



The Library of Congress
Office of the Inspector General



Library-Wide

*Library Policies and Procedures
Protecting Personally Identifiable
Information Require Overhauling
to Assure Adequate Security*

Audit Report No. 2008-PA-104
September 2009



UNITED STATES GOVERNMENT

LIBRARY OF CONGRESS

Memorandum

Office of the Inspector General

TO: James H. Billington
Librarian of Congress

September 23, 2009

FROM: Karl W. Schornagel
Inspector General

A handwritten signature in black ink, appearing to read "Karl W. Schornagel".

SUBJECT: Audit Report No. 2008-PA-104: *Library Policies and Procedures Protecting Personally Identifiable Information Require Overhauling to Assure Adequate Security*

This transmits our final report on the audit of Personally Identifiable Information. The Executive Summary begins on page *i*, and complete findings and recommendations appear on pages 11 to 18. Responses from the Chief Operating Officer are briefly summarized in the Executive Summary and in more detail after individual recommendations. Her complete responses are included as an appendix to the report.

Based on the written comments to the draft report, we consider all of the recommendations resolved. Please provide, within 30 calendar days, an action plan addressing implementation of the recommendations, including implementation dates, in accordance with LCR 211-6, Section 11.A.

We appreciate the cooperation and courtesies extended by the Chief Operating Officer, the Office of the General Counsel, Human Resources Services, and Information Technology Services.

cc: Chief Operating Officer
Associate Librarian for Strategic Initiatives

▶▶ TABLE OF CONTENTS

- ▶▶ Executive Summary *i*
- ▶▶ Background 1
- ▶▶ Objectives, Scope, and Methodology 10
- ▶▶ Findings and Recommendations 11
 - I. The Library Should Designate a Chief Privacy Officer to Oversee Key Privacy Functions 12
 - Recommendation 13
 - Management Response 13
 - OIG Comment 14
 - II. The Library Should Identify, Evaluate, Minimize, and Control Manual and Legacy Electronic Systems Containing PII 14
 - a. Develop Customized PIAs for Manual Systems 14
 - Recommendation 15
 - Management Response 16
 - b. PIAs for Legacy Electronic Systems 16
 - Recommendations 16
 - Management Response 16
 - c. Employee Ghost Files Should Be Limited and Controlled 16
 - Recommendation 17
 - Management Response 17
 - III. All PII Incidents Should Immediately Be Reported to OIG for Investigation 17
 - Recommendation 18
 - Management Response 18
- ▶▶ Conclusion 19
- ▶▶ Appendix A: Acronyms Used in This Report 20
- ▶▶ Appendix B: Management Response 21

▶▶ EXECUTIVE SUMMARY

The benefits of the information age have been accompanied by the serious side effects of increased identity theft, internet fraud, and predatory cyber activities. Increasingly, the criminal engines of the information age prey on unprotected personally identifiable information (PII) to fuel many of their schemes. PII is now almost as marketable as cash and financial securities. Therefore, Library management must assure that it designs its asset and information security strategies to adequately protect PII against ever increasing threats.

PII is any information that can be used to distinguish or trace an individual's identity, such as name, social security number, birthday, birthplace, mother's maiden name, biometric records, and/or any other piece of personal information which is linked or linkable to an individual. It involves a wide variety of data that has the potential to harm, embarrass, and inconvenience an individual if compromised.

We audited the Library's collection, use, and disposal of PII and concluded that its current approach was inconsistent with best practices as articulated by the Government Accountability Office. Additionally, we found that legacy electronic and non-electronic based systems pose special risks for the Library. The Library's approach to protecting PII can be improved and risk reduced by revising its organizational structure, policies, and procedures. To accomplish those changes we made the following recommendations.

The Library Should Designate a Chief Privacy Officer to Oversee Key Privacy Functions—The Library has not designated a senior official responsible for the oversight of key privacy functions. It leaves to individual Library managers and offices working with Information Technology Services the responsibility for protecting sensitive PII. We also determined that the Library handles PII security inconsistently.

We recommend that the Library designate a Chief Privacy Officer to oversee key privacy functions including formulating PII policy, security, compliance, and training.

The Library Should Identify, Evaluate, Minimize, and Control Manual and Electronic Legacy Systems Containing PII—Many units maintain inadequate security over manual files with employee information including name, address,

home phone number, and social security number for emergency contact information purposes and as unit level employee personnel and performance files. During our surprise inspections, we found files containing sensitive PII unsecured in 53% of cases and work areas with sensitive PII exposed and unattended in 33% of cases.

In addition, our review of legacy electronic systems found various issues, such as social security numbers, systems without password protection or access authorizations, lack of management review of logs, and inadequate segregation of duties in some aspect of system operation.

We recommend that the Library establish procedures to identify, evaluate, minimize, and control manual systems containing PII by designating a centralized function or official to have the responsibility for overseeing PII security for all manual systems; in addition, the Library should identify legacy electronic systems containing sensitive PII and develop a plan to conduct Privacy Impact Assessments. Finally, the Director of Human Resources Services should develop and implement a directive to uniformly control supervisors' employee files.

