Office of Inspector General

Audit Report

GOVERNMENT INFORMATION SECURITY REFORM ACT

STATUS OF EPA'S COMPUTER SECURITY PROGRAM

Report Number: 2001-P-00016

September 7, 2001

Inspector General Division Conducting the Audit	**Information Technology Audits Staff Washington, D.C.**
Regions covered	**Agency-wide**
Program Offices Involved	**Office of Environmental Information:** **Technical Information Security Staff** **Headquarters and Desktop Services Division** **National Technology Services Division**

Abbreviations

CPIC	Capital Planning and Investment Control
EPA	Environmental Protection Agency
GAO	General Accounting Office
GISRA	Government Information Security Reform Act
GPRA	Government Performance and Results Act
IRCC	Incident Response Coordinating Center
IT	Information Technology
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OA	Office of the Administrator
OAR	Office of Air and Radiation
OARM	Office of Administration and Resources Management
OCFO	Office of the Chief Financial Officer
OECA	Office of Enforcement and Compliance Assurance
OEI	Office of Environmental Information
OGC	Office of General Counsel
OIA	Office of International Activities
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPPTS	Office of Prevention, Pesticides, and Toxic Substances
ORD	Office of Research and Development
OSWER	Office of Solid Waste and Emergency Response
OW	Office of Water
QA	Quality Assurance

MEMORANDUM

TO: Christine Todd Whitman, Administrator

SUBJECT: GISRA: Status of EPA's Computer Security Program
Audit Report No. 2001-P-00016

Attached is our final report entitled "GISRA: Status of EPA's Computer Security Program." We conducted this audit pursuant to the Fiscal 2001 Defense Authorization Act (Public Law 106-398), including Title X, subtitle G, "Government Information Security Reform Act" (GISRA or the Act), which the President signed into law on October 30, 2000. The Act requires that Inspectors General provide an independent evaluation of the information security program and practices of the agency. In this initial year, the primary audit objectives were to assess the status of the Agency-wide information technology security program relative to existing policy; determine whether the program is at an acceptable level of effectiveness and improving; and ascertain to what extent the Agency has taken corrective action on significant recommendations from the General Accounting Office's report on EPA Information Security.

In accordance with the instructions contained in the Office of Management and Budget (OMB) Memorandum 01-24, I am forwarding this report to you for submission, along with the Agency's required information, to the Director, OMB, in conjunction with the Agency's fiscal 2003 budget materials.

Should your staff have any questions, please have them contact Pat Hill, Director, Information Technology Audits Staff, at (202) 260-3615, or Ed Shields, Team Leader, at (202) 260-3656.

Nikki L. Tinsley

cc: M. Schneider, Acting Assistant Administrator and Chief Information Officer

GOVERNMENT INFORMATION SECURITY REFORM ACT: STATUS OF EPA'S COMPUTER SECURITY PROGRAM

Report No. 2001-P-00016

EXECUTIVE SUMMARY

Despite the Environmental Protection Agency's (EPA) efforts to improve its security program, we found several key aspects of security that still require management's attention. These areas include: performance measures; risk management; incident handling; capital planning and investment; enterprise architecture; infrastructure protection; technical controls; and security program oversight. In our opinion, the Agency's past and present security weaknesses stem from the fact that management has not introduced comprehensive oversight processes to thoroughly assess security risks, plan for the protection of information resources, and verify that best security practices are implemented to ensure the integrity, confidentiality, and availability of environmental data. Given the Agency's decentralized organizational structure, it is essential that EPA establish a strong leadership and monitoring role to ensure the success of its computer security program.

The Office of Management and Budget (OMB) issued specific Government Information Security Reform Act (GISRA or the Act) reporting instructions to ensure agencies could provide results in a consistent form and format. Therefore, each of the numbered topics shown below relate to a specific agency responsibility outlined in the Act or OMB Circular A-11, "Planning, Budgeting, and Acquisition of Capital Assets***."***

Topic 1: ***Identify the agency's total security funding as found in the agency's fiscal 2001 budget request. fiscal 2001 budget enacted, and the fiscal 2002 budget request. This should include a breakdown of security costs by each major operating division and include critical infrastructure protections costs that apply to the protection of government operations and assets.***

Inspectors General are not expected to respond to this topic.

Topic 2: ***Identify the total number of programs included in the program reviews or independent evaluations.***

For the purposes of this independent evaluation, we reviewed the following computer security program components: risk management; tracking of computer security training; incident handling capability; capital planning and investment; and enterprise architecture. In addition, in recent years, we conducted numerous audits that resulted in findings for many components and aspects of EPA's security policies and practices. These findings also contributed to our overall conclusion regarding EPA's entity-wide computer security program.

Topic 3: ***Describe the methodology used in the program reviews or independent evaluations.***

The primary focus of this audit was to evaluate Agency policies for components of its computer security program and determine how effectively the Agency was monitoring implementation of these policies. To accomplish the audit objectives, we examined a variety of Federal and EPA documents. We also relied on the results of prior audits, as well as preliminary results from an ongoing audit.

We used the General Accounting Offices's (GAO) July 2000 audit report, entitled "Fundamental Weaknesses Place EPA Data and Operations at Risk," as a key component of our audit methodology. Using the results of GAO's systems tests, we judgmentally selected a sample of 26 GAO technical recommendations to determine how effectively management had implemented corrective actions.

Topic 4: ***Report any material weakness in policies, procedures, or practices as identified and required to be reported under existing law.***

We identified the following significant weaknesses: partially developed performance measures; inadequate risk assessment policy; weak incident handling program; inadequate capital planning and investment oversight; incomplete enterprise architecture; undefined infrastructure protection methodology; and under-developed security program oversight.

