



***OFFICE OF THE CHIEF
INFORMATION OFFICER***

***The Department's Privacy Impact
Assessment Process Is Generally
Implemented Well, But Some
Improvements Are Needed***

Final Inspection Report No. OSE-19047/September 2008

FOR PUBLIC RELEASE

Office of Systems Evaluation



UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

SEP 24 2008

MEMORANDUM FOR: Suzanne Hilding
Chief Information Officer

FROM: *Judith J. Gordon*
Judith J. Gordon
Assistant Inspector General for Audit and Evaluation

SUBJECT: *The Department's Privacy Impact Assessment Process Is Generally Implemented Well, But Some Improvements Are Needed*
Final Report No. OSE-19047

This is our final report on the results of our Federal Information Security Management Act (FISMA) evaluation of the Department's privacy impact assessment process and Web privacy policy and processes. We recommended several policy and process improvements, but overall we found that the Department's IT privacy policy and privacy impact assessments comply with the E-Government Act and OMB guidance, and a process is in place to ensure Web policy compliance.

In response to our draft report, you concurred with our findings and indicated that the Office of the Chief Information Officer will implement all the recommendations outlined in the report. We request that you provide us an action plan describing the actions you have taken or plan to take in response to our recommendations within 60 calendar days of the date of this report. The plan should be in the form of plans of action and milestones (POA&Ms) as required by FISMA.

We appreciate the cooperation and courtesies extended to us by your staff and Commerce operating unit personnel during our evaluation. If you would like to discuss any of the issues raised in this report, please call me at (202) 482-2754 or Allen Crawley, Deputy Assistant Inspector General for Systems Evaluation, at (202) 482-1855.

cc: Lisa Westerback, Director, Office of IT Policy and Planning
Earl Neal, Director, Office of IT Security, Infrastructure and Technology
Trudy Gallic, Audit Liaison

CONTENTS

Introduction.....	1
Findings and Recommendations	3
I. The Department’s IT Privacy Policy Is Out-of-Date and Needs Revision.....	3
II. Some PIAs Do Not Adequately Address All the Required Elements	5
III. The Department Has Implemented a Process for Determining Web Policy Compliance but Needs to Strengthen Validation.....	7
Appendix A: Objectives, Scope, and Methodology.....	9
Appendix B: Reviewed Privacy Impact Assessments	10
Appendix C: Chief Information Officer Response	11

INTRODUCTION

Federal agencies obtain and maintain significant amounts of personally identifiable information (PII) about individuals that must be safeguarded from loss or misuse. The E-Government Act of 2002 requires agencies to conduct privacy impact assessments (PIAs) of information systems and collections containing PII and, if practicable, to make them publicly available to assure the public that personal information is well protected. The act also requires agencies to post privacy policies on their public Web sites in a machine-readable format.

The Department's *Information Technology (IT) Privacy Policy*, last revised January 29, 2007, sets out Commerce's policies for implementing the privacy provisions in the E-Government Act and the requirements of the Office of Management and Budget's (OMB's) M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. The Department's IT privacy policy defines the responsibilities Commerce operating units have for conducting PIAs and posting PIAs and privacy policies on Commerce Web sites. In accordance with OMB M-03-22, the Department's IT privacy policy requires that all PIAs document the following elements:

- What information is being collected, maintained, or disseminated.
- Why the information is being collected, maintained, or disseminated.
- Intended use of the information.
- With whom the information will be shared.
- What opportunities individuals or businesses have to decline providing information in the case of voluntary collections; and opportunities to consent to particular uses of the information and how they can grant consent.
- How the information is secured.
- Whether the collection will result in the creation of a system of records¹ within the meaning of the Privacy Act.

In addition, the Department's Chief Information Officer (CIO) requires the following elements to be documented:

- Identifying information: OMB Exhibit 300 Identification Number; name of system or OMB information collection control number; related Privacy Act System of Records notice; and name, e-mail address, and phone number of a contact person.
- A brief description of the system.
- Event or reason the PIA was conducted.
- The law or regulation that authorizes collection and maintenance of the information.