The Library Should Require That All PII Incidents be Reported Immediately to OIG for Investigation—There is no Library policy direction for reporting unauthorized PII disclosures to the Office of the Inspector General immediately upon discovery. In the absence of an immediate investigation into a PII incident, the potential for greater harm to the violated individual(s) occurs with the passage of time. Additionally, the risk of the audit trail becoming eroded or destroyed increases with delays in commencing an investigation.

We recommend that the Library enact a policy requiring Library management and staff to immediately report all suspected unauthorized disclosures of PII to the Office of the Inspector General.

Library management agreed with our findings and recommendations, and has already acted on several by revising the proposed PII regulation.

▶▶ BACKGROUND

The advent of the information age with its computer technology and world-wide connectivity revolutionized the ability to gather information, expand knowledge, accelerate communication, and transact commerce. All areas of society have benefitted from these rapid technological developments. Unfortunately, as with other great advances, the numerous benefits of the information age have been accompanied by serious side effects. Much like pollution, labor unrest, and workplace illnesses were by-products of the industrial revolution, and weapons of mass destruction and radioactive contamination spun out of the atomic age, the information age has been marked by substantially increased identity theft, internet fraud, and predatory cyber activities.



The criminal engines of the information age rely on personally identifiable information (PII) to fuel many of their activities. PII is any information about an individual that can be used to distinguish or trace an individual’s identity, such as a person’s name, social security number, birthday, birthplace, mother’s maiden name, biometric records, and/or any other piece of personal information which is linked or linkable to an individual.¹



By definition, PII incorporates a wide variety of data. It includes information that has potential for substantial harm, embarrassment, inconvenience, or unfairness to an individual if it is compromised.² Such PII is defined as “sensitive PII” and can be in one of two categories: category 1 sensitive PII is a stand alone data element which may be harmful. Examples include a social security number, a driver’s license number, a passport number, and a bank account number. Category 2 sensitive PII is a piece of information that may be harmful when it is combined with other identity information such as

¹ National Archives and Records Administration Interim Guidance 1603-1, September 26, 2006. Additional examples of an individual’s distinguishing information include educational transcripts, financial transactions, medical history, criminal record, and employment history.

² U.S. Department of Homeland Security, *Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security*. See http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_spII_handbook.pdf

name, address, phone number and/or Social Security number. This sensitive PII may include a biometric record, credit card number, criminal record, date of birth, employment information, financial information, medical history, parent’s name(s), mother’s maiden name, place of birth, and security clearance information.

The information age not only accelerated the collection of PII, but also produced mass databases that expanded PII exposure to unauthorized access and misuse. Moreover, legacy systems³ that were conceived before business and government recognized the threats of the information age are still operating without adequate security protection.

PII Theft at the Library

The Library’s service and support units collect PII on an ongoing basis from employees, customers, donors, and vendors. The Library must be trusted by its constituents to protect the PII they share with it. Any breach in the Library’s protection of PII could harm the trust that Congress, benefactors, and the public place in the Library and adversely affect the Library’s funding and world-wide image.

Unfortunately, as with many other federal agencies, the Library recently experienced a theft of PII. In 2008, an employee who had access to manual documents and

automated systems in Human Resources Services (HRS) obtained and sold the PII of several Library employees. The buyer, who had prior felony convictions, used the stolen

The Washington Post

Woman gets prison for Library of Congress ID theft

By NEDRA PICKLER
The Associated Press
Monday, July 6, 2009 2:31 PM

WASHINGTON -- A woman who worked with her cousin to steal the identities of 13 unsuspecting Library of Congress employees was sentenced Monday to two and a half years in prison.

³ A legacy system is a computer system or application program which continues to be used because the user does not want to replace or redesign it. Legacy systems are considered to be potentially problematic for several reasons including inadequate security, unsupported software, and often, nonexistent documentation. Computer systems implemented prior to 2004 at the Library were not required to have a security certification and accreditation.

information to make fraudulent retail purchases totaling more than \$120,000. As part of its investigation, the Office of the Inspector General (OIG) obtained search warrants and conducted raids on the residences of the two individuals involved. The raids uncovered evidence which led to the individuals' indictments and subsequent guilty pleas to federal felony charges for the sale and misuse of PII.

The Library is by no means the only federal agency to experience a widely-publicized and embarrassing incident of this kind. Some of the many widely-publicized cases in recent years include:

- May 2006 – Department of Veterans Affairs (VA) computer equipment containing PII on approximately 26.5 million veterans and active duty members was stolen from the home of a VA employee.
- November 2004 – A VA e-mail system allowed the public to access folders and files that contained veterans' PII.
- December 2004 – the Department of Agriculture sent an e-mail message to 1,537 people which included an attachment providing the Social Security numbers and other PII for every one of the e-mail's recipients.
- Mid-2005 – the Department of Energy (DOE) announced that a computer hacker had gained access to a file containing the names and Social Security numbers of 1,502 individuals. The incident was detected in mid-2005, but was not reported to senior DOE officials until June 2006.
- June 2006 – the Department of Health and Human Services reported the theft of a contract employee's laptop computer. The computer contained a variety of PII, including medical information, and the incident may have affected 49,572 Medicare beneficiaries.⁴



⁴ U.S. Government Accountability Office, Report No. GAO-08-343, *Information Security—Protecting Personally Identifiable Information*, January 2008.