Topic 5: ***The specific measures of performance used by the agency to ensure that agency program officials have: 1) assessed the risk to operations and assets under their control; 2) determined the level of security appropriate to protect such operations and assets; 3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control; and 4) tested and evaluated security controls and techniques. Include information on the actual performance for each of the four categories.***

At the close of our field work, the performance measures addressing risk, the adequacy and testing of operational controls, and security plans were still being developed. As such, we were unable to analyze the appropriateness or sufficiency of EPA's measures. The Agency plans to finalize the performance measures before reporting to OMB, and we will evaluate the measures during the next GISRA reporting cycle.

Topic 6: ***The specific measures of performance used by the agency to ensure that the agency Chief Information Officer: 1) adequately maintains an agency-wide security program; 2) ensures the effective implementation of the program and evaluates the performance of major agency components; and 3) ensures the training of agency employees with significant security responsibilities. Include information on the actual performance for each of the three categories.***

Prior to GISRA, the Agency had not established specific measures to address security program performance. These performance measures were still being developed at the end of our field work and, therefore, not available for our review. The Agency plans to finalize the performance measures before submitting its GISRA report to OMB. Accordingly, we plan to review the reasonableness of these measures, as well as the accuracy of baseline measurement data, during the next GISRA reporting cycle.

Topic 7: ***How the agency ensures that employees are sufficiently trained in their security responsibilities. Identify the total number of agency employees and briefly describe what types of security training were available during the reporting period, the number of agency employees that received each type of training, and the total costs of providing such training.***

The Office of Environmental Information (OEI) has delegated the responsibility of ensuring employees are sufficiently trained in their security responsibilities to the various regions and program offices. Our audit did not include assessing the effectiveness of this effort.

As a response to Office of Management and Budget (OMB) Memorandum 01-24, EPA solicited data on the types of security training, the number of agency employees receiving each type of training, and the total costs of such training from its 23 regional and program offices. According to the data submitted by the regions and program offices, from February 2000 to June 2001, the Agency spent $780,426 to train its employees in various security-related courses (see Appendix II.) However, as of the writing of this report, OEI was still collecting missing and incomplete training data; as such, the numbers shown in Appendix II may not agree with the Agency's final totals. In addition, OEI has not verified the accuracy of collected data. Without such verification, the reliability of these numbers is uncertain

Topic 8: ***The agency's documented procedures for reporting security incidents and sharing information regarding common vulnerabilities. Include a description of procedures for external reporting to law enforcement authorities and to the General Services Administration's FedCIRC (Federal Computer Incidents Response Capability). Include information on the actual performance and the number of incidents reported.***

The Agency's official procedures for reporting security incidents and sharing information regarding vulnerabilities needs improvement. EPA solicited data on the number and type of incidents reported from its 23 regional and program offices (see Appendix III). EPA currently lacks an agency-wide program to ensure incidents are handled in a thorough, consistent and timely manner throughout regional and program offices. In light of this weaknesses, we question the Agency's ability to accurately determine whether *all* security incidents are identified, contained, eradicated, recovered, followed-up on, or reported to FedCIRC in a timely fashion. However, efforts are underway to create a comprehensive, consistent Agency-wide incident handling program. EPA management has

tentatively decided to implement a distributed business model to communicate and coordinate incident handling activities across the agency. At this point, management has neither developed an implementation schedule nor committed significant resources to achieve the goal.

Topic 9: ***How the agency integrates security into its capital planning and investment control process. Were security requirements and costs reported on every fiscal 2002 capital asset plan (as well as exhibit 53) submitted by the agency to OMB?***

EPA has not consistently integrated security into its Capital Planning and Investment Control (CPIC) process. Although EPA has begun to integrate security into its CPIC process, more work is needed. We reviewed 47 major Information Technology (IT) capital investment project proposals, as reported to OMB (via Exhibit 300B of the Agency's A-11 budget submission) in December 2000, and found that almost half of these projects were submitted to OMB without approved security plans.

Although the Agency includes cost data for IT capital investment project proposals reported to OMB, we question the accuracy of reported costs. EPA does not have a cost accounting system that would enable managers to track IT project costs; therefore, it may be difficult for EPA to substantiate the IT project costs reported via Exhibit 53 of the Agency's A-11 budget submission to OMB. We are currently evaluating the reliability of reported IT project costs in an on-going audit.

Topic 10: ***The specific methodology used by the agency to identify, prioritize, and protect critical assets within its enterprise architecture, including links with key external systems. Describe how the methodology has been implemented.***

At this point, management has not identified, prioritized, or otherwise specified a methodology for protecting critical assets under its enterprise architecture plan. EPA's Enterprise Architecture plan, dated March 29, 2001, does not define a security architecture. Whereas the Agency recognizes the importance of security, the plan defers completion of that component to some future time. This summer, the Agency stated its intent to form workgroups to address specific aspects of the architecture, and to clearly define roles and responsibilities. We expect it will take significant resources and time for EPA to complete the Enterprise Architecture, including the security architecture component.

Topic 11: ***The measures of performance used by the head of the agency to ensure that the agency's information security plan is practiced throughout the life cycle of each agency system. Include information on the actual performance.***

At the close of our field work, the Agency was still in the process of developing performance measures to ensure the Agency's information security plan is practiced throughout the life cycle of each agency system. The Agency plans to finalize the performance measures before submitting its GISRA report to OMB. As such, we will audit the measures in the next GISRA reporting cycle. At

this point, OEI management does not periodically validate whether regional and program offices actually implement Agency policy requirements by considering, planning for, and documenting security requirements throughout a system's life cycle.

