OFFICE OF THE INSPECTOR GENERAL

Catalyst for Improving the Environment

Audit Report

Security Configuration and Monitoring of EPA's Remote Access Methods Need Improvement

Report No. 2005-P-00011

March 22, 2005

Report Contributors: Rudolph Brevard
Teresa Richardson
Cheryl Reid
Vincent Campbell
William Coker

Abbreviations

EPA	Environmental Protection Agency
NTSD	National Technology Services Division
OIG	Office of Inspector General
OTOP	Office of Technology Operations and Planning

Cover Photo: A BlackBerry wireless handheld device (EPA OIG photo)

U.S. Environmental Protection Agency
Office of Inspector General

2005-P-00011
March 22, 2005

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

We sought to determine whether the Environmental Protection Agency's (EPA's) remote access methods, particularly through Web-Mail servers and BlackBerry servers and devices, have adequate controls to prevent abuse or unauthorized access to the Agency's information resources.

Background

Remote access is the connecting to EPA's data communications network from alternate locations not directly connected to the network. EPA establishes the security policy for the national data communications network and basic controls to ensure a secure infrastructure. Two key methods of attaining remote access are through an internet browser via Web-Mail or through a BlackBerry, which is a wireless handheld device.

For further information, contact our Office of Congressional and Public Liaison at (202) 566-2391.

To view the full report, click on the following link:

www.epa.gov/oig/reports/2005/20050322-2005-P-00011.pdf

Security Configuration and Monitoring of EPA's Remote Access Methods Need Improvement

What We Found

System administrators did not configure EPA's Web-Mail and BlackBerry servers to provide secure remote access to the Agency's network. We found that the system administrators did not configure or update 59 percent of the Web-Mail and BlackBerry servers to mitigate vulnerabilities. Consequently, confidentiality and integrity of EPA data, as well as the availability of the network, is at risk of unintentional or intentional exploitation. The weaknesses occurred because management did not implement processes to exercise proper oversight and provide detailed configuration settings.

We also found several of the Agency's BlackBerry devices were not adequately configured, secured, or monitored. We found devices that had no password enabled or had functionality that would allow users to disable passwords. We also observed devices left unattended in workstation cubicles. An unauthorized user of an unprotected handheld device has the potential to negatively affect the integrity and confidentiality of EPA information. These weaknesses occurred because management did not conduct a risk assessment or establish a process to consistently install BlackBerry devices.

What We Recommend

We made seven recommendations to the Director of EPA's Office of Technology Operations and Planning. They included establishing and requiring all remote access systems to have security monitoring and network vulnerability scanning; developing standards that define authorized open ports and services for the Web-Mail and BlackBerry servers' Operating System; and conducting a risk assessment and establishing a process to consistently configure devices. The Agency generally agreed with the recommendations and indicated corrective actions that, when implemented, would address the recommendations.

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

OFFICE OF
INSPECTOR GENERAL

March 22, 2005

MEMORANDUM

SUBJECT: Security Configuration and Monitoring of EPA's Remote Access Methods Need Improvement
Report No. 2005-P-00011

FROM: Eric Lewis /s/
Acting Director, Business Systems Audits (2421T)

TO: Kim T. Nelson
Assistant Administrator for Environmental Information
and Chief Information Officer (2810A)

This is our final report on the remote access methods audit conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). This audit report contains findings that describe problems the OIG has identified and corrective actions the OIG recommends. This audit report represents the opinion of the OIG, and the findings in this audit report do not necessarily represent the final EPA position. EPA managers in accordance with established EPA audit resolution procedures will make final determinations on matters in this audit report.

Action Required

In accordance with EPA Manual 2750, you are required to provide a written response within 90 calendar days of the date of this report. You should include a corrective action plan for agreed upon actions, including milestone dates. We have no objection to further release of this report to the public. For your convenience, this report will be available at http://www.epa.gov/oig.

