OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Audit Report

EPA Could Improve Processes for Managing Contractor Systems and Reporting Incidents

Report No. 2007-P-00007

January 11, 2007

Report Contributors: Rudolph M. Brevard
Neven Morcos
William Coker
Warren Brooks

Abbreviations

ASSERT	Automated Security Self Evaluation and Remediation Tracking
CSIRC	Computer Security Incident Response Capability
EPA	U.S. Environmental Protection Agency
EPAAR	Environmental Protection Agency Acquisition Regulation
FISMA	Federal Information Security Management Act
IRM	Information Resource Management
ISO	Information Security Officer
OEI	Office of Environmental Information
OIG	Office of Inspector General

U.S. Environmental Protection Agency
Office of Inspector General

2007-P-00007
January 11, 2007

At a Glance

Catalyst for Improving the Environment

Why We Did This Audit

We sought to determine whether the U.S. Environmental Protection Agency (EPA) defined security requirements for contractor-owned systems that collect data for EPA. We also sought to determine whether EPA offices identified and reported all computer security-related incidents to EPA's Computer Security Incident Response Capability (CSIRC) staff.

Background

EPA uses contractors to collect and process information on its behalf. Annually, the contractors review their systems' compliance with established information security requirements and record the results in EPA's security monitoring database. CSIRC defines the formal process by which EPA responds to computer security-related incidents such as computer viruses, unauthorized user activity, and serious software vulnerabilities.

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/2007/20070111-2007-P-00007.pdf

EPA Could Improve Processes for Managing Contractor Systems and Reporting Incidents

What We Found

Although EPA had defined the specific requirements for contractor systems, EPA had not established procedures to ensure identification of all contractor systems. Furthermore, EPA had not ensured that information security requirements were accessible by the contractors and appropriately maintained. As a result, EPA system inventories may not include all appropriate contractor systems, and its contractors may not be implementing adequate security safeguards.

Although EPA offices were aware of the Agency's computer security incident response policy, many offices lacked local reporting procedures, had not fully implemented automated monitoring tools, and did not provide sufficient training on local procedures. EPA offices also did not have access to network attack trend information necessary to implement proactive defensive measures. As a result, there was no consistency in how, what, and when EPA offices reported computer security incidents. Without all relevant security incident data, EPA may not accurately inform senior Agency officials regarding the performance and security of the Agency's network.

What We Recommend

To address weaknesses associated with contractor systems, we recommend that EPA assign duties and responsibilities for maintaining and updating information posted on EPA's Website. We also recommend that EPA update its guidance for identifying contractor systems. Further, we recommend that EPA establish formal procedures to ensure that all responsible program offices update and maintain their EPA-specific contract clauses on a regular basis.

To address the computer security incident reporting weaknesses, we recommend that EPA update the Agency's computer security incident guide to cover reporting instructions for all locations, establish a target date for when it will configure the Agency's anti-virus software to utilize the central reporting feature, train Information Security Officers on new procedures, and provide Information Security Officers with computer security incident reports.

The Agency generally agreed with our recommendations. In many cases, management provided milestone dates and planned actions to address the report's findings. The Agency's complete response is included at Appendices A and B.

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

OFFICE OF
INSPECTOR GENERAL

January 11, 2007

MEMORANDUM

SUBJECT: EPA Could Improve Processes for Managing Contractor Systems and Reporting Incidents
Report No. 2007-P-00007

TO: Molly A. O'Neill
Assistant Administrator
Office of Environmental Information

Luis Luna
Assistant Administrator
Office of Administration and Resources Management

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

The estimated cost of this report – calculated by multiplying the project's staff days by the applicable daily full cost billing rates in effect at the time – is $466,534.

Action Required

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

If you or your staff have any questions regarding this report, please contact Rudolph M. Brevard, Director for Information Resources Management Assessments, at (202) 566-0893 or brevard.rudy@epa.gov.