Topic 12: ***How the agency has integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., physical and operational).***

EPA needs to better integrate its information and IT security program with its critical infrastructure protection responsibilities. The Agency categorizes its critical assets as physical, emergency response, telephony, and information technology. However, management was unable to provide or describe the methodology used to identify, prioritize, and protect its critical assets. Without a sound methodology, EPA may not be properly applying its limited security resources to information assets consistent with their level of importance to the Agency's mission. Furthermore, our audit disclosed that major IT infrastructure projects did not have required security plans.

Topic 13: ***The specific methods (e.g., audits or inspections) used by the agency to ensure that contractor-provided services or services provided by another agency are adequately secure and meet the requirements of the Security Act, OMB policy and National Institute of Standards and Technology (NIST) guidance, national security policy, and agency policy.***

No quality assurance (QA) process exists across the agency to ensure contractor-provided services are adequately secure and meet the requirements of the Act. OEI management is beginning to address its oversight responsibilities, but management will need to dedicate additional resources to fully develop and implement QA processes throughout the Agency. The absence of this vital function was, we believe, a key contributing cause to the security program weaknesses mentioned in this report. For several years, in conjunction with the Integrity Act, the Office of Inspector General (OIG) has formally advised EPA to establish a centralized security program with strong oversight processes that would adequately address risks and ensure valuable information resources and environmental data are secure.

In fiscal 2000, management agreed to include an Integrity Act action item that partially addressed its oversight responsibilities (i.e., a commitment to conduct random, formal program office security plan reviews of mission-critical systems). After an initial round of reviews, management is revising its QA approach to achieve more reliable and comparable results. During the last year, management initiated other activities to verify the integrity of its system networks; however, many aspects of the security program are still left to the discretion of individual program and regional offices without benefit of any formalized oversight processes. In an agency as decentralized as EPA, it is imperative that management build a coordinated, comprehensive monitoring program to ensure the effectiveness of its entity-wide computer security program and practices.

Table of Contents

GOVERNMENT INFORMATION SECURITY REFORM ACT: STATUS OF EPA'S COMPUTER SECURITY PROGRAM

Report No. 2001-P-00016

The Environmental Protection Agency (EPA) a has made substantial progress toward ensuring the security of its information assets; however, more work is needed. During a fiscal 2000 audit, the General Accounting Office (GAO) performed significant tests of EPA's network and operating systems' security controls, and found many pervasive and serious security weaknesses. In response to noted technical weaknesses, EPA temporarily disconnected its network from the Internet to accelerate installation of improved security features. Since then, the Agency has taken steps to further separate EPA's Wide Area Network from the Internet; implement better approaches to monitor, detect, and deter Internet attacks and unauthorized users; conduct formal reviews of information security plans; update EPA's policies for protecting and handling sensitive business information; and increase the Agency's efforts to create a more security-minded workforce.

Despite EPA's efforts to improve its security program, we found several key aspects of security that still require management's attention. These areas include: performance measures; risk management; incident handling; capital planning and investment; enterprise architecture; infrastructure protection; technical controls; and security program oversight. In our opinion, the Agency's past and present security weaknesses stem from the fact that management has not introduced comprehensive oversight processes to thoroughly assess security risks; plan for the protection of information resources; and verify that best security practices are implemented to ensure the integrity, confidentiality, and availability of environmental data. Given the Agency's decentralized organizational structure, it is essential that EPA establish a strong leadership and monitoring role to ensure the success of its computer security program.

PURPOSE

The audit objectives were to assess the status of the Agency-wide information technology (IT) security program relative to existing policy; determine whether the program is at an acceptable level of effectiveness and progressing upwards; and ascertain to what extent the Agency has taken corrective action on significant recommendations contained in GAO's report on EPA Information Security (GAO/AIMD-00-215).

BACKGROUND

On October 30, 2000, the President signed into law the Fiscal 2001 Defense Authorization Act (Public Law 106-398), including Title X, subtitle G, "Government Information Security Reform Act" (GISRA or the Act). The Act primarily addresses the program management and evaluation aspects of information security. The Act became effective on November 29, 2000, and expires in two years. Sub-chapter II, section 3535, requires that Inspectors General provide an independent evaluation of the information security program and practices of the agency. On

January 16, 2001, the Office of Management and Budget (OMB) issued guidance on implementing GISRA, and subsequently issued finalized reporting instructions in Memorandum 01-24 on June 22, 2001. These reporting instructions highlighted topics outlined in the Act and provided a consistent form and format for agencies to use.

Under GISRA, Inspectors General, or independent evaluators they choose, are to perform an annual evaluation of the agency's security program and practices. The evaluations are to include tests related to the effectiveness of security controls for an appropriate subset of Agency systems.

SCOPE AND METHODOLOGY

The primary focus of this audit was to evaluate Agency policies for components of its computer security program and determine how effectively the Agency was monitoring implementation of these policies. To accomplish the audit objectives, we examined a variety of Federal and EPA documents, including policies on risk management; incident handling capability; capital planning and investment; enterprise architecture; and system life cycle management. In addition, we relied on the results of prior audits as well as preliminary results of ongoing audits.

GAO's July 2000 audit report, entitled "Fundamental Weaknesses Place EPA Data and Operations at Risk," was a key component of our audit methodology. We used the results of GAO's systems tests as a basis for identifying serious, technical weaknesses. Rather than conducting new tests of controls, we judgmentally selected a sample of 26 GAO technical recommendations to determine how effectively management had implemented corrective actions. Thirteen recommendations related to Novell Local Area Network (LAN) weaknesses, while the other 13 involved mainframe computer operations.

