information in identifiable form allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information in operation of the program, and
E. Provide NARA with recommendations, strategies, and specific steps, to improve privacy and data protection management.
F. Evaluate NARA's use of information in identifiable form.

We examined NARA's PII policies, practices and data protection procedures and mechanisms in operation. Specifically, the tasks focused on:

- a review of NARA's technology, practices and procedures with regard to the collection, use, sharing, disclosure, transfer and storage of information in identifiable form;
- a review of NARA's stated privacy and data protection procedures with regard to the collection, use, sharing, disclosure, transfer, and security of personal information in identifiable form relating to NARA's employees and the public;
- a detailed analysis of NARA's internet, network and Websites for privacy vulnerabilities, including 1)Non-compliance with stated practices, procedures and policies; and 2) Risks for inadvertent release of information in an identifiable form from NARA's website; and

[1] *information in identifiable form is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).*

- a review of NARA's compliance with section 522-d of the Omnibus Spending Bill for Transportation, Treasury, Independent Agencies, and General Government Appropriations Act of 2005;
- an analysis of the extent to which the Privacy Report filed with the OIG is accurate, account's for NARA's current technologies, information processing, and whether all areas are consistent with the Consolidated Appropriations Act, 2005, Division H, Title V, Section 522;
- an assessment of the reasonableness of NARA internal legal assessments of compliance requirements for privacy regulations, laws and other federal guidelines; and
- an assessment of whether Privacy Impact Assessments are completed and approved for a sample of required systems.

The E-Government Act of 2002 requires agencies to conduct a PIA either (1) before developing or procuring information technology systems or projects that collect, maintain or disseminate information in identifiable form or (2) when initiating a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government). In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks, for example, when converting paper-based records to electronic systems. On the other hand, no PIA is required where (1) information relates to internal government operations, (2) has been previously assessed under an evaluation similar to a PIA, or (3) where privacy issues are unchanged.

To accomplish the above-mentioned objectives, we:

- Reviewed NARA's report to the OIG dated September 27, 2006. This report was prepared in fulfillment of Section 522-c of the Appropriations Act. "*...Each agency shall prepare a written report of its use of information in an identifiable form, along with its privacy and data protection policies and procedures and record it with the Inspector General of the agency to serve as a benchmark for the agency. Each report shall be signed by the agency privacy officer to verify that the agency intends to comply with the procedures in the report. By signing the report, the privacy officer also verifies that the agency is only using information in identifiable form as detailed in the report.*"
- Verified that NARA had identified and maintained an inventory of information systems containing PII and systems requiring PIAs and had conducted PIAs for electronic information systems.
- Reviewed a sample of PIAs for the systems selected under review and noted the following:
  - What information was collected (e.g., nature and source).
  - Why the information was collected (e.g., to determine eligibility).
  - Intended use of the information (e.g., to verify existing data).
  - With whom the information was shared (e.g., another agency for a specified programmatic purpose).
  - What opportunities individuals had to decline to provide information or to consent to particular uses of the information (other than required or authorized uses), and how individuals communicated consent.
  - How the information was secured from abusive use (e.g., administrative and technological controls).
- Selected a representative sample of systems and tested technical controls to achieve the PII protection objectives.
- Reviewed the nature and use of PII, to determine whether a SORN was required and if required, whether one was published. We further reviewed NARA's publication of SORNs in the Federal Register and verified that they contained only information about individuals that was "*relevant and*

necessary" to accomplish NARA's purpose. We verified that this information was updated as necessary.

For the Fiscal Year 2008 Privacy Assessment, we were not engaged to and did not perform procedures to determine if the inventory of systems containing PII data was exhaustive and if NARA had performed procedures to ensure all NARA IT systems had been reviewed for existence of PII information. We reviewed the inventory of 19 PII systems received from the NARA Inspector General office. From this population, we selected a representative sample of 15 systems for testing, 13 PII systems and 2 non-PII systems. The results and exceptions noted in this report are based on this sample.

DETAILED RESULTS OF REVIEW

1. Although the NARA Privacy Office and Office of Information Services (NH) have established policies and procedures to protect NARA's PII systems and data, the Privacy Office does not properly monitor its privacy processes for quality compliance with the provisions of Section 522.

The NARA Privacy Office has made significant progress in addressing its statutory responsibilities under the General Government Act by developing processes to ensure implementation of privacy protections in agency wide programs. For example, the Privacy Office has established processes for ensuring agency wide compliance with the PIA requirement in the E-Government Act of 2002. Instituting this framework has led to increased attention to privacy requirements on the part of agency wide components, contributing to an increase in the number of PIAs issued.