The policy names the Department's CIO as the official responsible for ensuring that personally identifiable information in Commerce systems is effectively protected. These responsibilities include developing and disseminating policy and guidance on preparation of and posting Web privacy policies and PIAs and reviewing and approving PIAs. The CIO is also responsible for the

¹ The Privacy Act of 1974 (5 U.S.C. § 552a) defines a system of records as a group of records under the control of the agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

submission of mandatory PIAs to OMB as well as required E-Government Act compliance reports.

OMB requires offices of inspector general to qualitatively assess the agencies' PIA processes as part of the Federal Information Security Management Act (FISMA) reporting requirements. To meet our FY 2008 FISMA requirements, we evaluated the Department's PIA and Web privacy processes. We sought to determine whether the Department's PIA process included all the key aspects of conducting and publicly posting PIAs as called for in the E-Government Act and in OMB guidance. We also sought to determine whether policies and processes for determining continued compliance with stated Web privacy policies are adequate and ensure machine-readability on public Web sites. (See appendix A.)

Chief Information Officer Response

In responding to our draft report, the Department's Chief Information Officer concurred with all of our recommendations. The CIO's written response is included as appendix C.

FINDINGS AND RECOMMENDATIONS

I. The Department's IT Privacy Policy Is Out-of-Date and Needs Revision

The Department's IT privacy policy provides guidance for determining when a PIA must be conducted for an information system or collection and what information must be documented. The policy is consistent with the E-Government Act and OMB M-03-22 guidance but is outdated. The policy does not include new PIA requirements recently imposed by the Department's CIO.

In a December 18, 2007, memorandum to all chief information officers, *Data Extract Log and Verify Requirement*, the Department's CIO required operating units to take the following actions by March 28, 2008:

1. Review and update all existing PIAs, specifically describing how the log and verify requirement of OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, has been implemented for the system.²
2. Develop PIAs for all investigative, law enforcement case files, and human resource databases even if they were previously exempt because they have not been modified or contain information only about federal employees.

Although the stated purpose of the memorandum was to document the implementation of OMB's data extract log and verify requirement, it effectively changes the IT privacy policy PIA exemption for legacy and currently operational systems, as well as systems that contain information only about federal employees and requires that *all* Commerce systems containing PII be assessed for privacy impact. We confirmed that the Department intends *all* Commerce systems with any personally identifiable information to have a PIA.

We also found the Department's Office of the CIO (OCIO) has requested that PIAs document whether the records collected are being retained, and if so, to include the specified retention schedule. However, these requirements are not part of the Department's IT privacy policy.

As the authoritative source for guidance on the PIA process, the Department's IT privacy policy should be updated and revised to incorporate all new requirements. We note the *Data Extract Log and Verify Requirement* memorandum has been posted to the Department's IT security and privacy Web page but there is no indication that it contains new requirements or changes to the PIA process.

Finally, in describing the requirements for privacy impact assessments, the Department's IT security policy references the E-Government Act but does not refer to the IT privacy policy. This reference should be included in the current IT security policy update.

² OMB M-07-16 requires that agencies log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required.

Recommendations

The Department's Chief Information Officer should direct appropriate managers to

- 1.1 update the IT privacy policy to incorporate all new PIA requirements; and
- 1.2 update the Department's *IT Security Policy and Minimum Implementation Standards* to refer to the IT privacy policy for guidance in developing PIAs.

II. Some PIAs Do Not Adequately Address All the Required Elements

The Department's IT privacy policy requires operating units to submit PIAs for review and approval. The Department's CIO is responsible for the review and approval of PIAs to ensure compliance with the privacy provisions of the E-Government Act, OMB M-03-22, and Department policy.

We reviewed 20 PIAs and found they generally met the intent of OMB's guidance. We believe this is attributable in part to the helpfulness of OCIO staff in providing guidance and consultation to the operating units during the PIA development and review process. However, 4 PIAs did not provide sufficient information for certain specific elements required by OMB M-03-22—what information is being collected, maintained, or disseminated; with whom the information will be shared; and how the information will be secured.

We also determined that 14 of the PIAs did not include sufficient information for 1 or more of the additional elements required by Department policy (but not by OMB)—identifying information (point of contact information or the OMB Exhibit 300 identification number); event or reason the PIA was conducted; and the law or regulation authorizing the collection and maintenance of the information.