Laws and Regulations

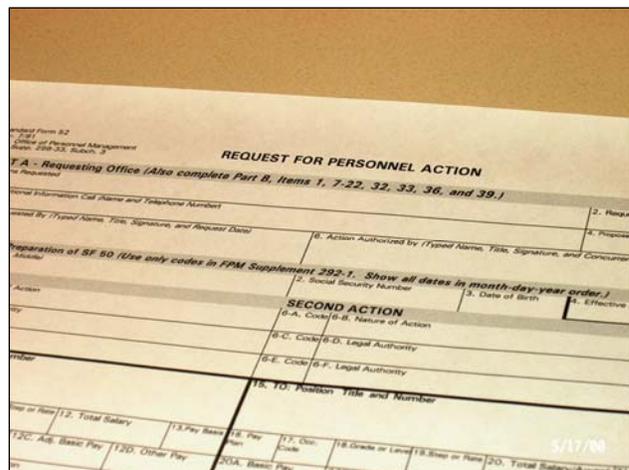
Congress enacted three major pieces of legislation over a 25-year period in response to concerns regarding the federal government’s collection, use, and disposal of PII. The legislation reflects increased threats to PII that have come to light during the information age.

The first was the Privacy Act of 1974 (5 U.S.C. § 552a) which was enacted to control the collection, use, and disclosure of PII within and by the federal government. It was passed during the infancy of the information age prior to the introduction of personal computers, network systems, and the internet.

The second was the E-Government Act of 2002 (Public Law 107-347) which was enacted to promote and enhance electronic services in the Federal government. One of the law’s eleven specific purposes involves...“enhanc[ing] access to Government information and services in a manner consistent with laws regarding protection of personal privacy..., records retention,...and other relevant laws.”

The third was the Federal Information Security Management Act of 2002 (FISMA) (44 U.S.C. § 3541) which was enacted to respond to the need for cyber security in federal government operations. Among other things, FISMA requires:

- A comprehensive framework for ensuring the effectiveness of information security controls over information resources;
- The effective government-wide management and oversight of information security risks related to the highly networked nature of the federal computing environment; and
- The development and maintenance of minimum controls to protect federal information and information systems.



The E-Government Act and FISMA address the realities of networked systems, the internet, and cyber crime.

With limited exceptions, the three statutes do not apply to legislative branch agencies, including the Library. Although it lags behind other agencies in addressing threats to PII, the Library has adopted some of the statutes' requirements as best practices.

Privacy Impact Assessment

The E-Government Act establishes requirements for federal agencies to perform privacy impact assessments (PIAs) for their existing information systems that collect PII and all such systems that agencies plan to develop or procure. PIAs must accompany agencies' funding requests to Congress for new systems. A PIA must identify:

- the information that will be collected,
- why the information will be collected,
- the intended use of the information,
- with whom the information will be shared,
- what notice or opportunities for consent will be provided to individuals regarding the information that will be collected and how that information will be shared, and
- how the information will be secured.

According to the Act, a PIA must be "... commensurate with the size of the information system...the sensitivity of [the system's] information⁵...and the risk of harm from unauthorized release of that information."

A PIA provides assurance that an agency's management has considered the implications of collecting, maintaining, and disseminating PII in an electronic system. Those implications include complying with privacy laws and regulations, realizing the risks and effects of handling PII, and recognizing the security required to mitigate privacy risks.

⁵ The National Institute of Standards and Technology (NIST), in its Federal Information Processing Standards Publication 199 (FIPS PUB 199), *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, prescribes standards to be used by all federal agencies to categorize all information and information systems to determine their sensitivity. FIPS PUB 199 determines sensitivity through categorizing (confidentiality, integrity, and availability) information and information systems and determining the impact levels (low, moderate, and high) on agencies or individuals should there be a breach of security.

Chief Privacy Officers

Federal agencies have scrambled to provide effective protection and security for information systems and other means of managing PII. Unfortunately, they have often had fragmented responses to the fast-moving evolution of information systems, the acceleration in PII collection, and the increased demands of privacy laws and regulations.

Such fragmented approaches have led some agencies to assign PII security responsibilities to their Chief Information Officers. Other agencies have designated officials from their general counsel, civil rights, or public disclosure organizations to directly oversee or share oversight responsibilities for PII protection. Some agencies have even designated such responsibilities to officials who rank below the agencies' senior level. As a result, attention to PII security policies, procedures, compliance, and training throughout the federal government has been uneven and incomplete.

In reaction to continuing PII breaches and concerns regarding fragmented oversight of PII security, the Office of Management and Budget (OMB) issued OMB Memorandum 05-08, which directs executive branch agencies to designate a senior agency official responsible for privacy. This official's role includes overseeing, coordinating, and facilitating the agency's privacy compliance efforts. It requires that the senior official review the agency's information privacy procedures to ensure they are comprehensive and up-to-date, and when necessary, work with the relevant agency offices to revise them. Finally, the designated official should ensure that the agency's employees and contractors receive training on privacy subject matter.