While substantial progress has been made in these areas, more work needs to be done in other important aspects of NARA's privacy protection processes. The details of the matter are as follows:

General conditions found during the audit

- No formalized policies and procedures are in place for Personally Identifiable Information which:
  - explicitly identify the rules for determining whether physical removal is allowed
  - require the information be encrypted and that appropriate procedures, training, and accountability measures are in place to ensure that remote use of this encrypted information does not result in bypassing the protections provided by the encryption.
  - explicitly identify the rules for determining whether remote access is allowed for personally identifiable information that can be removed,
  - require that this access be accomplished via a virtual private network (VPN) connection established using agency-issued authentication certificate(s) or hardware token, when remote access is allowed,
  - identify the rules for determining whether download and remote storage of the information is allowed (For example, the policy could permit remote access to a database, but prohibit downloading and local storage of that database.), when remote access is allowed.

M 06-15, Memorandum for Heads of Departments and Agencies for Safeguarding Personally Identifiable Information states: "This memorandum reemphasizes your many responsibilities under law and policy to appropriately safeguard sensitive personally identifiable information and train your employees on their responsibilities on these areas. In particular, the Privacy Act requires each agency to establish 'appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained."

M 06-16, Memorandum for the Heads of Departments and Agencies for Protection of Sensitive Agency Information states: "(1) Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing. (2) Allow remote access only with two factor authentication where one of the factors is provided by a device separate from the computer gaining access (3) Use a time out function for remote access and mobile devices requiring user re-authentication after 30 minutes of inactivity (4) Log all computer readable extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required.

Recommendations:

We recommend that NARA management:

- Develop and formalize NARA policies which explain the rules for determining whether physical removal/remotely accessing PII is allowed and the appropriate procedures involved.

2. NARA Technical Controls related to the protection of personally identifiable information need to be strengthened.

The NARA Privacy Office has made significant effort in carrying out its statutory responsibilities and its related role in ensuring compliance with Section 522 of the General Government Appropriations Act, notably by establishing a framework for securing data contained in privacy systems. However, our review of a sample of 20 privacy systems highlighted that technical control over access to these systems needed to be strengthened. The details are as follows:

- Encryption mechanisms are not in place on portable devices containing privacy data such as laptops, portable digital assistants (PDAs) or thumb drives leaving the NARA premises.
- Two factor authentication mechanisms are not in place for remote access login.
- Risk assessments for Badging and Access System (B&A) and Automated Collection Management Database (IO/ACMD) is outdated and has not been updated at least every three years as required by federal mandates.

M 06-16, Memorandum for the Heads of Departments and Agencies for Protection of Sensitive Agency Information states: "(1) Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing. (2) Allow remote access only with two factor authentication where one of the factors is provided by a device separate from the computer gaining access (3) Use a time out function for remote access and mobile devices requiring user re-authentication after 30 minutes of inactivity (4) Log all computer readable extracts from databases

holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required.

OMB Circular A-130, Appendix III, Management of Federal Information Resources states: "Management authorization should be based on an assessment of management, operational, and technical controls. Re-authorization should occur prior to a significant change in processing, but at least every three years. It should be done more often where there is a high risk and potential magnitude of harm."

NIST 800-53: Recommended Security Controls for Federal Information Systems states: "Based on the results of the updated risk assessment, the organization should determine what additional security controls and/or control enhancements may be necessary to address the vulnerability (or vulnerabilities) related to the event or what corrective actions may be needed to fix currently implemented controls deemed to be less than effective. The security plan for the information system should then be updated to reflect these corrective actions."

NIST 800-37: Guide for the Security Certification and Accreditation of Federal Information Systems states: "The FIPS 199 security category should be considered during the risk assessment to help guide the information system owner's selection of security controls for the information system. Security categorization information is typically documented in the system identification section of the system security plan or included as an attachment to the plan."

M 07-16 Memorandum for the Heads of Executive Departments and Agencies for Safeguarding Against and Responding to the Breach of Personally Identifiable Information states: "Assign an impact level to all information and information systems: Agencies must follow the process outlined in FIPS 199 to categorize all information and information systems according to the standard's three levels of impact. Agencies should consider categorizing sensitive personally identifiable information as moderate or high impact."

Recommendations:

We recommend that NARA management:

- Ensure encryption mechanisms are in place for on all portable devices containing privacy data such as laptops, thumb drives and PDAs.
- Implement two factor authentications for remote access logins.
- Ensure risk assessments for the Badging and Access System (B&A) and Automated Collection Management Database (IO/ACMD) and all major applications and general support systems are conducted at least every three years or upon significant changes in its operating environment, prior to its expiration.

National Archives and Records Administration

700 Pennsylvania Avenue, NW
Washington, DC 20408-0001

Date: September 17, 2008

To: Paul Brachfeld, NARA Inspector General

From: Allen Weinstein, Archivist of the United States

Subject: Response to Draft Audit Report 08-15, Clifton Gunderson LLP (CG) 2008 Review of NARA's Compliance with Section 522 of the Consolidated Appropriations Act of 2005 (Policies, Procedures, and Practices for Protection of Personally Identifiable Information

Thank you for the opportunity to review and comment on the draft audit report 08-15 on NARA's compliance with Personally Identifiable Information (PII) requirements. We appreciate the efforts of your staff and all parties associated with this audit process.