If you or your staff has any questions regarding this report, please contact the Assignment Manager, Rudolph Brevard, at (202) 566-0893, or me at (202) 566-2708.

Table of Contents

Chapter 1
Introduction

Purpose

Our objective was to determine whether the Environmental Protection Agency's (EPA's) remote access methods provide adequate controls to prevent abuse or unauthorized access to the Agency's information resources. Specifically, we determined whether remote access points are effectively configured and adequately secured.

Background

EPA defines "remote access" as connection to the Agency's systems from an alternate location not directly connected to the network. EPA allows employees or contractors who have legitimate business requirements to connect remotely to systems. Additionally, EPA allows the public to connect to various data systems on its internal and public networks. To provide security, EPA implemented a robust network defense infrastructure, which includes intrusion detection systems, firewalls, and routers. These defenses, in general, provide adequate security to prevent intruders from exploiting the Agency's network.

The Office of Technology Operations and Planning (OTOP), within EPA's Office of Environmental Information, is responsible for establishing the Agency's policy for the national data communications network and basic controls to ensure a secure network infrastructure. OTOP's National Technology Services Division (NTSD) is responsible for managing EPA's network and for providing a capability to access systems remotely, as well as implementing the policies and standards for network security and publishing standards for remote access server configuration.

Configuration management of security controls over remote access servers is essential to mitigate disruption to business processes due to increased external connections. Based on a 2004 Office of Environmental Information survey, over 9,000 users connect to EPA's network using various methods of remote access. This many remote access connections increase the chances of intentional or unintentional exploitation of the Agency's network and the supporting servers.

Two key methods EPA uses to support remote access include:

- **Web-Mail,** which allows users to connect to their electronic mail accounts via an Internet browser.

- **BlackBerries,** which are wireless handheld devices that allow personnel to send, receive, and read electronic mail.

Scope and Methodology

We conducted our field work from June 2004 to December 2004 at EPA headquarters in Washington, DC; the National Computer Center, Research Triangle Park, North Carolina; and several regional offices. We interviewed Agency and contract personnel at various locations. We reviewed a variety of Federal and Agency criteria, summarized in Appendix A. This audit was conducted in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States.

To select the remote access methodologies to review, we conducted vulnerability testing to determine those methods with significant vulnerabilities, and determined there was a need to review the Web-Mail and BlackBerry methods. We did not review other methods that we determined had limited vulnerabilities or we recently reviewed.

We reviewed the configuration management and security controls surrounding the Web-Mail and BlackBerry servers and devices. We provided the vulnerability test results to NTSD, and management has implemented a process to mitigate all identified vulnerabilities.

Results in Brief

System administrators did not configure EPA's Web-Mail and BlackBerry servers to provide secure remote access to the Agency's network. Our vulnerability testing results identified that system administrators did not configure or update 59 percent of the servers to mitigate vulnerabilities. These weaknesses occurred because management had not implemented processes to exercise proper oversight or provide detailed configuration settings to secure remote access servers. As a result, the confidentiality and integrity of EPA's data and the availability of the network was at risk of unintentional or intentional exploitation. Also, the Agency did not consistently configure, secure or monitor several of the BlackBerry devices. Devices did not have passwords enabled or had functionality that would allow users to disable passwords. We also observed devices left unattended in workstation cubicles.

We made seven recommendations to EPA to correct deficiencies noted. EPA generally agreed with most of the recommendations in our report, but disagreed with the recommendations for conducting a formal risk assessment and establishing a security policy for the BlackBerry devices. Furthermore, the Agency suggested language changes and, in some cases, we modified the report. The Agency's comments and our evaluation are detailed in the following chapters. We included EPA's complete response as Appendix B.