In conjunction with OMB M-01-24, we attempted to obtain and audit relevant data. Whereas management was able to provide some data on security risk assessments and security incidents, we discovered that EPA did not formally coordinate, measure or track these statistics prior to the OMB request. During the audit cycle, the Agency began the process of developing performance measures and gathering baseline information. However, in many instances, the data was not available in time for sufficient analysis and audit verification.

The Office of Inspector General conducted this audit in accordance with Government Auditing Standards (1999 revision) issued by the Comptroller General of the United States. We conducted our audit fieldwork from June 18, 2001 through July 20, 2001, at EPA Headquarters in Washington, D.C., as well as the Agency's National Computer Center in Research Triangle Park, North Carolina. In conjunction with our field work, we interviewed personnel within the Office of Environmental Information's Technical Information Security Staff, Headquarters and Desktop Services Division, and the National Technology Services Division.

PRIOR AUDIT COVERAGE

During recent years, we have audited many components and aspects of EPA's security policies and practices. As a result of OIG report findings, EPA first declared Information Systems Security Planning as a material weakness in its fiscal 1997 Federal Managers' Financial Integrity Act Report (Integrity Act). In following years, management continued to work on security problems and, in fiscal 1999, extended the material weakness to address GAO report findings and to assess the effectiveness of new Agency policies and procedures.

The following audit reports highlight some recent security findings:

- In March 2001, we issued Report No. 2001-P-00004, "Environmental Protection Agency Payroll and Personnel Systems (EPAYS) Access Controls." This audit found that EPA did not adequately control access to EPAYS. Some users had EPAYS access when they did not need it, and others were granted access authorities greater than needed. Furthermore, some users continued to have access after they left the Agency or transferred to different job functions. EPAYS is used to process all EPA payroll and personnel-related data, and improperly managed access controls increase the potential for fraud, waste, and abuse of such data. In addition, users were granted excessive access to EPAYS data sets that contained sensitive information. Many of these users generally needed access to some of the data sets but not all. Excessive access can result in EPA employees' personnel information being vulnerable to misuse or abuse.

- In July 2000, GAO issued Report No. GAO/AIMD-00-215, "Fundamental Weaknesses Place EPA Data and Operations at Risk." This audit found serious and pervasive problems that essentially rendered EPA's agency-wide information security program ineffective. GAO's tests of computer-based controls concluded that the computer operating systems and the Agency-wide computer network that support most of EPA's mission-related and financial operations were riddled with security weaknesses. Of particular concern was that many of the most serious weaknesses identified had been previously reported to EPA management by EPA's OIG in 1997.

- In June 2000, we issued Report No. 2000-1-00330, "RACF Security Controls." This audit found that EPA's Resource Access Control Facility settings did not adequately protect system resources. Specifically, excessive authority was granted to users via the resource classes. In addition, resource class settings did not optimize system security. As a result, the potential misuse, manipulation, and/or destruction of EPA's information resources was increased.

- In January 1999, we issued Report No. 9300001, "Operating System Software Controls." This audit found EPA's Enterprise Technology Services Division (ETSD) - currently called the National Technology Services Division - was not maintaining and reviewing authorized program facility (APF) libraries in a timely manner, and was not adequately

controlling the number of users who had ALTER and/or UPDATE access capabilities to APF libraries. Without effectively managing the contents of the APF, and controlling access to APF, ETSD management could not be assured programs running in an authorized state would adhere to Multiple Virtual Storage system integrity requirements or Agency integrity guidelines. In addition, without effective access controls to the APF, a knowledgeable user could circumvent or disable security mechanisms and/or modify programs or data files on the computer without leaving an audit trail.

- In December, 1997, we issued three reports on Physical and Environmental Information Systems Controls at EPA Regional Facilities. These reports involved Region I (Report No. E1AMN7-15-7001-8300007), Region III (Report No. E1AMN7-15-7001-8300006), and Region V (Report No. E1AMN7-15-7001-8300003). These audits found that Regions I, III, and V did not require General Services Administration contractors, who were responsible for Agency information systems, to undergo criminal and financial background investigations.

- In September, 1997, we issued Report No. 7100284, "EPA's Internet Connectivity Controls." This audit found EPA had not sufficiently developed or implemented adequate controls to prevent or detect improper/illegal access to its systems from the Internet. As a result, EPA could not be assured its information resources were sufficiently protected from unauthorized access/use, manipulation, and destruction. These weaknesses occurred primarily because EPA had not developed and implemented a network security policy for the Agency that included Internet access and usage.

ONGOING AUDIT WORK

We are currently evaluating EPA's IT Capital Investment Process to determine whether IT projects are adequately planned, screened, and formally approved prior to being recommended for funding in the budget. In addition, this audit is assessing how effectively and efficiently IT investment projects are managed.

CRITERIA

Federal laws, policies, and guidelines were used to form a framework of prudent, stable business practices and, therefore, served as a means to evaluate the effectiveness of Agency security policies and practices. Appendix I contains a summary of the criteria used during our audit.

SECURITY PROGRAM PERFORMANCE

EPA is making progress toward implementing an Agency-wide security program and responding to GAO recommendations. However, our audit identified several areas where improvement is necessary. These areas include: performance measures; risk assessment; management; incident

handling; capital planning and investment; enterprise architecture; infrastructure protection; technical controls; and security program oversight.

Performance Measures Not Fully Developed

Prior to implementation of the GISRA, the Agency had not established specific measures to address security program performance. Pursuant to the OMB reporting instructions, the Agency recognized the valuable role performance measures play in supporting an effective information security program. In this spirit, management directed resources to develop performance measures addressing specific OMB topics. At the close of our field work, the performance measures were still being developed and, therefore, not available for audit analysis. The Agency plans to finalize the performance measures before reporting to OMB. As such, we will audit the measures in the next GISRA reporting cycle.

