UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF
INSPECTOR GENERAL

December 20, 2007

MEMORANDUM

SUBJECT: Supplemental Fiscal 2007 FISMA Audit Results – OIG Results of EPA's Efforts to Protect PII and Contractor Results of EPA Standard Configuration Documents' Compliance with Federal Guidance or Industry Best Practices
Assignment No: 2007-000802

FROM: Patricia H. Hill /s/
Assistant Inspector General for Mission Systems

TO: Molly O'Neill
Assistant Administrator for Environmental Information
and Chief Information Officer

This memorandum provides the results of the Office of Inspector General's review of Environmental Protection Agency (EPA) offices' compliance with Chief Information Officer (CIO) Policy Transmittal 06-11: *Interim Policy and Procedures for Protecting Personally Identifiable Information (PII)*. This memorandum also transmits Williams, Adley and Company, LLP, results regarding their review of EPA's standard configuration documents' compliance with Federal standards or industry best practices.

Personally Identifiable Information

During the Fiscal 2007 audit-planning meeting, the Deputy Chief Information Officer requested that the OIG conduct a review of EPA offices' compliance with procedures specified in CIO Policy Transmittal 06-11. The OIG conducted a limited review and interviewed numerous EPA officials responsible for overseeing and implementing the CIO policy at EPA Region 8 and the Office of Acquisition Management at Research Triangle Park, North Carolina. The OIG also interviewed EPA officials within the Office of Administration and Resources Management; Office of Water; Office of the Chief Financial Officer; and the Office of Enforcement and Compliance Assurance at EPA Headquarters, Washington DC.

Our results determined that the CIO should take more steps to increase overall awareness of the EPA officials' responsibilities for protecting PII. Although we visited six offices, variances of the noted occurrences were prevalent at each location. In particular:

.

- Offices permitted employees to collect and maintain PII files on EPA computers without obtaining prior written permission from the Senior Information Officer (SIO). One office allowed an employee to access PII remotely without authorization. Program officials indicated they were aware of the requirement to obtain prior approval, yet they did not complete and collect the approval forms as required by EPA policy.

- Offices had not developed and implemented local procedures for downloading PII nor were employees' laptops inspected to verify whether employees downloaded PII and if so, erased as required by the policy. Program officials indicated they had not developed procedures because the offices were awaiting additional CIO guidance.

We recommend the Chief Information Officer:

1. Issue a memorandum to Senior Information Officers reminding them of the Agency's policy requirements for protecting personally identifiable information and the need for the SIO to reiterate and reinforce compliance with the Agency policy within their offices.

2. Complete efforts to publish the Privacy Program procedures related to the Privacy Program policy issued on September 27, 2007.

EPA Standard Configuration Documents

During the Fiscal 2007 Federal Information Security Management Act (FISMA) audit, the OIG hired Williams, Adley and Company, LLP (WA&Co) to review a sample of EPA Standard Configuration Documents (SCDs) for compliance with standards established by the National Institute of Standards and Technology (NIST). If a NIST standard was not available for a reviewed SCD, we asked WA&Co to evaluate the SCD against known industry best practices. Due to the time constraints of the FISMA audit, we did not have WA&Co test EPA servers for compliance with the selected SCDs. However, the attached results provide your office with useful information regarding whether EPA system standards are consistent with Federal guidelines. We encourage the Office of Environmental Information (OEI) to incorporate methods for obtaining feedback on SCD implementation through using quarterly BindView and routine network vulnerability assessment tests. Attachment 1 contains WA&Co review results.

Action Required

Please provide a written response to the above recommendations within 30 days of the memorandum date. The response should indicate concurrence or nonconcurrence with each proposed recommendation. If you do not concur with a proposed recommendation, please provide any alternative actions you plan to take to address the recommendation. If you or your staff have questions, please contact me at (202) 566-0894 or Rudolph M. Brevard, Director, Information Resources Management Assessments, at (202) 566-0893, or brevard.rudy@epa.gov.