We surveyed the PII security practices followed by legislative branch agencies, recognizing that such agencies are not required to implement OMB Memorandum 05-08. We found that the Government Accountability Office and the U. S. Capitol Police have designated Chief Privacy Officers. Designating a senior agency official to be the agency's Chief Privacy Officer provides an effective means of assuring appropriately strong attention is provided to PII security matters. Accordingly, if an agency is not required to implement OMB Memorandum



05-08, we believe the agency should implement the memorandum's requirements as best practices.

The Library's PII Protection Efforts

The Library has made notable efforts to improve its protection of PII through communication, information system security practices, internal control oversight, and employee training. These efforts have involved work performed by the Library's legal, technical, educational, financial, security, personnel, and managerial elements. Significant initiatives recently undertaken at the Library are summarized in the following paragraphs.

Special Announcement 06-4. The Library issued Special Announcement 06-4, *Sensitive Information Security*, in August 2006. The announcement officially advised Library staff regarding management's concern for PII security and staff responsibilities for protecting that information. It included basic procedures and guidelines for providing PII protection, and details about online Information Technology (IT) security training covering PII protection. It also advised staff that violating PII security policies and guidelines could result in disciplinary action.

Draft Policy on PII Responsibilities. Since October 2008, the Office of General Counsel (OGC) has been developing a Library policy (i.e., draft Library of Congress Regulation (LCR) 1921, *Protection and Disclosure of Personally Identifiable Information*) for handling PII collected and maintained by the Library and defining responsibilities for the proper use, disclosure, and protection of PII. At the time of this audit, OGC advised us that the draft policy was undergoing review by the Library's Executive Committee.

The draft policy requires all service units to inventory their systems that collect and store PII, identify the PII and the purposes for its use, limit PII collection to only the information necessary for required uses, assess PII sensitivity and determine appropriate protection, limit PII access to authorized individuals, respond immediately to reports of improper disclosure,

establish and provide training on PII handling, and update PII analyses as needed.

In the event of unauthorized access or improper disclosure of PII, the draft policy directs staff to notify their supervisor who should then relay the incident's information to the OIG.

We are pleased to report that management revised the proposed LCR in response to our draft report, incorporating significantly all of our best-practice recommendations.

Customized PIA. The Library's Information Technology Security Group (ITSG) developed a customized PIA for Library-wide use and recently placed it into service. More rudimentary PIAs have been in Information Technology Services (ITS) directives since 2005 and used as far back as the fall of 2004 in the implementation of the Momentum financial system. The customized PIA developed by the ITSG is an integral component of the systems development life cycle model⁶ for electronic information systems that are developed at the Library. We commend the ITSG for its leadership and advocacy of PII security at the Library and the progress made to date in improving the Library's awareness of the issue.



Coverage of PII by the Internal Control Program (ICP). The Library's ICP calls for service and infrastructure units to conduct assessments of their internal control systems yearly (i.e., Vulnerability Assessments) and also, depending on the assessed risk level, in more detail once every one to five years (i.e., Detail Control Reviews). PII security is reviewed in the

⁶ The systems development life cycle is a conceptual model used in project management that describes the stages involved in developing an information system, from its initial feasibility study to the maintenance of the completed application and concluding with the system's disposal.

process of such assessments. Ongoing training covering PIAs, PII security, and FIPS PUB 199 requirements is provided by the ICP for service and infrastructure unit ICP coordinators and ICP module officials to facilitate the performance of the units' internal control assessments.

PII Coverage by ITS' Security Awareness Training.

The Library has included PII subject matter in its annual online ITS security awareness training since 2006. This mandatory security awareness training course stresses the importance of PII protection directly to each member of the Library's staff.

» OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of our audit were to determine if management adequately protected PII during its collection, use, and disposal. We performed our fieldwork from October 2008 through June, 2009.

The scope of our audit included evaluating the effectiveness of existing policies and procedures for protecting PII, analyzing Library management's oversight for protecting PII, and reviewing staff compliance with Library policies and procedures for protecting PII.

Our audit methodology included:

- Reviewing applicable laws and regulations,
- Benchmarking Library policies and procedures with other Federal Agencies,⁷
- Surveying service and program units to determine the type and content of PII collected, and to identify the systems used to maintain PII,⁸
- Interviewing service and program unit management to document PII protection practices, and
- Conducting surprise inspections of service and program units' facilities to randomly observe the handling of PII and their compliance with PII security policies and procedures.

We conducted this performance audit in accordance with generally accepted government auditing standards and LCR 211-6, *Functions, Authority, Responsibility of the Inspector General*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our conclusions based on our audit objectives.

⁷ We benchmarked against agencies such as the Government Printing Office, Government Accountability Office, Securities and Exchange Commission, U.S. Capitol Police, and National Archives and Records Administration. Our inquiries included reviewing audit recommendations regarding the protection of PII at those agencies.

⁸ We surveyed seven service and program units as well as six separate functions in the Librarian's Office.

►► FINDINGS AND RECOMMENDATIONS

Congress has enacted legislation to regulate and protect the collection, use, and disposal of PII by executive branch agencies. However, legislative branch agencies including the Library have generally been left to devise their own policies and procedures for protecting PII. Recent events demonstrate that the Library is not immune to PII abuse and reveal that it must strengthen its PII protection.