Chapter 2
Protection of Web-Mail and BlackBerry Servers Needs Improvement

EPA did not appropriately configure its Web-Mail and BlackBerry servers to provide secure remote access to the Agency's network. We found that system administrators did not configure or update 59 percent of the Web-Mail and BlackBerry servers to mitigate vulnerabilities. Federal and EPA policy establish requirements for monitoring information resources and ensuring security is commensurate with risks. The weaknesses noted occurred because management did not implement processes to exercise proper oversight or provide detailed configuration settings to secure remote access servers. As such, confidentiality and integrity of EPA data, as well as the availability of the network, is at risk of unintentional or intentional exploitation; intruders could exploit the servers and attack systems inside and outside EPA.

Servers Not Configured to Provide Security

EPA did not adequately configure its Web-Mail and BlackBerry servers to provide security. Our vulnerability testing identified that 19 of the 32 servers, or 59 percent, were not: (1) configured with the proper security settings, or (2) updated with the latest security patches and/or necessary updates to protect them from actual and potential threats. In particular, we identified 56 high and medium risk vulnerabilities on EPA's Web-Mail and BlackBerry servers related to unapplied patches and/or upgrades. High and medium risk vulnerabilities can enable an intruder to: (1) access restricted data, (2) browse the remote web server for account information, and (3) exploit a program with known weaknesses to gain control of the system.

Oversight Processes Needed for Remote Access Servers

EPA has not implemented processes to exercise oversight over the Web-Mail and BlackBerry remote access servers. EPA Order 2195.1 A4, *Agency Network Security Policy*, establishes the overall requirement for oversight and monitoring of information and computing resources. We found EPA has not assigned responsibility for implementing processes to independently verify and validate that these servers comply with Agency policies and standards. NTSD has established an E-mail platform manager position, responsible for developing system standards, policies, and procedures for the Agency's electronic mail methods, which include Web-Mail and BlackBerry. However, the platform manager is not involved in: (1) establishing new servers, or (2) approving servers' access through the Agency's firewall. Although NTSD conducts monthly security reviews of the servers, the platform manager reviews reports for selected

centrally managed Web-Mail and BlackBerry servers only and relies on program and regional offices to provide oversight on distributed servers.

EPA has not implemented a comprehensive security-monitoring program that includes all remote access servers. NTSD has implemented a monthly security-monitoring program to evaluate server's compliance with EPA's standards and forwards the results to senior Agency officials. These results report NTSD's monthly security status as "Green," but only 18 percent of the servers (7 of 38) are included in this assessment. Further, security monitoring occurs on a voluntary basis and managers are not required to participate in the program.

EPA's security monitoring software is not effective in discovering all vulnerabilities. EPA uses a commercial-off-the-shelf software program to monitor servers for compliance with NTSD standards and common security configuration practices. This software does not scan for computer security industry-identified threats. Our vulnerability scanning results indicated that three of the five servers monitored by the Agency contained at least one "high-risk" vulnerability. Further, interviews with several System Administrators disclosed that they do not perform the regular scanning required by Agency policy.

Detailed Configuration Parameters Needed

We noted 190 instances where servers transmitted low level, but sensitive, information regarding: (1) server configuration, (2) possible entry points available on the server, and (3) Operating System-specific information that should not be available to users. NTSD published the Standard Configuration Document, which defines the *minimum* configuration and security requirements for single purpose servers and requires system administrators to open only authorized ports and services necessary for operation. However, NTSD has not defined which ports and services that system administrators should open. A port is a logical connection place dedicated to a specific software program, while a service is a software program assigned a designated port. For example, an Internet Browser, a service, uses port 80 to communicate with servers to retrieve web-site information.

Recommendations

We recommend that the Director, Office of Technology Operations and Planning:

2-1 Establish processes and assign accountability for independently verify and validate that Web-Mail and BlackBerry servers comply with published EPA policies and standards.

2-2 Develop and implement a security-monitoring program that includes testing all servers, and require all system administrators to register their servers with NTSD and participate in the security-monitoring program.

2-3 Expand the Agency's security-monitoring program to include using a variety of network vulnerability scanning tools to monitor registered servers.