Sincerely,

Bill A. Roderick
Acting Inspector General

Table of Contents

Chapters

Appendices

Chapter 1
Introduction

Purpose

Our overall objective was to evaluate the implementation and effectiveness of the U.S. Environmental Protection Agency's (EPA's) information security practices. We reviewed EPA's processes for managing contractor systems and handling computer security incidents. Specifically, we sought to identify to what extent EPA has defined security requirements for contractor-owned systems that collect data on EPA's behalf.[1] We also sought to determine whether EPA program and regional offices identified and reported all computer security-related incidents to EPA's Computer Security Incident Response Capability (CSIRC) staff.

Background

We performed this audit pursuant to the Federal Information Security Management Act (FISMA) of 2002. FISMA establishes a framework for ensuring the effectiveness of EPA's information security programs. FISMA requires EPA to implement policies and procedures commensurate with the risk and magnitude of harm resulting from the malicious or unintentional impairment of Agency information assets.

Contractor Systems

EPA uses a variety of contractor support services to operate its information technology resources. This includes contractors who operate EPA-owned systems that reside in Government facilities. This also includes contractors who own and operate systems that collect and process information on EPA's behalf. To monitor the contractors' systems' compliance with established information security requirements, EPA requires its contractors to complete an annual self-assessment for their systems. The self-assessment is intended to identify system weaknesses and create plans to remediate them. This self-assessment is consistent with guidance published by the National Institute of Standards and Technology.

EPA's Office of Environmental Information (OEI) is responsible for establishing the framework in which EPA offices oversee the annual self-assessment. EPA offices are responsible for ensuring that all of their contractor systems are identified and the self-assessments are completed. EPA offices record the self-assessment information in a central database, called the Automated Security Self Evaluation and Remediation Tracking (ASSERT) database. EPA uses ASSERT

[1] Throughout this report, we refer to contractor-owned systems with EPA data as *"contractor systems."*

to report the status of its information security program to the Office of Management and Budget (OMB). Therefore, it is essential that all contractor systems are identified and results recorded in ASSERT.

The Office of Acquisition Management is responsible for overseeing EPA's contracting processes. This includes establishing a process to ensure that EPA Acquisition Regulation (EPAAR) clauses are updated. EPA offices are responsible for updating their offices' EPAAR clause. EPA offices are also responsible for ensuring information referenced in EPAAR clauses is current. OEI informs contractors about EPA-specific information system security requirements through an EPAAR clause. The EPAAR directs contractors to an EPA Website that contains applicable Agency security requirements. As such, it is vital that the information be accurate and accessible so EPA contractors can implement the necessary controls to protect the data processed on EPA's behalf.

Incident Reporting

EPA's CSIRC staff manages the computer security incident reporting process. CSIRC defines the formal process by which EPA responds to computer security-related incidents such as computer viruses, unauthorized user activity, and serious software vulnerabilities. CSIRC facilitates the centralized reporting of incidents and provides support to help EPA Information Security Officers (ISOs). OMB and the National Institute of Standards and Technology provide guidelines for the sharing and timely reporting of computer security incidents. Other Federal guidance requires organizations to provide personnel with initial and annual refresher training on computer security. This training includes training personnel on computer security incident handling.

EPA developed the following policies to guide the Agency's computer security incident reporting processes:

- **EPA Order 2195.1 A4** - Directs that the ISO is the primary point of contact for all security incidents. In addition, it directs the ISO to document and retain records of computer security incidents.

- **EPA Directive 200.06** - Provides the framework for EPA's computer security incident reporting program. It requires the ISO to develop, maintain, and publish local computer security incidents procedures.

- **The ISO Handbook** - Directs EPA personnel to follow local procedures to report computer security incidents.

Scope and Methodology

We performed our audit in accordance with *Government Auditing Standards,* issued by the Comptroller General of the United States. We conducted field work

from March 2006 until June 2006. We conducted site visits in EPA Regions 1, 2, and 3. We also conducted teleconferences with EPA Regions 5 and 8 and held meetings with representatives from EPA's Office of Water and Office of Air and Radiation, located in Washington, DC.