We found that the Library needs to address organizational, policy, and compliance issues to more appropriately protect PII. The Library's decentralized approach to PII security runs counter to current best practices and has been accompanied by inadequate internal control compliance.⁹

Although the Library through the Information Technology Security Group (ITSG) implemented a customized PIA and certification and accreditation¹⁰ (C&A) process for new and existing systems, the process has not caught up with a number of legacy systems present in the Library. Our review leads us to conclude that PII in both manual and legacy electronic systems at the service unit level is at risk for compromise and theft. We determined that many of these systems had inadequate internal control design and deficient security.¹¹ We believe a comprehensive Library-wide effort is needed to

⁹ During our field work we conducted surprise inspections in the working areas of seven service units. We found that 53% of file cabinets containing PII documents were left unsecured and unlocked. In addition, we found documents containing PII unsecured in 33% of unattended work areas we inspected.

¹⁰ NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004, states that security certification and accreditation are important activities that support a risk management process and are an integral part of an agency's information security program. <http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf>

¹¹ Our review of 17 electronic systems in seven service units found: 1) systems data with social security numbers, 2) systems allowing access without passwords, 3) systems without user access forms documenting authorization to use and user signed confidentiality statements, 4) service unit management not reviewing system activity logs to identify and investigate unusual or suspicious system activity, and 5) systems with inadequate segregation of duties in some aspect of system operation.

improve PII security and to diminish the existing level of risk. To that end, our findings and recommendations follow:

I. The Library Should Designate a Chief Privacy Officer to Oversee Key Privacy Functions

The existing Library policies which address management responsibilities for PII assign those responsibilities to several Library persons and organizations.

Existing Library policy on privacy information is provided in Special Announcement 06-4, *Sensitive Information Security*, which was issued by the Office of the Librarian in August 2006. The Special Announcement assigns responsibility for access to and use of sensitive information to individual Library managers and offices in coordination with ITS.

The Library's existing approach for managing PII is contrary to the GAO's opinion on that subject. In the GAO's view, centralizing authority for an agency's information privacy programs is very important. In its May 2008 report *PRIVACY-Agencies Should Ensure That Designated Senior Officials Have Oversight of Key Functions*, the GAO states that "[a]gencies that have more than one internal organization carrying out privacy functions run the risk that those organizations may not always provide the same protections for personal information if they are not overseen by a central authority. Thus, unless steps are taken to ensure that key privacy functions are under the oversight of [a senior agency privacy officer]...agencies may be limited in their ability to ensure that information privacy protections are implemented consistently across their organizations."¹²

The existing Library approach for managing PII is also inconsistent with OMB Memorandum 05-08, *Designation of Senior Agency Officials for Privacy*, which was issued in February 2005. In that memorandum, OMB calls for executive branch agencies to designate a senior agency official to be responsible for agency-wide information privacy. OMB envisioned that such an official would have:

¹² GAO Report GAO-08-603, *PRIVACY-Agencies Should Ensure That Designated Senior Officials Have Oversight of Key Functions*, May 2008, p-17.

- a central role in overseeing, coordinating, and facilitating the agency's compliance efforts;
- a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals;
- responsibility for ensuring the agency's employees and contractors receive appropriate training and education programs regarding information privacy; and
- overall responsibility and accountability for ensuring the agency's implementation of information privacy protections.

Using the decentralized strategies described in the existing Library policy to manage Library-maintained PII makes accountability for the information's security questionable and hampers the protection that could otherwise be provided for the information if Library-wide responsibility for it was assigned to one senior-level official. The absence of a designated Chief Privacy Officer for the Library to provide oversight for privacy information functions exposes the Library to substantial risk for PII loss and compromise that could result from inconsistent procedures on handling and security of PII.

Although it is not required to conform to OMB Memorandum 05-08, the Library should either follow the memorandum's direction as a best practice or adopt the memorandum's requirements as part of an agency-wide PII policy.

Recommendation

The Library should designate a senior-level Library official to serve as Chief Privacy Officer. This official should be assigned overall responsibility for all of the Library's privacy information activities, including the formulation of PII policy, design and implementation of PII security, assurance of PII policy compliance, and provision of PII training.

Management Response

Management agreed with our recommendation.

OIG Comment

Subsequent to the release of our draft report, management revised proposed LCR 1921 to reflect the best-practice approach we recommended. We commend management for acting quickly.

II. The Library Should Identify, Evaluate, Minimize, and Control Manual and Legacy Electronic Systems Containing PII*a. Develop Customized PIAs for Manual Systems*

Existing Library policy which addresses management responsibilities for PII assigns those responsibilities to several Library persons and organizations. As indicated in this report's previous finding, the existing policy is provided in Special Announcement 06-4, *Sensitive Information Security*. Specifically, it assigns responsibility for access to and use of sensitive information to individual Library managers and offices in coordination with ITS. However, the Special Announcement does not assign overall responsibility for or specifically identify procedures to provide protection for PII that is contained in the Library's manual record-keeping systems and files. Accordingly, individual Library managers and offices are left on their own to develop, implement, and enforce security procedures that provide protection for PII contained in the Library's manual systems and files.

