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."

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