We conducted a survey to obtain preliminary information on program and regional offices' processes regarding contractor systems and computer security incident reporting. To obtain an understanding of EPA's management control processes for contractor systems and computer security incident reporting, we collected documentation, interviewed personnel, and reviewed EPA's implementation of management controls over these two areas. EPA has not conducted management reviews of its processes to identify contractor systems. EPA had conducted a review of its incident handling processes and we collected and analyzed management's evaluation of its processes. We collected information on the number of contractor systems, establishment of incident handling procedures, and the number of incidents reported to the Agency's central incident collection center.

We spoke with representatives from OEI, responsible for overseeing the Agency's information security processes, and EPA's Office of Acquisition Management within the Office of Administration and Resources Management, responsible for overseeing the Agency's acquisition processes. We also spoke with EPA contractors and employees responsible for monitoring EPA's contractor systems and following EPA's computer security incident reporting policies and procedures.

We conducted a survey with all EPA offices and did the following analyses:

- **To identify contractor systems** - We developed a definition of contractor systems with the assistance of OEI. The definition contained elements that described contractor-owned systems, located outside of a Government facility, used to collect information on EPA's behalf. We collected information regarding whether the location categorized the sensitivity of the data. We collected and reviewed contractor oversight policies and procedures. We conducted followup interviews with respective offices and research within EPA's intranet to validate the survey results.

- **To select locations to visit regarding computer security incidents -** Each location provided us the number of computer security incidents that occurred from September 1, 2005, through February 14, 2006. We compared the results to a CSIRC report that identified the number of computer security incidents each location reported to CSIRC for the same period. We used the information to select a judgmental sample of 14 locations. The sample included locations whose results matched the CSIRC report and those that did not. We conducted site visits and telephone conferences with the selected locations. We met with the site's

primary ISO, helpdesk personnel, network managers, and EPA employees and contractors.

- **To determine whether a location complied with EPA's incident reporting procedures -** We considered the site compliant with EPA's policy if the location formally documented the procedures in either a policy document or the location's security plan.

There were no significant audits or recommendations to follow up on during this audit.

Chapter 2
EPA Could Improve Processes for Managing Contractor Systems

EPA could improve its practices for managing contractor compliance with Federal and EPA system security requirements. EPA established the ASSERT database to track EPA systems, their security weaknesses, and the status of remediation plans. However, EPA did not define how EPA offices should identify contractor systems or ensure these systems' vulnerabilities were consistently tracked through ASSERT. In addition, EPA had not established processes for maintaining its EPA-specific contract clauses and Information Resources Management (IRM) requirements. As a result, EPA had not identified all of its contractor systems. Additionally, EPA has no assurance that its contractors identified their systems' vulnerabilities and implemented appropriate security controls, or that they were promptly informed of their contractual obligations when EPA-specific information security requirements changed.

Additional Guidance Needed for Identifying Contractor Systems

EPA's method for identifying contractor systems does not consider the type and sensitivity of the data needing protection. Instead, EPA's current guidance for identifying contractor systems only considers whether a contractor system is co-located at an EPA facility or connected to EPA's network infrastructure. Since some contractor systems do not reside at an EPA location or connect to EPA's network, offices did not identify these systems for routine assessment of security controls. As a result, EPA offices do not know whether the contractors are knowledgeable of Agency-specific information security requirements or whether the contractor applied the security controls necessary to protect the data it collects on EPA's behalf.

We developed a *"limited"* definition of contractor systems that contained EPA data. We included this definition in a survey sent to all EPA offices. All EPA office responded to our survey. The results identified four additional contractor systems that were not included in ASSERT. We provided the results to OEI and the office took immediate action to recognize the systems in the Agency's system inventory.

Procedures Needed for Updating EPA-Specific Contract Clauses

The Office of Acquisition Management (OAM) had not established formal procedures to ensure responsible EPA offices regularly review and update their EPA-specific contract clauses (EPAAR clause). Instead, OAM uses an informal

process to notify offices when to update their clause. The informal approach creates a security risk because contractors may not receive timely guidance and instructions about new security requirements. For instance, we discovered the existing EPAAR clause on information security directed contractors to an inoperable EPA Website. As a result, contractors did not have access to the latest guidance for system security requirements. Upon bringing this weakness to the Agency's attention, EPA took immediate action to activate the Website.