2-4 Establish and implement a process to ensure program and regional offices conduct regular security monitoring that includes vulnerability scanning.

2-5 Develop and publish standards that define authorized open ports and services for the Web-Mail and BlackBerry servers' Operating System.

Agency Comments and OIG Evaluation

OTOP's Director for Technical Information Security Staff concurred with our recommendations. We are encouraged that OTOP plans a proactive approach to improve its compliance oversight and vulnerability management capabilities. In addition, OTOP indicated that it is expanding its monitoring oversight to include other Agency-supported platforms. In our view, the corrective actions planned are appropriate and, when fully implemented, will adequately address the recommendations. Furthermore, in the response, the Agency suggested revised wording and we modified the report accordingly.

Chapter 3
BlackBerry Devices Need Improved Security Controls

Several of EPA's BlackBerry devices were not adequately configured, secured, or monitored. Specifically, we found devices that had no password enabled or had functionality that would allow users to disable passwords. We also observed devices left unattended in workstation cubicles. Further, EPA did not monitor the level of sensitivity for information transmitted or stored on BlackBerry devices. These weaknesses occurred because management did not conduct and document a risk-based assessment, or establish a process to ensure consistent configuration of BlackBerry devices. As such, an unauthorized user of an unprotected device could negatively affect the integrity and confidentiality of EPA information.

BlackBerry Devices' Password Settings, Physical Security, and Monitoring Not Adequate

BlackBerry devices did not have required password settings to secure them from unauthorized use. EPA published the BlackBerry Standard Configuration Document to give program and regional offices a consistent method to configure BlackBerry devices. We selected a random sample of headquarters users located within five program offices and checked implemented password configurations. However, we found that four of the nine devices did not have a password enabled, or had functionality that would allow users to disable passwords.

During our office area review and interviews with Agency officials, we noted several security concerns regarding BlackBerry devices. We observed devices left unattended in workstation cubicles, which subjected the devices to theft and EPA data to compromise. EPA also had not determined the level of sensitivity for information transmitted or stored on the devices, nor did the Agency analyze or monitor the data records to determine whether users transmitted sensitive information. Although the National Institute of Standards and Technology published guidelines that agencies can use to secure their wireless devices, we noticed many of these practices were not in place. The small size and mobility of BlackBerry devices make them more likely to be stolen, misplaced, or lost. As a result, these small and mobile devices are vulnerable to theft and subsequent misuse by a potential intruder.

EPA Has Not Conducted a Risk Assessment for BlackBerry Devices

EPA did not identify strategies to mitigate potential risks and threats that BlackBerry use posed for the EPA computing environment. Specifically, NTSD did not conduct and document a risk assessment before allowing the Agency to introduce the devices into the EPA computing environment. Our interviews

disclosed instances where NTSD needed improved managerial controls to protect the computing environment. For example, if an existing user requests a transfer of their BlackBerry account to a new device, management could not tell if the old device had been lost (or stolen), broken, or simply retired because the inventory records do not capture that information. Therefore, EPA does not know whether unauthorized persons have access to those BlackBerry devices and whether those devices contain sensitive data. Additionally, EPA had not established a process to ensure consistent configuration of BlackBerry devices. For the program offices reviewed, the Agency's BlackBerry Standard Configuration Document was not used to install these devices.

Recommendations

We recommend that the Director, Office of Technology Operations and Planning:

3-1 Conduct and document a risk assessment using a risk-based approach that includes accessing a device's password and disabling function, physical security, and data sensitivity, and implement corrective and/or mitigative control procedures.

3-2 Establish a procedure to ensure program offices use the BlackBerry Standard Configuration Document to configure all devices. Specifically, this procedure should address validating installation requirements of a device's security settings and users' security responsibilities. The procedure should also address the handling of lost, stolen, and discarded devices.