We also noted that EPA's current Government Performance and Results Act (GPRA) goals and objectives do not contain any security-related annual performance goals (APGs) or measures. Given the absence of such GPRA APGs and measures, we are uncertain how management intends to align the newly-developed, internal security measures (i.e., the major aspects of its security program) with EPA's strategic goals and objectives to help managers effectively use systems and data to achieve environmental results.

Risk Assessment Guideline Missing Significant Elements

EPA's draft "Risk Assessment Guideline" is a good first step toward developing a robust risk assessment framework; however, it is missing key elements. Our comparison of National Institute of Standards and Technology (NIST) Publication 800-30, "Risk Management Guide" and EPA's "Risk Assessment Guideline" revealed significant gaps between the two documents. The NIST guidance presents a comprehensive approach that will allow IT personnel to isolate a variety of risks, determine the extent of a compromise, and identify potential mitigation options. It covers several risk assessment and risk mitigation issues that EPA's Guide does not discuss in sufficient detail:

- Risk Assessments
  - ✓ Control Analysis
  - ✓ Likelihood Determination
  - ✓ Impact Analysis
  - ✓ Level of Risk Determination

- Risk Mitigation
  - ✓ Cost-benefit Analysis
  - ✓ Residual Risk

EPA's information assets may be more vulnerable to loss of availability, integrity, and confidentiality if the risk assessment and mitigation elements listed above are excluded from its policy, procedures, and practices.

Security Awareness Training Tracked But Not Verified

Chapter 8 of EPA Manual 2100, Information Resources Management Policy Manual, authorizes the information program offices and region to determine whether employees are sufficiently trained in their security responsibilities. Our audit did not include assessing the effectiveness of this effort.

In response to M-01-24, EPA solicited data on the types of security training, the number of agency employees receiving each type of training, and the total costs of such training from its 23 regional and program offices. The results of the data collected indicate that for the February 2000 through June 2001 time period, the Agency spent $780,426 to train its 17,382 (540 technical staff and 16,842 general staff) employees in various security-related courses (see Appendix II.) The Agency estimated spending an additional $40,000 for a security conference held in August. As shown in Appendix II, the percentages of staff trained ranged from 0.02 percent to 20.5 percent for general staff and from 6.48 percent to 95.93 percent for technical staff, depending on the type of training delivered. For example, 3,453 general staff (20.50 %) and 518 technical staff (95.93 %) received "Other Security Awareness Training" during the stated period. However, when it came to specialized training, such as "Security Management Training," only 20 general staff (0.12 %) and 74 technical staff (13.70 %) received training.

As of the writing of this report, OEI is still collecting missing and incomplete training data; as such, the numbers shown in Appendix II may not agree with the Agency's final totals. In addition, OEI has not verified the accuracy of collected data. Without such verification, the reliability of these numbers is uncertain.

Incident Handling Program Needs Improvement

The EPA does not have a robust, agency-wide security incident handling program. At this point, EPA is unable to accurately determine whether *all* security incidents are identified, contained, eradicated, recovered, followed-up on, or reported to FedCIRC (Federal Computer Incidents Response Capability) in a timely fashion. OEI, in response to OMB's reporting instructions, solicited data on the number and type of incidents reported from EPA's 23 regional and program offices (see Appendix III). In light of the possible interpretations that regions and program offices may have made to generate data for the Agency's collection instrument, we are uncertain that total reliability can be placed on the completeness or consistency of incident handling data, as presented in the Agency's annual agency program review responding to GISRA. These concerns are compounded by the fact that OEI management only inquired about missing or seemingly abnormal data; they have not, nor do they plan to, verify the accuracy of data collected for performance measurement purposes. As it looks to the future, OEI has undertaken

efforts to create a comprehensive, consistent Agency-wide incident handling program. After considering several business model options, EPA's senior IT management has tentatively decided on a distributed business model solution.

A distributed business model involves creating an Incident Response Coordinating Center, which would be the central point of contact assisting with communicating and coordinating incident handling activities across the Agency in cooperation with local business units (see Appendix IV). According to Agency documents, this approach will address computer security incidents, including unauthorized root access, unauthorized user access, malicious code, virus detection, denial of service, and theft of data. Although the Agency has selected a model that appears to address the relevant issues, it has neither developed an implementation schedule nor has it committed significant resources to implementing the plan. Without a comprehensive, Agency-wide security incident handling program, the EPA management will not be able to ensure incidents are handled in a thorough, consistent, and timely manner throughout regional and program offices, or gauge the Agency's progress in minimizing threats.

Capital Planning and Investment Control Needs Improvement

EPA has begun to integrate security into its Capital Planning and Investment Control process, although we have significant concerns regarding the progress to date. We reviewed 47 major IT capital investment project proposals, as reported to OMB (via Exhibit 300B of the Agency's A-11 budget submission) in December 2000. EPA submitted almost half of these projects to OMB without approved security plans, although such plans are required for each general support system according to OMB Circular A-11. (See Appendix I for further details regarding Federal requirements.) As of December 2000, OMB had approved EPA's budget document, funding major IT systems despite the exclusion of approved security plans. In our opinion, EPA should develop risk-based security plans for all its major IT systems before submission to OMB.

Although the Agency includes cost data for IT capital investment project proposals reported to OMB, we question the accuracy of reported costs. EPA does not have a cost accounting system that would enable managers to track IT project costs; therefore, it may be difficult for EPA to substantiate the IT project costs reported via Exhibit 53 of the Agency's A-11 budget submission to OMB. We are currently evaluating the reliability of reported IT project costs in an on-going audit.