The Library manages security for PII maintained in its manual systems and files differently from the way that it manages security for PII in its electronic systems. Where PII security for the manual systems is left to many different parties to manage and oversee, management and oversight of such security for the electronic systems is centrally provided by the ITSG element of the ITS organization. ITSG does not have any management or oversight responsibilities for manual systems and files maintained by Library personnel that do not support the Library's electronic systems.

Using the decentralized general strategy described in the existing Library policy to manage protection for PII maintained in manual systems and files hampers the security that could otherwise be provided for the information if

responsibility for it was assigned to one senior-level Library official and Library-wide procedures for it were available.

The absence of a senior-level Library official and uniform procedures to manage protection for PII maintained in manual systems and files exposes the Library to unacceptable levels of risk for PII loss and compromise that could result from inconsistent PII procedures on handling and security.

Moreover, the absence of a senior-level official and uniform procedures make it more difficult for the Library to prevent the use of unauthorized manual systems or manual systems that collect and maintain unnecessary PII.

PIAs are used by ITSG and agencies of the executive branch to evaluate the need for their electronic systems to collect PII and the PII security that their electronic systems provide. In our view, PIAs should be applied to the Library's manual systems for the same purposes.

Recommendation

The Library should assign overall responsibility for managing protection of PII maintained in the Library's manual systems and files to the Library's Chief Privacy Officer, once that officer has been designated. That officer should ensure that:

1. a comprehensive inventory of all of the Library's manual systems which contain PII is taken,
2. the use of manual systems that contain PII is minimized to the greatest extent possible,
3. procedures are established to evaluate, protect, and control manual systems, and
4. a customized PIA is developed for manual systems containing PII which identifies:
 - the information that will be collected;
 - why the information will be collected;
 - the intended use of the information;
 - with whom the information will be shared;
 - what notice or opportunities for consent will be provided regarding the information that will be collected and how that information will be shared; and
 - how the information will be secured.

Management Response

Management agreed with our recommendation.

b. PIAs for Legacy Electronic Systems

We found evidence of substantial risk of PII loss and compromise when reviewing legacy electronic systems (see footnote 11). Some of these systems, due to age, limited use, or other valid factors, did not receive a high priority when resources were being allocated to conduct costly C & As. Notwithstanding this fact, the presence of sensitive PII in these systems requires a uniform approach to assure basic PII internal controls are present. The ITSG has begun addressing this through the Internal Control Program; however, we believe a stronger emphasis on PIAs should be adopted.

Recommendations

The Library should:

1. identify legacy electronic systems containing sensitive PII, and
2. adopt a plan to conduct PIAs for these systems.

Management Response

Management agreed with our recommendations.

c. Employee Ghost Files Should Be Limited and Controlled

Many Library service units maintain manual files which contain PII regarding Library employees, including employee names, addresses, home residence phone numbers, and social security numbers. We were informed by some organizations that the PII in these files is retained as contact information for emergency situations and also as reference data accompanying personnel performance information.

We found that the Library's collective bargaining agreements¹³ (CBA) address the maintenance of secondary files for Library employees by their supervisors but Library policies, regulations, and procedures do not. The CBAs allow Library supervisors to maintain files with emergency and performance

¹³ Agreements with AFSCME locals 2910 and 2477.

related material provided that employees have the right to review the file contents and management controls access to and disposal of those files. The CBAs prohibit any other employee files not complying with their requirements while referring to unauthorized files as “ghost files.”

Special Announcement 06-4, issued by the Librarian’s Office in 2006, provides general requirements for protecting sensitive data collected and maintained by the Library and HRS Directive 7-01-02 titled *Security of Sensitive Data*, issued in 2008, provides procedures for protecting PII (HRS should edit its directive by referring to the related IT security directive for PII). Neither of these specifically addresses the maintenance of employee ghost files by supervisors.

Because Library policies, regulations, and procedures do not specifically address ghost files for non-bargaining unit employees, supervisors may be unnecessarily collecting and retaining PII for them without adequate security. As a result, such PII may be vulnerable to theft and compromise.

Recommendation

The Director of HRS should develop and implement a policy directive that specifically addresses worksite files, supervisory notes, and ghost files for non-bargaining unit employees to ensure uniformity and security.

Management Response

Management agreed with our recommendation.

III. All PII Incidents Should Immediately Be Reported to OIG for Investigation

The value of a quick response to an incident involving a person’s PII is recognized in OMB Memorandum 06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*. That memorandum requires all agencies to report PII security incidents to a federal incident response center within one hour of discovering the incident. The federal response center then forwards all agency reports to the appropriate Identity Theft Task Force point-of-contact within one hour of being notified.

At the time of this audit, the Library did not have a policy for responding to PII incidents when they are discovered. But, direction on PII incident response was included in the original version of the Library's proposed policy on protecting PII that was under review by the Executive Committee when we concluded our audit fieldwork. Section 7 of that proposed policy version, draft LCR 1921, *Protection and Disclosure of Personally Identifiable Information*, stated that "[l]ibrary employees, contractors, and others with access to PII must report any known or suspected instance of unauthorized access or improper disclosure of PII to their immediate supervisor or Contracting Officer's Technical Representative (COTR) immediately upon discovery. These individuals shall relay the information to the Office of the General Counsel without delay. The General Counsel will promptly notify the Chief Operating Officer and appropriate service and infrastructure units."