Table 1 identifies the PIAs that did not adequately address the elements discussed in the preceding paragraphs and identifies those elements.

Six PIAs we reviewed did not include the OMB Exhibit 300 identification number. (See table 1.) The Department's CIO uses the Exhibit 300 process to ensure that systems containing personally identifiable information are identified and assessed. The Department's IT privacy policy elaborates on the specific relationship between the assessment and Exhibit 300. It states PIAs "must clearly indicate the link between the privacy system or information collection covered by the PIA and the related major information system described in the OMB Exhibit 300." OCIO staff told us, however, that Exhibit 300 numbers might not be applicable for certain PIAs. OCIO should revise the Exhibit 300 section of the policy to stipulate when an Exhibit 300 number is not needed.

Recommendations

The Department's Chief Information Officer should direct appropriate managers to

- 2.1 revise the Exhibit 300 section of the IT privacy policy to make it clear when Exhibit 300 identification numbers are needed in PIAs;
- 2.2 ensure that PIAs are not approved unless they contain all elements required by the Department's IT privacy policy; and
- 2.3 consider developing additional guidance on the level of detail to be provided for each PIA element required by the Department's IT privacy policy.

Table 1. PIAs That Did Not Adequately Address the Required Elements

PIAs	PIA Elements						
	OMB M-03-22 elements			Additional Department elements			
	Information Collected	Information Shared	Security controls	OMB Exhibit 300 No.	Point of Contact	Event	Law
Economic Development Administration (EDA)							
WebCIMS				X		X	
National Telecommunications and Information Administration (NTIA)							
Digital Coupon Program			X	X			
Office of the Secretary (OS)							
ZyIndex					X	X	X
CSTARS		X				X	
MAPS					X	X	
ACES				X		X	
HSPD-12				X	X		
National Oceanic and Atmospheric Administration (NOAA)							
Crab EDR	X						
Permits Alaska	X					X	
Grants Online						X	
National Vessel Monitoring System						X	
Marine and Aviation Health Services							X
Web Application Subsystem						X	
U.S. Census Bureau							
Population Estimates				X			
National Longitudinal Mortality Study				X			

The following Census PIAs addressed all elements: Center for Economic Studies, Field Support System, Geographic Support Systems, Longitudinal Employer Household Dynamic (LEHD) Program, and Survey of Business Owners.

III. The Department Has Implemented a Process for Determining Web Policy Compliance but Needs to Strengthen Validation

The E-Government Act requires federal agencies to post machine-readable Web privacy policies on their sites. The Department's Web policy, *Privacy of Visitors to DOC Web Sites*, requires all Commerce public Web sites to have privacy policy statements that describe in plain language what information is collected; how long it is retained; how it is used; what information is shared, with whom it is shared, and how the user can give consent; the prohibition on the use of persistent technology except under certain circumstances; and how Web sites that have interactions with children handle getting parental consent.

Machine readability of posted Web privacy policies ensures users can be alerted automatically when posted Web site privacy practices do not match personal privacy preference settings in Web browsers. Machine readability is provided by the Platform for Privacy Preferences Project (P3P) protocol.

OCIO, through its Web Advisory Group, has developed two presentations for training system administrators and users on implementing P3P. The training for system administrators covers development of machine-readable policies on Web sites. The user training covers setting browser preferences.

In January 2001, the Department's CIO established an annual Web site certification policy, which requires operating unit CIOs to certify their Web sites comply with the Department's Web policy, including machine readability of privacy policies on public Web sites. For those Web sites that are determined to be noncompliant, the operating unit CIOs must submit a noncompliance report that includes an explanation for the noncompliance and a target date for compliance.

To validate the annual operating units' certification, Department CIO staff evaluates Commerce's 21 major Web sites³ for compliance. However, this approach does not consider the variations in the number of Web sites within operating units. For example, 5 operating units have 1 or 2 Web sites, whereas 3 operating units have more than a hundred. To be effective, the validation should evaluate for each operating unit a number of Web sites proportional to its total number of Web sites. For FY 2007, the Department identified a total of 842 Web sites.