Agency Comments and OIG Evaluation

OTOP did not agree with our recommendation to conduct a formal risk assessment of the BlackBerry computing environment, asserting that a formal assessment would not be cost effective and produce additional findings beyond those already known. We subsequently held an Exit Conference to discuss this issue with the Agency. We expressed our agreement that the Agency should use a cost effective risk assessment methodology to make the most efficient use of its resources. We reiterated our concerns that the Agency had not conducted a risk assessment and that it should document the security controls surrounding the BlackBerry computing environment to give management better information to: (1) secure its systems, (2) justify expenditures as part of the budget process, and (3) assist in authorizing the system for operations. OTOP concurred with our approach and we modified the report and recommendations to clarify our position.

In addition, OTOP did not concur with our recommendation that the Agency establish a security policy for the BlackBerry. OTOP believes such polices already exist within the framework of the Agency's Network Security Policy. The OIG agrees that sufficient policy exists. However, we believe the Agency

should give clearer guidance to the program and regions offices regarding configuration requirements and users' security responsibilities. We modified the report and recommendations to clarify our position.

Appendix A

Federal and Agency Criteria

The Clinger - Cohen Act states that the Chief Information Officer has primary responsibility for monitoring the Agency's information technology program performance, through monitoring and evaluation against the Agency's applicable performance measurements.

The E-Government Act provides a comprehensive framework for ensuring the effectiveness of information system security controls, and provides a mechanism for improved oversight of Federal agency information security programs. The Act directs the head of each Federal agency to provide information security protection commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information.

National Institute of Standards and Technology (NIST) Special Publication 800-48, Wireless Network Security: 802.11, Bluetooth and Handheld Devices, states that Information Security Officers and Network Administrators should conduct a risk assessment before handheld devices are introduced into the Agency's computing environment. Moreover, network administrators should establish and document security policies that address their use and the users' responsibilities. The policy document should include proper password selection and use. Handheld devices should have security settings that comply with the Agency's security policy prior to distribution.

EPA Order 2195.1 A4, Agency Network Security Policy, requires network security to be managed as a mission-critical activity in accordance with risk management principles. The policy requires oversight monitoring to be conducted for potential and actual threats to the network and Agency information and computing resources. Systems attached to the network must be certified as compliant with the standards and/or procedures outlined in the policy. It also requires that general support systems and/or major application managers conduct and update risk assessments at least every 3 years or whenever a substantive configuration change occurs. Configurations and settings of network-attached resources must (1) be tested by the responsible information system manager prior to implementation; (2) be documented; and (3) conform to Deputy Chief Information Officer for Technology approved procedures and standard configurations based on user business requirements, published security vulnerabilities, and best industry security practices. The policy requires EPA data communications network resources be documented, monitored, tested, evaluated, and verified to ensure adequate security in accordance with information sensitivity and other Federal and Agency requirements.

EPA's Operating System Standard Configuration Document requires all servers connected to the EPA network to be monitored for security compliance and vulnerabilities. The standard requires all servers connected to any part of the network to comply with this document. Furthermore, it requires system administrators to only open ports required for operation.

EPA's BlackBerry Standard Configuration Document states that several default settings must be set up on each BlackBerry handheld device used at EPA. The document sets defaults for desktop and BlackBerry synchronization and ensures that the device's configuration complies with EPA security policies. The document requires program and regional offices to enable passwords and to remove the option that would allow users the ability to disable password security.

Appendix B

Agency Response to Draft Report

March 14, 2005

MEMORANDUM

SUBJECT: OEI Response to Draft Audit Report: "Security Configuration and Monitoring of EPA's Remote Access Methods Needs Improvement" Assignment No. 2004-000739

FROM: George Bonina /s/
Senior Agency Information Security Officer and
Director, Technical Information Security Staff
Office of Technology Operations and Planning (2831T)

TO: Eric Lewis, Acting Director
Business Systems
Office of Inspector General (2421T)

Thank you for the opportunity to review and comment on this draft report. Mark Day has delegated to me the responsibility for responding to the audit.