Processes Needed for Maintaining IRM Requirements

Although OEI chartered a workgroup to maintain IRM policies, OEI has not formally assigned duties and responsibilities for maintaining the policy guidance. Further, OEI has not developed and implemented a process to ensure that IRM policy posted for contractor use is current, accurate, and complete. Without up-to-date policy, contractors cannot adhere to the latest security requirements. While OEI has made progress in implementing processes to manage the IRM Website content, OEI personnel agreed that further progress is needed to fulfill its responsibilities.

Recommendations

We recommend that the Assistant Administrator for Environmental Information:

2-1 Develop and implement guidance that EPA offices can use to identify contractor systems that contain EPA data.

2-2 Assign duties and responsibilities to internal offices for maintaining the IRM requirements posted on the EPA Website available to contractors.

We recommend that the Assistant Administrator for Administration and Resources Management, through its Office of Acquisition Management:

2-3 Establish formal procedures to ensure all responsible program offices update and maintain applicable EPA-specific contract clauses on a regular basis.

Agency Comments and OIG Evaluation

The Agency concurred with the findings and provided descriptions of planned actions, including milestone dates, for addressing the recommendations.

Chapter 3
EPA Could Improve Its Incident Reporting Processes

Although EPA locations were aware of the Agency's computer security incident reporting process, not all locations reported computer security incidents to the Agency's CSIRC staff in a timely manner. This occurred because:

- EPA offices lacked local procedures for reporting incidents,
- EPA had not fully implemented automated tools to monitor Agency network resources for security incidents,
- EPA did not provide sufficient training to its employees on their responsibilities and local procedures, and
- EPA did not share information on network attack trends.

As a result, EPA offices are not consistent in what, when, and how they report security incidents to CSIRC. EPA needs to consider all relevant security incident data to assess vulnerabilities, identify attack trends, and contain security threats. Without all relevant security incident data, CSIRC personnel cannot promptly respond to and contain security threats before they potentially affect wider portions of the Agency's network.

EPA Locations Need Local Incident Reporting Procedures

Although required by EPA Directive 200.06, *Computer Security Incident Response*, only 29 percent (4 of 14) of the sampled locations developed local incident handling procedures. Our fieldwork identified several weaknesses that contribute to sites inconsistently reporting security incidents within their locations and subsequently to the CSIRC. For example:

- Although some sites established informal procedures for reporting incidents, we found that the sites did not always follow these processes and did not keep records of incidents.

- Several sites did not create local procedures because EPA's policy did not provide enough guidance to assist them in developing procedures. The sites also indicated that they needed additional assistance from the Agency to improve their processes.

- One office with eight geographically dispersed offices under its purview did not have standardized procedures to identify and report computer security incidents.

- Two offices indicated that users often contacted the local system administrator or ISO directly for faster assistance. In doing so, these

offices bypassed the established call centers responsible for receiving reports about potential computer problems. We found that when the call center is by-passed, the ISO might not contact the call center to ensure a record was kept of the incident.

Without local procedures for reporting computer security incidents, CSIRC and EPA may not have all the information necessary to adequately protect information assets and respond to actual and potential incidents.

EPA Had Not Fully Implemented Its Centralized Monitoring Software

EPA's Office of Technology Operations and Planning specified that all Agency locations must configure their anti-virus software to utilize the centralized monitoring feature. During our fieldwork, several locations had not yet configured their anti-virus software to use the feature. The centralized monitoring feature allows all recognized instances of computer security attacks to be reported and collected at one location for analysis. However, EPA's CSIRC does not have the capability to determine which locations have properly configured their software for centralized monitoring.