Quickly recognizing, investigating, and resolving an incident involving a person's PII is critical and will generally minimize the harmful effects that the person will sustain from the incident. Moreover, the longer it takes to commence an investigation of a PII incident correspondingly increases the probability that the audit trail will be eroded or destroyed, making facts surrounding the incident more difficult to find or unavailable.

Members of the Library's Office of the Inspector General (OIG) have the training and experience to quickly respond to, investigate, and resolve PII incidents. Accordingly, Library policy on protecting PII should require Library management and staff to promptly report all unauthorized disclosures of PII incidents to the OIG.

Recommendation

The Library should develop and implement policy that requires Library management and staff to promptly report all PII incidents to the OIG.

Management Response

Management agreed with our recommendation and has made the necessary change to the current draft of the PII LCR.

» CONCLUSION

The trust of employees, customers, donors, and the Congress in the Library's ability to protect PII must be continuously justified. However, doing so could be problematic as the Library's PII protection activities move forward. The Library's current fragmented approach to PII protection is inconsistent with best practices that currently prevail in federal agencies.

To improve its protection for the PII in its custody, the Library must improve its policies and procedures to make certain its overall approach to PII security is consistent. Moreover, it must address controls in its legacy and manual systems and prompt investigations of PII incidents.

The starting point for establishing effective PII security policies and procedures is the designation of a senior-level official and making that official responsible for administering PII security. Under that officer's leadership, all current and future efforts to collect, store, and dispose of PII can be uniformly evaluated and, if justified, processed in a secure and consistent manner.

Major Contributors to This Report:

Nicholas Christopher, Assistant Inspector General

John Mech, Lead Auditor

Jennifer Spruill, Auditor

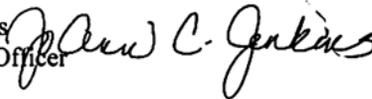
Peter TerVeer, Management Analyst

▶▶ APPENDIX A: ACRONYMS USED IN THIS REPORT

AFSCME	American Federation of State, County and Municipal Employees
CBA	Collective Bargaining Agreement
DHS	Department of Homeland Security
DOA	Department of Agriculture
DOE	Department of Energy
DCR	Detailed Control Review
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
HHS	Health and Human Services
HRS	Human Resources Services
ICP	Internal Control Program
IT	Information Technology
ITS	Information Technology Services
ITSG	Information Technology Security Group
LCR	Library of Congress Regulation
OCFO	Office of the Chief Financial Officer
OGC	Office of the General Counsel
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
VA	Department of Veteran's Affairs

▶▶ APPENDIX B: MANAGEMENT RESPONSE

UNITED STATES GOVERNMENT

Memorandum*Office of the Chief Operating Officer
Library of Congress***TO:** Karl Schornagel
Inspector General**DATE:** August 31, 2009**FROM:** Jo Ann C. Jenkins
Chief Operating Officer**SUBJECT:** Personally Identifiable Information

Thank you for the opportunity to respond to your draft audit, Personally Identifiable Information (PII). There are two points we want to highlight – the LCR on PII and the concept of “ghost files.”

First, as you are aware, the Office of General Counsel has incorporated your recommendations into the draft LCR on PII and will be forwarding that draft to the EC and LCR working group. OGC had held off issuing the draft, at your request, until they received the draft audit. We agree with your recommendations and are pleased that you are comfortable with the revisions to the draft LCR. OGC plans to have this regulation issued by early September.

Second, we want to respond to Section II.c. “Employee Ghost files should be Limited and Controlled.” The draft audit report characterizes all manual files maintained by service units that contain PII regarding Library employees as “ghost files.” The assumption is that any “secondary” file with employee PII maintained by a service unit is a “ghost file” and is contrary to Library policy. This assumption is incorrect.

In fact, there are three major types of appropriate personnel files that contain employee PII:

- (a) the Official Personnel Folder (OPF) which is now maintained as an Electronic Official Personnel Folder (eOPF);
- (b) the worksite file; and
- (c) supervisory notes

There is only one type of inappropriate personnel file, the so-called “ghost file.” The draft audit report does not distinguish between appropriate worksite files and supervisory notes, on the one hand, and inappropriate “ghost files,” on the other.