This audit highlighted areas where OEI can improve administration of the Agency's remote access methods. We offer the following comments on the draft report:

- OTOP is aggressively improving its Agency-wide network compliance monitoring and vulnerability management capabilities. For compliance monitoring, OTOP is deploying the Bindview tool as EPA's compliance management standard and expanding management scorecards to include all major platforms. For vulnerability management, OTOP is in the final stages of identifying a vulnerability management standard and selecting a tool. For patch management, OTOP is completing Agency-wide implementation of PatchLink.

  These tools will provide Agency system managers with the ability to better-manage their network-attached devices, as well as provide OTOP with independent oversight capability. These tools will address most of the findings and recommendations identified in the report.

- OTOP is responsible for monitoring Agency-wide compliance with standards. OTOP currently monitors Netware Agency-wide and is adding other platforms. As our security program matures we are extending our Agency-wide monitoring oversight to all platforms.

- The stated findings indicate that the E-mail platform manager does not review monthly security reports. This finding should more accurately state that the E-mail platform manager does currently review monthly compliance reports for all centrally-managed webmail servers

only and relies on system administrators and information security officers in programs and regions for oversight of distributed webmail servers.

- Mobile devices present a risk challenge. However, mobile devices remain a vital component of EPA's daily business. User surveys within EPA senior executive ranks report significant conversion of idle time to productive time when managing their email workload through mobile devices. The majority of senior executives report improved ability to respond to time sensitive messages when equipped with mobile devices. EPA has consciously accepted the risks, in light of the substantial returns in business opportunities.

- The BlackBerry Standard Configuration Document (SCD) sets defaults for desktop and handheld configurations in accordance with Agency policies and standards. Password enablement is among the default settings. While OTOP agrees that the inability to enforce passwords for mobile devices presents a risk, there currently is no automated means for detecting the absence of password enablement and locking of Blackberry handheld, or enforcing other standard configuration requirements. Future versions of Blackberry operating systems may implement such a capability.

- OTOP does not agree with the recommendation that it conduct a formal risk assessment of BlackBerry devices. OTOP does not believe a formal risk assessment targeting mobile devices will produce additional vulnerabilities and findings beyond those already known and understood. The technology is evolving to provide effective countermeasures to mobile device threats. Instead of investing in additional risk assessments, OTOP believes a more effective use of resources is to identify and test mitigation measures for known risks such as password enforcement.

- The Agency Network Security Policy requires that all devices connected to the network must conform to approved standards. Therefore a formal policy does exist. The issues raised in the audit are more related to the adequacy of approved standards and the ability to enforce standards on mobile devices, rather than whether there is a policy requiring compliance with standards.

We appreciate the efforts of your staff in conducting this audit and the opportunity to work together to improve the security of the Agency's IT assets. Please feel free to contact me at 202-566-0304 or via email if you have any questions.

cc: Mark Day
Melissa Heist
Myra Galbreath
Robin Gonzalez
Bill Boone
John Gibson
Kim Farmer
Karen Maher
Rudy Brevard
Teresa Richardson

Appendix C

Distribution

Office of the Administrator (1101A)
Assistant Administrator for Environmental Information (2810A)
Director, Office of Technology Operations and Planning (2831T)
Director, National Technology Services Division (N229-01)
Director, Technical Information Security Staff (TISS) (2831T)
Chief of Security, National Technology Services Division (N276-01)
Audit Coordinator, Office of Environmental Information (OEI) (2812T)
Audit Coordinator, Technical Information Security Staff (2831T)
Agency Followup Official (the CFO) (2710A)
Agency Followup Coordinator (2724A)
General Counsel (4010A)
Associate Administrator for Congressional and Intergovernmental Relations (1301A)
Associate Administrator for Public Affairs (1701A)
Inspector General (2410)