Further, EPA did not maximize the use of its centralized monitoring software because it did not establish a deadline for locations to upgrade to the latest version of anti-virus software. EPA approved several versions of the anti-virus software for use within the Agency. By utilizing the latest version, the CSIRC would have more readily available information about the different types of computer attacks across the Agency. EPA allows each location to implement the software upgrade because each location maintains its own desktop support. However, EPA does not monitor how quickly the software upgrade occurs. The current situation compromises the effectiveness of EPA's computer security incident capability, as well as the Agency's ability to control the availability and integrity of its network.

EPA Employees Need Training on Local Reporting of Incidents

Most locations rely on the Agency's annual security awareness training to inform employees about reporting computer security incidents. Our review disclosed that EPA's annual security awareness training lacked specific local training procedures. While the training provided general information regarding how to recognize a computer security attack, the training did not provide information on how and where to report these security incidents and what information should be reported. Additionally, the training was inconsistent about whom an employee should contact. For instance, one section of the training program informs the employee to report threats to the immediate supervisor; yet, in another section, the training instructs the employee to notify local computer security personnel. Subsequent to audit fieldwork, EPA implemented new annual security awareness training. However, the training is not specific enough to prescribe how computer security incident reporting should take place locally.

Incident Trend Reports Not Provided to Information Security Officers

Although CSIRC distributes weekly management and quarterly trend analysis reports to EPA's Office of Technology Operations and Planning, CSIRC does not share this information with the local ISOs. The reports reflect all computer security activity across the EPA network. During fieldwork, several ISOs indicated that these reports would assist them in proactively monitoring their networks and implementing risk mitigation practices. Further, sharing information with all individuals involved with protecting network resources strengthens EPA's proactive and agile computer security response capability. With trend information, network managers can implement security measures that could ultimately reduce the number of successful attacks on EPA's network.

Recommendations

We recommend that the Assistant Administrator for Environmental Information, through its Office of Technology Operations and Planning:

3-1 Collect and analyze the Agency's local computer security incident reporting procedures to ensure compliance with established Agency policies. If necessary, update the CSIRC guidance accordingly.

3-2 Establish a target date when all EPA locations will implement the latest anti-virus software and configure the software to use centralized monitoring.

3-3 Develop and implement a strategy to train ISOs on any updates to the CSIRC guide.

3-4 Provide local ISOs and responsible information technology personnel with trend analysis reports on computer security incidents.

Agency Comments and OIG Evaluation

EPA generally agreed with the report's findings. OEI disagreed with our recommendation to update the CSIRC guidance because management felt the guide provides detailed information on proper reporting, prioritization, and escalation of security incidents. Although the CSIRC guide provides detailed information, the guide does not provide the specificity needed to address local operating needs. Given the high number of locations without local computer security incident reporting procedures, EPA should conduct an analysis of the Agency's local incident reporting practices to identify instances where the Agency could improve its incident reporting processes and, if necessary, update the CSIRC guidance accordingly. We modified the recommendation accordingly.

OEI indicated that it could not corroborate evidence that the ISO community lack an understanding of the Agency's incident reporting policies. Although EPA locations were aware of the Agency's incident reporting policies, our site visits and interviews determined that many of the locations did not institute management control processes to enforce the Agency's policies. As such, several weaknesses existed that contributed to sites inconsistently reporting security incidents within their locations and subsequently to the CSIRC. OEI also indicated the report misstated the CSIRC's responsibilities for deploying and following up on the anti-virus software implementation. We modified the report to address the Agency's concerns.