Review of Standard Configuration Documents

Performed By
Williams, Adley and Company, LLP (WA&Co)

The Environmental Protection Agency's (EPA's), Office of Inspector General hired Williams, Adley and Company, LLP (WA&Co) to evaluate EPA's standard configuration documents (SCDs) against National Institute of Standards and Technology (NIST) requirements, if available, or industry best practices. WA&Co noted that for all EPA SCDs selected for review, the SCDs content was consistent with a published authoritative document for securing the applicable operating system platform. However, WA&Co identified that EPA should take steps to update six of the reviewed SCDs. Based on interviews with EPA officials, WA&Co learned that EPA is revising five of the SCDs in question. The table below contains an overall summary of the SCDs reviewed. We removed the detailed test results due to the sensitivity of the security weaknesses discussed.

Table 1. Summary of Standard Configuration Document Review Performed By Williams, Adley and Company, LLP (Wa&Co)					
Standard Configuration Document Number	**Standard Configuration Document Name**	**NIST/Center for Internet Security (CIS)/Defense Information Systems Agency (DISA) Guidance**	**SCD Date**	**Number of Configurations Reviewed**	**Test Results ***
1	Microsoftware SQL Server 2000	CIS SQL 2005 Benchmark v1.0; Microsoft SQL 2k (April 6, 2007)	8/23/03	10	
2	Network File System	NA	7/19/03	NA	
3	AIX 5L	CIS AIX Benchmark v1.0.1 (October 19, 2005)	3/29/04	10	
4	Cisco Wireless LAN	CIS Wireless Benchmark v1.0; Wireless STIG v5r1 final20feb07 (February 20, 2007)	12/11/06	6	
5	Red Hat Linux 9 Server	CIS Red Hat Linux Benchmark v1.0.5 (June 26, 2007)	11/12/03	10	
6	Solaris 10	CIS Solaris 10 Benchmark v2.1.3 (June 26, 2007)	8/8/05	10	
7	SUSE Linux 10	CIS SUSE Linux Benchmark v1.0; (March 1, 2006)	3/2/06	10	

*** We removed the test result details due to the sensitivity of the security weaknesses discussed. The full details of these weaknesses are not available to the public.**

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

JAN 25 2008

OFFICE OF
ENVIRONMENTAL INFORMATION

MEMORANDUM

SUBJECT: OEI Response to Supplemental Fiscal 2007 FISMA Audit Results-OIG Results of EPA's Efforts to Protect PII and Contractor Results of EPA Standard Configuration Documents' Compliance with Federal Guidance or Industry Best Practices, Assignment No: 2007-000802, dated December 20, 2007

FROM: Molly A. O'Neill
Assistant Administrator and Chief Information Officer

TO: Patricia Hill
Assistant Inspector General for Mission Systems

Attached please find the Office of Environmental Information's response to the two recommendations included in the OIG review of Environmental Protection Agency (EPA) offices' compliance with Chief Information Officer (CIO) Policy Transmittal 06-11: "*Interim Policy and Procedures for Protecting Personally Identifiable Information (PII)*", dated December 20, 2007.

Any questions can be directed to Myra Galbreath, Director, Office of Technology Operations and Planning at 202-566-0300 or Marian Cody, Chief Information Security Officer, at 202-566-0302.

Attachment

cc: Myra Galbreath
Mark Luttner
Judy Hutt
Sara Hisel-McCoy
Robert Gunter
Cynthia Simbanin
Marian Cody
Johnny Davis
Rodney Bailey
Bob Trent

OEI Comments on Findings in: *Supplemental Fiscal 2007 FISMA Audit Results – OIG Results of EPA's Efforts to Protect PII and Contractor Results of EPA Standard Configuration Documents' Compliance with Federal Guidance or Industry Best Practices*

1. *Issue a memorandum to Senior Information Officials (SIOs) reminding them of the Agency's policy requirements for protecting personally identifiable information (PII) and the need for the SIOs to reiterate and reinforce compliance with the Agency policy within their offices.*

   OEI accepts the recommendations and will issue a memorandum to SIOs reminding them of their responsibilities to protect personally identifiable and ensure compliance with Agency privacy policies within organizations by February 15, 2008.

2. *Complete efforts to publish the Privacy Program procedures related to the Privacy Program policy issued on September 27, 2007.*

   The Privacy Program procedures will be presented to the Quality Information Council (QIC) for approval on January 27, 2008.