Enterprise Architecture Does Not Define Security Architecture

We reviewed the Agency Enterprise Architecture[1] plan, dated March 29, 2001, and concluded that the plan did not define a security architecture. OMB had requested EPA's enterprise

1 An Enterprise Architecture is an integrated framework that defines the baseline, transitional and target business processes, and information technology of an organization.

architecture plan on November 9, 2000, although it was not submitted to OMB until April 6, 2001. The plan identified security architecture as one of its seven main components, but stated that the Agency would identify a security architecture in the future. In July 2001, EPA management convened an Enterprise Architecture Summit where team roles and responsibilities were discussed. As a result of the meeting, EPA plans to form workgroups to address specific aspects of the architecture. We expect it will take significant resources and time to complete the Enterprise Architecture, including the security architecture component. At this point, management has not identified, prioritized, or otherwise specified a methodology for protecting critical assets under its critical enterprise architecture plan. As of July 2001, management had not approved a plan to complete the security architecture.

Need To Better Integrate IT Security With Infrastructure Protection

OEI categorizes its critical assets as physical, emergency response, telephone, and information technology. However, at the end of our field work, OEI was unable to provide the methodology used to identify, prioritize, and protect critical assets, or describe how this methodology has been implemented. Without a sound methodology, EPA may not be properly applying its security resources to information assets consistent with their level of importance to the Agency's mission.

Our audit disclosed that major IT infrastructure projects did not have required security plans. Of the 47 IT project proposals mentioned previously, 10 were major IT infrastructure projects. We reviewed the Exhibit 300B reports for the 2002 budget, and found that 7 of the 10 projects did not have approved security plans. (We did not review the adequacy of the security plans for 3 of the 10 infrastructure projects.) In our opinion, the project managers of infrastructure projects should complete an approved risk-based security plan to ensure critical controls are adequate to protect the major information systems, business processes, and data these infrastructures support.

Agency Correcting Technical System Weaknesses

In July 2000, GAO reported numerous technical-oriented recommendations to improve security over EPA's wide area network. The Agency continues to eliminate these technical weaknesses and improve overall network security configuration and practices; however, management needs to do more. We reviewed the implementation of 26 recommendations during our audit cycle. Thirteen of the recommendations related to mainframe computer operations and 13 concerned Novell LAN security. The Agency provided adequate evidence to support corrective actions for all 13 mainframe recommendations, as well as three of the 13 Novell recommendations. However, EPA did not provide timely documentation to support its corrective actions for the remaining 10 Novell weaknesses; therefore, we could not determine whether EPA had fully implemented GAO's technical recommendations for its Novell systems.

The Agency's inability to provide sufficient support and evidence of adequate corrective action raises questions about the extent to which these recommendations have been addressed. If EPA

does not completely address these recommendations, unauthorized users could gain control of individual EPA computer applications and the data used by these applications.

Oversight Role Needed To Verify Effectiveness Of Security Program

OEI is only beginning to establish some security oversight for EPA's complex information systems network. The absence of this vital function was, we believe, a key contributing cause to the security program weaknesses mentioned in this report. For several years, in conjunction with the Integrity Act, the OIG has formally advised EPA to establish a centralized security program with strong oversight processes that would adequately address risks and ensure valuable information resources and environmental data are secure.

Under the Integrity Act, EPA has implemented numerous corrective actions to improve its information systems security plans and program, and eliminate this material weakness from its Integrity Act reporting. However, OEI management has repeatedly excluded establishing a robust oversight role from its corrective action plan for the program. In its fiscal 2000 Integrity Act Report, EPA agreed to include an action item that partially addressed these responsibilities (i.e., a commitment to conduct random, formal program office security plan reviews of mission-critical systems). To that end, OEI used contractor services to evaluate a sampling of information system security plans; however, OEI ultimately found the results unsatisfactory for QA purposes. Consequently, OEI has decided to revise its QA review approach by (1) better defining evaluation criteria, and (2) ensuring that contractors follow consistent verification procedures and adequately evaluate the substance of relevant source documents.

By establishing a limited QA process, OEI management is taking its first step towards addressing its oversight responsibilities for EPA's security program. However, we believe much more needs to be done to ensure the effectiveness of EPA's entity-wide computer security program and practices. For example, OEI currently does not perform oversight to determine whether regional and program offices follow Agency policies for system life cycle management (EPA Directive 2100, Chapter 17). This policy identifies the stages of the system life cycle, and requires managers to comply with Federal and Agency security requirements for planned and on-going information systems. However, OEI does not periodically validate whether regional and program offices actually implement the policy requirements by considering, planning for, and documenting security requirements throughout a system's life cycle.

As another example, OEI is collecting data from regional and program offices through an Agency-wide, self-assessment tool. OEI will use this data as a baseline for its new security-related performance measures; however, management has no plans to perform field work to verify the accuracy of collected data. OEI officials stated that they will only inquire about missing or seemingly abnormal responses prior to reporting to OMB; after submission, no additional checks will be performed.

To their credit, EPA hired a contractor to conduct subsequent rounds of penetration tests on its network systems. The first round of tests applied the same methodology GAO used during their security audit, and the contractor reported that only minor vulnerabilities were found. OEI plans to conduct another round of penetration tests over the next six months, and states that these tests will be more intrusive in nature. During our audit, we evaluated the contractor's Draft Penetration Testing Program Concept of Operations (i.e., the draft penetration test plan for the second set of tests), dated June 22, 2001. The draft plan mainly defined penetration terms, but did not include key elements, such as: tools to be used; specific system targets; penetration limits; and expected, acceptable outcomes.

EPA is a very decentralized agency - a fact that increases the importance of using a coordinated, comprehensive monitoring program. Without regular, effective oversight processes, EPA management will continue to place unsubstantiated trust in its many components to fully implement, practice, and document security requirements. Moreover, the public and Congress may continue to question how well the Agency plans for and protects its information resources to ensure the integrity, confidentiality, and availability of environmental data.