Status of Recommendations and Potential Monetary Benefits

RECOMMENDATIONS						POTENTIAL MONETARY BENEFITS (in $000s)	
Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Claimed Amount	Agreed To Amount
2-1	6	Develop and implement guidance that EPA offices can use to identify appropriate contractor systems that contain EPA data.	O	Assistant Administrator for Environmental Information	9/18/08	0	
2-2	6	Assign duties and responsibilities to internal offices for maintaining the IRM requirements posted on the EPA Website available to contractors.	O	Assistant Administrator for Environmental Information	TBD	0	
2-3	6	Establish formal procedures to ensure all responsible program offices update and maintain applicable EPA-specific contract clauses on a regular basis.	O	Assistant Administrator for Administration and Resources Management/Office of Acquisition Management	3rd Quarter Fiscal Year 2007	0	
3-1	9	Collect and analyze the Agency's local computer security incident reporting procedures to ensure compliance with established Agency policies. If necessary, update the CSIRC guidance accordingly.	U	Assistant Administrator for Environmental Information/ Office of Technology Operations and Planning		0	
3-2	9	Establish a target date when all EPA locations will implement the latest anti-virus software and configure the software to use centralized monitoring.	O	Assistant Administrator for Environmental Information/ Office of Technology Operations and Planning	2/27/07	0	
3-3	9	Develop and implement a strategy to train ISOs on any updates to the CSIRC guide.	O	Assistant Administrator for Environmental Information Office of Technology Operations and Planning	TBD	0	
3-4	9	Provide local ISOs and responsible information technology personnel with trend analysis reports on computer security incidents.	O	Assistant Administrator for Environmental Information/ Office of Technology Operations and Planning	TBD	0	

[1] O = recommendation is open with agreed-to corrective actions pending
C = recommendation is closed with all agreed-to actions completed
U = recommendation is undecided with resolution efforts in progress

Appendix A

Office of Environmental Information Response to Draft Report

November 30, 2006

MEMORANDUM

SUBJECT: OEI Response to the Draft Audit Report: EPA Could Improve Processes for Managing Contractor Systems and Reporting Incidents, Assignment No. 2006-000068

FROM: Linda A. Travers
Acting Assistant Administrator and Chief Information Officer

TO: Rudolph M. Brevard
Director, Information Technology Audits
Office of Inspector General

Thank you for the opportunity to respond to the Draft Audit Report: EPA Could Improve Processes for Managing Contractor Systems and Reporting Incidents. We appreciate your efforts to hold informational meetings to ensure clarity of your findings and allow for early review of your recommendations.

The attachment provides corrections to factual errors noted in the Audit Findings and OEI responses to the specific recommendations for the Office of Technology Operations and Planning (OTOP). Please contact Marian Cody, Director of the Technology and Information Security Staff, at 202-566-0302 if you have any questions or need additional information

cc: Myra Galbreath
Marian Cody
Karen Maher

Attachment

OEI Comments on Draft Audit Report:
EPA Could Improve Processes for Managing Contractor Systems and Reporting Incidents
Assignment No. 2006-000068

OEI noted factual errors in the Audit Findings. The factual errors involve the validity of the Audit's findings that EPA offices are unfamiliar with the Agency's Computer Security Incident Response Capability (CSIRC) and confusion about CSIRC's roles and responsibilities.

Pertaining to the first issue, OEI did not find corroborating evidence indicating a lack of understanding in the EPA general community about computer security incident response procedures in either the Office of Inspector General's (OIG) February data collection or in the OIG's detailed back-up data about incidents. In the February data collection, most respondents answered the incident response questions as they applied to any contractor sites identified in the first half of the questionnaire, not as they pertained to their own organization. Nor could OEI discern any evidence of a lack of understanding about incident response procedures in the OIG's detailed back-up data about incidents. While OEI accepts that there probably can never be enough training and communication, we do not accept that the data collected offers clear evidence that EPA lacks policies and procedures for reporting incidents or that EPA offices do not know how, what, or when security incident information should be reported.

Our second area of concern is the OIG's confusion about CSIRC's roles and responsibilities. The Audit Report assigns CSIRC roles and responsibilities for anti-virus. The Agency's Anti-Virus program is managed by the Network Infrastructure Services (NIS) and it is this organization which has responsibility for deploying and following up on implementation of anti-virus software.