-2-

Worksite File

The worksite file is addressed in the Library's collective bargaining agreements. For example, Article 12, Personnel Records, of the AFSCME Local 2910 collective bargaining agreement, defines "worksite files," the controls on access to such files, and disposal schedule for such files, as follows:

Section 2. Worksite File

- A. In addition to the OPF, the Library may maintain one (1) employee file in the service unit to which the employee is assigned and one employee file at the worksite or the operational "division" office to which the employee is assigned. These files are intended as sources of information relating to emergency addresses, record copies of PARs, production records, attendance, job performance, training, discipline, awards, and other information pertinent for the supervisor's use. Nothing in this article shall prohibit the Library from establishing and maintaining other files, such as health, training, payroll, central book charge, LC Police, personnel security, and other such necessary records. However, the following official operating files kept by the Library for investigative purposes shall not be subject to employee access upon request: LC Police, personnel security, and internal audit.
- B. No record in a worksite personnel file which has not been disclosed to the employee may be used as a basis for disciplinary action.
- C. No derogatory material which may reflect adversely upon the employee's character or government career may be included in a worksite personnel file without evidence that the employee saw and had the opportunity to initial the material.
- D. An officially authorized person may inspect such records and files only after signing in advance of inspection of a record indicating his/her name, organization and office, and the reasons for the inspection. This record shall be maintained as part of the file and shall be available at all times for inspection by the employee or his/her representative. The management official designated to be responsible for the file, and clerks who must use the file in the course of their work, are exempt from signing this record. No record or document in an employee's file will be made available to any unauthorized persons to inspect, review, copy, or photocopy. Such information will be made available to authorized persons only for official use as provided in the FPM.
- E. Each employee or designated representative has the right upon request to review and photocopy without charge his/her records and files. The Library employee having custody of the file may monitor the photocopying of documents from the files.

-3-

- F. The employee or his/her designated representative may review the contents of such files upon demand unless it becomes necessary because of reasons of workload to require an appointment for such review.
- G. When a supervisor who has kept detailed records of an employee's performance or conduct has determined that there is probable cause for recommending an adverse action, there should be written evidence that the employee is aware of this. The supervisor must inform the employee of the existence of these records within thirty (30) days of initiating the records. These records should be destroyed after: (a) appropriate action has been taken, if any; (b) opportunity for any appeals has expired; or © after one (1) year, whichever comes last.
- H. Worksite files are considered temporary records and should be disposed of one (1) year following the separation or reassignment of the employee. All other employee files retained by the Library shall be disposed of in accordance with the General Records Schedule and other laws or directives of higher authority to which the Library is subject.
- I. Official memoranda or letters of admonishment, warning, caution, and similar documents are considered temporary and are not to be kept in a worksite file longer than two (2) years unless the Director of Human Resources shows cause why a longer retention period is necessary. Human Resources Services shall notify the employee of the retention period.
- J. Employees may put any statement on record in response to information they consider unfavorable to themselves which is filed in the worksite personnel file.
- K. Employees have the right to update their personnel files with relevant information regarding experience, education, or training, etc., which might enhance their careers. Supervisory Notes: Supervisory notes also are addressed in the collective bargaining agreements. For example, the same Article of the AFSCME Local 2910 collective bargaining agreement has the following provision on supervisory notes: Section 7. Supervisory Notes Supervisory notes are not "Ghost files." Supervisory notes (files) are records that contain notes on meetings; discussions with staff members, managers, and the public; editorial comments; historical events; recollections that are regularly kept by supervisors in places which are intended to be accessible to that supervisor only. These records are, in effect, an extension of the supervisor's memory, and may be legitimately kept by the supervisor for any length of time. Supervisory notes belong to the supervisor; they must not be used by or be accessible to any other supervisors who wish to make personnel decisions. These notes or records involving employees can be and often are the basis for the action or warning against an employee and would be reflected, but not necessarily divulged to an employee, in a

-4-

formal memorandum which would contain the basis for the action or warning against an employee.

Such documentation would be consistent with the pertinent provisions of the Collective Bargaining Agreement. Supervisory notes (files) may be established by a supervisor who counsels an employee and makes notations over a period of time and later documents an oral warning pursuant to LCR 2017-5 (Obligations of Management and Staff to Fulfill Position Requirements). He/she may keep these notations for use as a basis for any testimony at a hearing. Similarly, a supervisor may make notations on an individual's tardiness, use them for an action, and keep them for use at a meeting or hearing. "Ghost Files": The same Article of the AFSCME Local 2910 collective bargaining agreement distinguishes impermissible "Ghost Files," which are prohibited: Section 6. Ghost Files "Ghost files" are collections of papers or publications arranged or classified by an employee's name and maintained in a folder, case, cabinet, or file and kept from the employee, and used by other supervisory personnel in making personnel decisions about unit employees. "Ghost files" will not be kept and are illegal and contrary to the purposes and intent of this Agreement.

- L. Note that files that are available to employees, such as the worksite file, are by definition not "ghost files." Similarly, files, such as supervisory notes, that are used only by the employee's supervisor rather than by "other supervisory personnel," are by definition not "ghost files."

Conclusion

Human Resources Services respectfully requests that the Inspector General rewrite the section of the draft audit report on "ghost files" to include a discussion of worksite files and supervisory notes (which are appropriate "secondary files"). The report should distinguish worksite files and supervisory notes from "ghost files" (which could be characterized as inappropriate "tertiary files").

There is no need to task Human Resources Services with developing and implementing a policy directive that addresses secondary personnel and performance files for bargaining-unit staff, because such policies already exist in the collective bargaining agreements. Although it is likely that the service units apply the same policy regarding such files with regard to non-bargaining unit staff, Human Resources Services will issue a directive applying the same policy to worksite files, supervisory notes and "ghost files" maintained on non-bargaining unit employees.

Please let me know if you have any questions regarding this response.