Recommendations

We recommend EPA's Chief Information Officer implement the following actions.

For performance measures:

1. Review the newly-developed performance measures to ensure they adequately cover major aspects of the security program. Also, incorporate major performance measures into annual performance goals, and align them with the Agency's strategic goals and objectives.

2. Establish a system to effectively monitor progress on the established performance measures.

For risk assessments:

3. Revise the Risk Assessment Guideline to include the risk assessment and mitigation items contained in NIST Publication 800-30, as described in this report.

For incident handling:

4. Formally approve and proceed with implementing the Distributed Business Model.
5. Develop a detailed plan and schedule for agency-wide implementation of the Distributed Business Model.

6. Develop and implement a process to monitor the agency-wide implementation of the Distributed Business Model.

For IT Capital Planning and Investment Control:

7. Develop risk-based security plans for all major IT systems before submission to OMB.

For Enterprise Architecture:

8. Develop and approve a formal plan to develop a security architecture, and include it in the enterprise architecture.

For Information Technology Security Infrastructure:

9. Complete an approved risk-based security plan to ensure critical general controls are adequate to protect the major information systems these infrastructures support.

For GAO technical recommendations:

10. Implement all GAO Novell LAN recommendations, thoroughly documenting how each technical weakness was corrected.

For Computer Security Oversight Role:

11. Establish a comprehensive and robust security oversight role, with sufficient resources, to verify Agency practices conform to relevant performance measures and Agency policies.

12. Develop and implement an agency-wide strategy for overseeing major aspects of EPA's computer security program.

13. Routinely assess, test, and provide feedback to regional and program offices regarding the effective implementation of Agency policies.

14. Validate whether regional and program offices consider, plan for, and document security requirements throughout a system's life cycle.

15. Identify tools to be used; specific system targets; penetration limits; and expected, acceptable outcomes in all future penetration testing plans.

Criteria and Guidance

Government Information Security Reform Act (GISRA)
GISRA addresses the program management and evaluation aspects of information security. The Act requires that Inspectors General provide an independent evaluation of the information security program and practices of the Agency. The independent evaluation must include testing the effectiveness of information security control techniques for an appropriate subset of the Agency's information systems, and an assessment of the results of that testing.

Reporting Instructions for the Government Information Security Reform Act
OMB Memorandum, M-01-24, dated June 22, 2001, requests IGs to respond to 12 topics when reporting an agency's actual performance in implementing the Security Act.

OMB Circular No. A-11 (Appendix 300B) - Planning, Budgeting, and Acquisition of Capital Assets
The policy requires agencies to demonstrate that security plans for major IT projects:

- include security controls for components, applications and systems that are consistent with the Agency's IT architecture;
- are well-planned;
- manage risks;
- protect privacy and confidentiality; and
- explain any planned or actual variance from NIST security guidance.

OMB Circular No. A-130 (Appendix III) - Security of Federal Automated Information Resources
This appendix establishes a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and management control systems established in accordance with OMB Circular No. A-123.

NIST Special Publication 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
This document provides a baseline that organizations can use to establish and review their IT security programs.

NIST Special Publication 800-18 - Guide for Developing Security Plans for Technology Systems

This publication provides a guideline for Federal agencies to follow when developing security plans to document the management, operational, and technical controls for Federal automated information systems.

NIST Special Publication 800-30 - Draft Risk Management Guide

This document provides both definitional and practical guidance regarding the concept and practice of managing IT-related risk. The publication defines risk as the net impact of an adverse IT-related event.

EPA Manual 2100, Chapter 8

This policy authorizes the various program offices and regions to determine whether employees are sufficiently trained in their security responsibilities.

EPA Manual 2100, Chapter 17

This policy establishes the life cycle requirements of EPA's automated information systems. It identifies the stages of the systems life cycle and requires that information systems comply with Federal and Agency policies. It applies to all automated information application systems EPA develops, produces, or maintains.

Security Training-Related Data

Reported For February 1, 2000 Through June 15, 2001

Total Number of Employees					17,382
Total Number of General Staff					16,842
Total Number of Technical Staff					540
	General Staff	**Percent Trained**	**Technical Staff**	**Percent Trained**	**Cost**
2000 Information Security Officer (ISO) Forum	0	0.0%	68	12.59%	$40,000
System Security & Exploitation Training (SYTEX)	0	0.0%	35	6.48%	$50,000
New Employee Orientation Training	930	5.52%	92	17.04%	$0
Senior Executive and Management Training	86	0.51%	0	0.0%	$146,399
Agency-wide Security Awareness Training	not reported		0	0.0%	$100,000
Other Security Awareness Training	3,453	20.50%	518	95.93%	$10,515
Security Management Training	20	0.12%	74	13.70%	$84,985
Systems Management Training	4	0.02%	92	17.04%	$71,461
Database Management Training	7	0.04%	62	11.48%	$108,629
Technical Certification Training	3	0.02%	60	11.11%	$168,437
Total Dollars Spent					*$780,426

*This figure does not include $40,000 which the Agency planned to spend on a security conference held in August 2001.