OEI Comments on Draft Audit Report:
EPA Could Improve Processes for Managing Contractor Systems and Reporting Incidents
Assignment No. 2006-000068

REC. NO.	RECOMMENDATION	ACCEPT/ DISAGREE	ACTION PLAN	COMMENT
2-1	Develop and implement guidance that EPA offices can use to identify appropriate contractor systems that contain EPA data.	Accept	Update of the Information Security Manual. Completion date: 9/18/2008 ASSERT Task ID 105647	
2-2	Assign duties and responsibilities to internal offices for maintaining the IRM requirements posted on the EPA Website available to contractors	Accept	To Be Determined (TBD)	
3-1	Update the CSIRC guide to include specific instructions for reporting computer security incidents at EPA locations. The updated guide should include specific instructions for prioritizing security incidents and escalating the notification of security incidents within a location. The guide should also include instructions that EPA locations could use to train employees on the local procedures for reporting computer security incidents.	Disagree		OEI has instructions in the current "*Agency Guidance to Incident Handling and Information Security Officer Handbook*". http://intranet.epa.gov/otop/security/CSIRC/CSIRC_Handbook.doc The "*Agency Guidance to Incident Handling and Information Security Officer Handbook*" provides detailed information for Information Security Officers (ISOs) on the proper reporting, prioritization, and escalation of security incidents. The handbook provides specific instructions on incident types, incident reporting, information flows, and specific actions to take during an incident that EPA locations could use to train employees
3-2	Establish a target date when all EPA locations will implement the latest	Accept	Completion date: February 27, 2007	

REC. NO.	RECOMMENDATION	ACCEPT/ DISAGREE	ACTION PLAN	COMMENT
	anti-virus software and configure the software to use centralized monitoring.			
3-3	Develop and implement a strategy to train ISOs on the updated CSIRC guide.	Accept	TBD	While OTOP accepts this recommendation because training is always a good idea, CSIRC has provided training for the past three years to EPA ISOs through monthly teleconferences and at the yearly IT Security and Operations Conference. OTOP, however, will enhance its training strategy to include: - training at the annual Office of Environmental Information (OEI) National Symposium and IT Security and Operations Conference - daily interaction with ISO's on specific incidents - updating EPA's annual Information Security Awareness training to focus on the roles and responsibilities of all employees pertaining to incident reporting, escalation and prioritization.
3-4	Provide local ISOs and responsible information technology personnel with trend analysis reports on computer security incidents.	Accept	TBD	CSIRC creates quarterly trend reports for EPA Management. Historically, these reports were provided to Technical Information Security Staff (TISS) for review and distribution. Effective immediately, these reports will be provided to the ISO community following National Computer Center (NCC) Management review.

Appendix B

Office of Administration and Resources Management Response to Draft Report

December 15, 2006

MEMORANDUM

SUBJECT: Draft Report, EPA Could Improve Processes for Managing Contractor Systems and Reporting Incidents – Assignment No. 2006-000068

FROM: Luis A. Luna, Assistant Administrator
Office of Administration and Resources Management

TO: Rudolph M. Brevard, Director
Information Resources Management Assessments

This is in response to the subject draft report dated October 31, 2006. Specifically, this memorandum addresses recommendation 2-3 of the report which states that the Office of Acquisition Management (OAM) "establish formal procedures to ensure all responsible program offices update and maintain applicable EPA-specific contract clauses on a regular basis."

OAM will periodically request that program offices review EPA-specific contract clauses for any needed updates and/or maintenance. This will be done both in writing (through OAM News Flash Notices), and verbally (through the Contracts Customer Relations Counsel and other forums with our customers). The Service Center Manager of the Acquisition Policy and Training Service Center within OAM, will be established as the point of contact for the receipt of this information from program offices. This initiative will be implemented beginning in the third quarter of FY 2007.

If your staff has any questions, please contact Larry Wyborski at (202) 564-4369. If I can assist in any way, please call me on 564-4600.

Appendix C

Distribution

Office of the Administrator
Assistant Administrator for Environmental Information
Assistant Administrator for Administration and Resources Management
Director, Technology and Information Security Staff
Director, Acquisition Management
Audit Followup Coordinator, Office of Environmental Information
Audit Followup Coordinator, Office of Administration and Resources Management
Audit Followup Coordinator, Technology and Information Security Staff
Agency Followup Official (the CFO)
Agency Followup Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Acting Inspector General