We are pleased that CG notes the proactive and significant progress that the NARA Privacy Office has made in addressing our statutory responsibilities by developing processes to ensure implementation of privacy protections in agency wide programs. We concur with the need to develop and formalize NARA policies regarding physical removal and remote access of PII with corresponding procedures. Efforts to update our privacy related policies are already underway.

We are also pleased that CG comments on the framework we have established for securing data in privacy systems. We concur with the need for more technical control. Risk assessments are part of our Certification and Accreditation process. We are near the end of a business impact analysis on our systems that will help us ensure that risk assessments are completed as appropriate for each system. Efforts related to encryption and two factor authentication are already underway.

As new requirements for personally identifiable information are implemented by OMB, we will make every effort to comply in the prescribed timeframes. Again, we would like to thank the Office of Inspector General and Clifton Gunderson LLP for working in a professional and dedicated manner with NARA staff.

Allen Weinstein

ALLEN WEINSTEIN
Archivist of the United States

National Archives and Records Administration

Office of the Inspector General

8601 Adelphi Road, Suite 1300
College Park, Maryland 20740

Date : September 30, 2008

To : Allen Weinstein, Archivist of the United States

From : Paul Brachfeld, Inspector General

Subject : Management Letter 08-016: Security Response at A-1

This memorandum is intended to ensure effective, tested security measures are in place to protect the safety and integrity of the National Archives building (A-1), staff and visitors in the heart of our nation's capital. These concerns are neither theoretical nor abstract, but grounded in direct observation of events that unfolded the morning of September 23, 2008 when security vulnerabilities were exploited allowing protesters to gain access to and remain in control of the southwest corner of the Archives building on Constitution Avenue. NARA's response to this illegal trespass and occupation (DC Code Section 22-302) demonstrated a lack of planning, preparation, coordination and training on the part of security personnel entrusted with the paramount duty of protecting NARA structures, persons and holdings. Based upon the defined "success" of the demonstrators, the potential for copy-cat actions exists with absolutely no assurance they will be as docile as this event. Therefore, it is essential security defects be addressed expeditiously.

In an article published in the Baltimore Chronicle and Sentinel, one of the "Veterans for Peace" demonstrators (identified as Ellen Barfield) who participated in the self-described "Ledge-In" defines the mode of their ruse that allowed them unchallenged access to the building perimeter. Garbed as construction workers they circumvented the moat surrounding the building. Once secure, Ms. Barfield states "it was interesting that the Archives seemed to have no contact with any of the ...law enforcement entities in DC even though it is a Federal Building." Per Ms. Barfield they were even able to reinforce their sundries by having a supporter surreptitiously smuggle water to them when their supplies ran low, despite the fact security had allegedly quarantined the area.

[redacted]
Redacted pursuant to FOIA Exemptions b(2) and b(5)
[redacted]

Additionally, the protesters were allowed to set their protest time schedule of twenty-four hours and then were permitted to leave without arrest or consequence. This type of capitulation will only encourage further trespassing. As one of the protestors, Elliott Adams, has been quoted as saying "We considered staying longer this time but we are not prepared for longer than this...although we may be back again, soon."

All NARA staff, visitors and stakeholders should be concerned as to the events of September 23rd, and their future implications at A-1 and other NARA facilities including A-2 in College Park, Md. It is imperative that responsible NARA officials take immediate steps to develop, implement and test security measures addressing the vulnerabilities so clearly exposed and exploited by a handful of protesters at A-1.

Paul Brachfeld
Inspector General

National Archives and Records Administration

700 Pennsylvania Avenue, NW
Washington, DC 20408-0001

Date: September 17, 2008

To: Paul Brachfeld, NARA Inspector General

From: Allen Weinstein, Archivist of the United States

Subject: Response to Draft Audit Report 08-15, Clifton Gunderson LLP (CG) 2008 Review of NARA's Compliance with Section 522 of the Consolidated Appropriations Act of 2005 (Policies, Procedures, and Practices for Protection of Personally Identifiable Information

Thank you for the opportunity to review and comment on the draft audit report 08-15 on NARA's compliance with Personally Identifiable Information (PII) requirements. We appreciate the efforts of your staff and all parties associated with this audit process.

We are pleased that CG notes the proactive and significant progress that the NARA Privacy Office has made in addressing our statutory responsibilities by developing processes to ensure implementation of privacy protections in agency wide programs. We concur with the need to develop and formalize NARA policies regarding physical removal and remote access of PII with corresponding procedures. Efforts to update our privacy related policies are already underway.

We are also pleased that CG comments on the framework we have established for securing data in privacy systems. We concur with the need for more technical control. Risk assessments are part of our Certification and Accreditation process. We are near the end of a business impact analysis on our systems that will help us ensure that risk assessments are completed as appropriate for each system. Efforts related to encryption and two factor authentication are already underway.

As new requirements for personally identifiable information are implemented by OMB, we will make every effort to comply in the prescribed timeframes. Again, we would like to thank the Office of Inspector General and Clifton Gunderson LLP for working in a professional and dedicated manner with NARA staff.

Allen Weinstein

ALLEN WEINSTEIN
Archivist of the United States