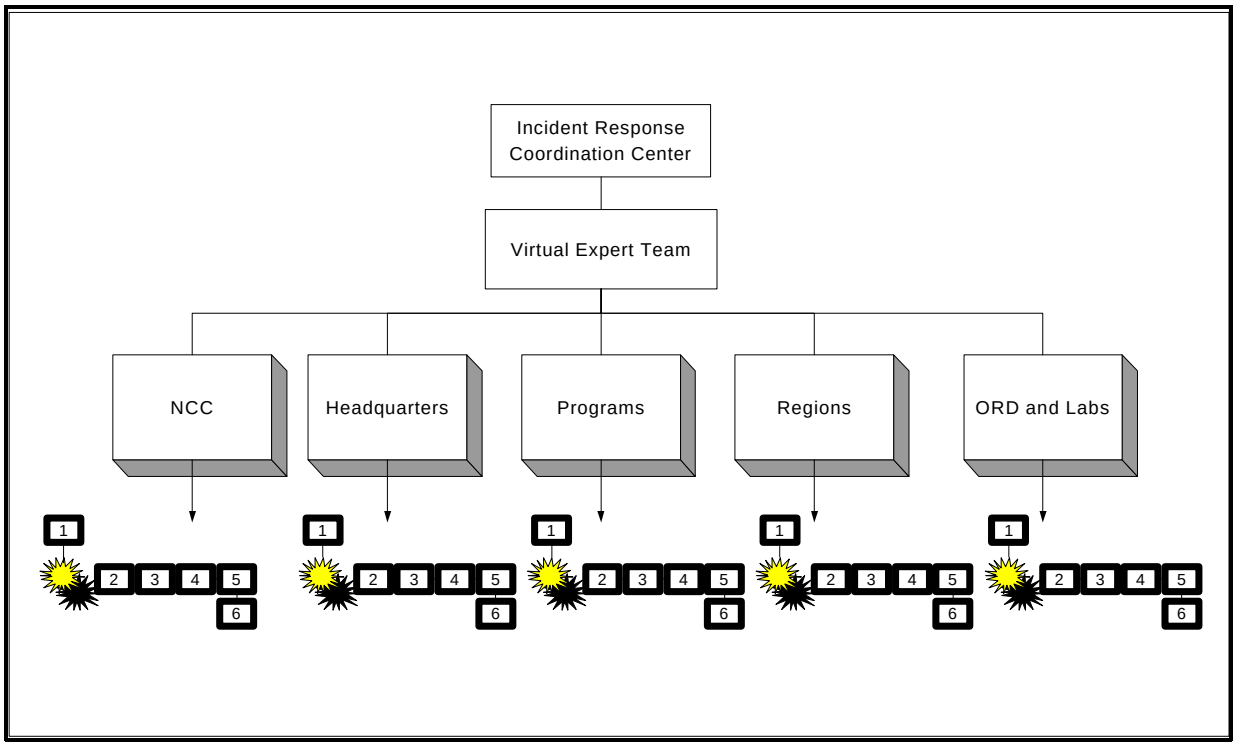
Information Security Incidents

Reported For February 1, 2000 Through June 15, 2001

	NUMBER OF INCIDENTS		STATUS		
Region/Program Office	Total Number of Security Incidents	Number Reported to Technical Support Center	Number of Incidents Open	Number of Incidents Closed	Documented Procedures for Handling Incidents?
Region 1	10	7	0	8	No
Region 2	69	0	0	69	Yes
Region 3	152	0	0	152	Yes
Region 4	5	0	0	5	Yes
Region 5	2	2	2	2	No
Region 6	87	0	0	0	Yes
Region 7	3,000	0	0	0	Not Reported
Region 8	216	2	0	216	Yes
Region 9	Not Reported	Not Reported	Not Reported	Not Reported	Not Reported
Region 10	14	7	0	14	Yes
OA	202	0	1	201	Yes/No
OAR	129	5	0	23	No
OARM	82	12	1	81	Yes
OCFO	12	12	0	12	Yes
OECA	11	0	0	11	Yes
OEI	121	117	21	99	Yes
OGC	13	0	0	13	Yes
OIA	0	0	Not Reported	Not Reported	No
OIG	1	1	0	1	Not Reported
OPPTS	3	0	0	3	Yes
ORD	141	9	3	138	Yes
OSWER	7	5	0	5	Not Reported
OW	8	0	0	6	Yes
Total	4,278	179	28	1,059	

Distributed Business Model for Incident Response Coordinating Center

The Distributed Business Model involves creating an Incident Response Coordinating Center (IRCC), which would be the central point of contact assisting with communicating and coordinating incident handling activities across the Agency in cooperation with local business units. A central expert team available upon request would further support the central IRCC in responding to local business units or in responding to complex and/or catastrophic incidents. The expert team would comprise virtual team members. A virtual team means the team members are positively identified and available when needed. Virtual team members would not have incident handling as a full-time job, but it would be their priority duty during an incident. The virtual team members would be selected based upon skill sets necessary to address Agency platforms and operating systems. This distribution of virtual team membership would add to the expert teams' understanding of Agency business and infrastructure. Local business units at each campus (e.g., headquarters, labs, regions, programs) would have a local incident response team providing the technical, management, and communication response for localized incidents. Local business units would provide reports to the central IRCC.



Report Distribution

Recipients

Director, OMB
Administrator, Environmental Protection Agency (1101A)

Office of Inspector General

Inspector General (2410)
Assistant Inspector General for Audit (2421)
Media and Congressional Liaison (2410)
Agency Business Systems Lead (2421)
Counsel (2411)
Editor (3AI00)

Headquarters Office

Chief Information Officer (2801A)
Assistant Administrator, Office of Environmental Information (2801A)
Director, Office of Technology Operations and Planning (2831)
Director, National Technology Services Division (MD-34)
Director, Technical Information Security Staff (2831)
Chief, Formulation and Control Policy Branch, Annual Planning and Budget Division (2732A)
Agency Follow-up Official (2710A)
Agency Audit Follow-up Coordinator (2724A)
Audit Liaison, Office of Environmental Information (2812A)
Alternate Audit Liaison, Office of Environmental Information (2812A)