We also found that the evaluation process did not validate P3P implementation. After we brought this problem to the attention of OCIO staff, the validation process was modified to use both the Internet Explorer browser and the World Wide Web Consortium P3P Validator tool to validate P3P implementation. OCIO staff provided us an overview and demonstration of the P3P validation process on several operating unit Web sites we selected.

³Commerce defines the major Web sites as the home pages for Commerce, operating units including six NOAA line offices, the U.S. Patent and Trademark Office, the Office of Inspector General, and Office of General Counsel.

Recommendation

- 3.1 The Department's Chief Information Officer should ensure that a more representative number of Web sites across the operating units are examined to validate reported annual compliance with the Department's Web policy.

APPENDIX A: OBJECTIVES, SCOPE, AND METHODOLOGY

As part of our FY 2008 FISMA requirements, we evaluated whether the Department's PIA process adheres to existing policy, guidance, and standards. In addition, we evaluated policies and processes for determining continued compliance with stated Web privacy policies and ensuring machine readability on public Web sites (i.e., use of Platform for Privacy Preferences Project [P3P]). The results of this evaluation will be included in our annual FISMA report to OMB.

To meet our objectives, we randomly selected for review 20 of the 36 PIAs that had been approved by the Department. (See appendix B.) We also interviewed the manager and staff from the Office of IT Policy and Planning, which handles the PIA process and Web privacy for the Department's CIO office, as well as staff from Census, NOAA, and NIST involved in the PIA development and Web privacy compliance processes. Our evaluation criteria included the E-Government Act of 2002; OMB M-07-19, *Reporting Instructions for FISMA*; OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*; U.S. Department of Commerce *Information Technology Privacy Policy*; and U.S. Department of Commerce *Privacy of Visitors to DOC Web Sites*.

We conducted this evaluation in accordance with the Inspector General Act of 1978, as amended, and the Quality Standards for Inspections, January 2005, issued by the President's Council on Integrity and Efficiency. We performed our fieldwork from February through April 2008.

APPENDIX B: REVIEWED PRIVACY IMPACT ASSESSMENTS

EDA

1. WebCIMS Correspondence Tracking System

NTIA

1. Coupon Program for Digital to Analog Converter Boxes

Office of the Secretary

1. ZyIndex Personnel Security System
2. Commerce Standard Acquisition Reporting System (CSTARS)/CBUY
3. Office of Security Management Application for Security (MAPS)
4. Automated Commerce Employment System
5. Homeland Security Presidential Directive 12 (HSPD12) Personal Identity Verification PART-1 (PIV-1)

NOAA

1. Crab Economic Data Report for Bering Sea/Aleutian Islands Management Areas off the Coast of Alaska (NMFS)
2. Permits and Registrations for Fisheries of the Exclusive Economic Zone off the Coast of Alaska (NMFS)
3. NOAA Vessel Monitoring System
4. NOAA Grants Online System
5. Marine and Aviation Operations Health Services Database
6. NOS Web Application Subsystem

Census

1. Center for Economic Studies
2. Field Support Systems
3. Geographic Support Systems
4. Longitudinal Employer Household Dynamic (LEHD) Program
5. Population Estimates
6. National Longitudinal Mortality Study (NLMS)
7. Survey of Business Owners

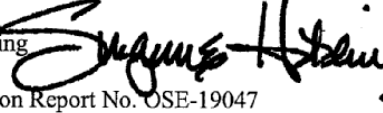
APPENDIX C: CHIEF INFORMATION OFFICER RESPONSE



UNITED STATES DEPARTMENT OF COMMERCE
Chief Information Officer
Washington, D.C. 20230

SEP 10 2008

MEMORANDUM FOR Judith J. Gordon
Assistant Inspector General for Audit and Evaluation

FROM: Suzanne Hilding 

SUBJECT: Draft Inspection Report No. OSE-19047

Thank you for your review of the Department's privacy impact assessment and Web privacy policy and processes. I concur with your draft report, *The Department's Privacy Impact Assessment Process Is Generally Implemented Well, But Some Improvements Are Needed*. My office will implement your recommendations.