



Office of Inspector General

Evaluation Report

GOVERNMENT INFORMATION SECURITY REFORM ACT

STATUS OF EPA's COMPUTER SECURITY PROGRAM

Audit Report Number: 2002-S-00017

September 16, 2002

Inspector General Division
Conducting the Evaluation

Information Technology Audits
Division, Washington, D.C.

Regions Covered

Agency-wide

Program Office Involved

Office of Environmental Information

Team Members

James Rothwell
Anita Mooney
Chuck Dade
Rudy Brevard
Debbie Hunter
Teresa Richardson
Michael Young
Neven Morcos
Carolyn Bowers



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

SEP 16 2002

THE INSPECTOR GENERAL

MEMORANDUM

SUBJECT: Government Information Security Reform Act: Status of
EPA's Computer Security Program
Report No. 2002-S-00017

TO: Christine Todd Whitman
Administrator

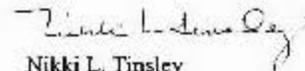
Attached is our final report entitled *Government Information Security Reform Act: Status of EPA's Computer Security Program*. We performed this evaluation pursuant to the Fiscal 2001 Defense Authorization Act (Public Law 106-398), including Title X, subtitle G, "Government Information Security Reform Act (the Act)". Our objectives were to provide an independent evaluation of the Agency's information security program and practices, and to determine whether it has taken appropriate corrective actions in response to the Unix and Novell recommendations provided by the General Accounting Office (GAO/AIMD-00-215, *Fundamental Weaknesses Place EPA Data and Operations at Risk*).

The Office of Management and Budget (OMB) issued specific reporting instructions to ensure agencies could provide results in a consistent form and format. As such, each of the numbered topics shown in the report relates to a specific agency responsibility outlined in the Act or OMB Circular A-11, "Planning, Budgeting, and Acquisition of Capital Assets."

We performed field work from June 5, 2002 through July 30, 2002, and followed general standards for conducting audits, as issued by the Comptroller General of the United States. We conducted our review primarily at the Office of Environmental Information, located at EPA Headquarters in Washington, D.C. The evaluation focused on responding to questions posed by OMB. We accomplished this by conducting interviews with appropriate Agency personnel and, where possible, verifying their responses by analyzing supporting documentation.

In accordance with the OMB reporting instructions, I am forwarding this report to you for submission, along with the Agency's required information, to the Director, OMB.

Should your staff have any questions, please have them contact Pat Hill, Director, Business Systems, at (202) 566-0894.


Nikki L. Tinsley

Attachment

cc: Kimberly T. Nelson, Chief Information Officer

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

Audit Report No. 2002-S-00017

Question A.1 *Identify the agency's total security funding as found in the agency's FY02 budget request, FY02 budget enacted, and the President's FY03 budget. This should include a breakdown of security costs by each major operating division or bureau and include critical infrastructure protection costs that apply to the protection of government operations and assets. Do not include funding for critical infrastructure protection pertaining to lead agency responsibilities such as outreach to industry and the public.*

Inspectors General were not expected to respond to this question.

Question A.2 *Identify and describe as necessary the total number of programs and systems in the agency, the total number of systems and programs reviewed by the program officials, CIOs, or IGs in both last year's report (FY01) and this year's report (FY02) according to the format provided below. Agencies should specify whether they used the NIST self-assessment guide or an agency developed methodology. If the latter was used, confirm that all elements of the NIST guide were addressed.*

	FY01	FY02
a. Total number of agency programs	24	24
b. Total number of agency systems	189	
c. Total number of programs reviewed	24	24
d. Total number of systems reviewed	189	

The Environmental Protection Agency (EPA) had not finalized its list of agency systems for FY02 by the end of our fieldwork. At that time, program and regional offices had been sent a list of systems for which they were responsible. The Agency planned to finalize the actual list of reportable systems for FY02 by the end of August 2002, after all programs and regions had submitted their assessments and/or documentation. Managers were asked to either perform an assessment on the systems or provide documentation as to why the systems should not be reported under the Government Information Security Reform Act (GISRA).

The Agency deployed a web-enabled self-assessment tool that incorporates National Institute for Standards and Technology (NIST) Self-Assessment, Special Publication 800-26. This tool was the basis for performing system assessments for FY02. EPA's Office of Environmental Information (OEI) stated it would perform a quality assurance review to determine the reasonableness and logic of the responses received.

Question A.3 *Identify all material weakness in policies, procedures, or practices as identified and required to be reported under existing law. Identify the number of reported material weaknesses for FY01 and FY02, and the number of repeat weaknesses in FY02.*

For FY01, the Agency reported Information Systems Security as a material weakness under the Federal Managers' Financial Integrity Act. In FY02, the OIG is recommending that Information Systems Security be downgraded to an agency-level weakness due to the considerable progress EPA made in implementing its computer security program. There were no repeat weaknesses involving security issues.

Question B.1 *Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth the Security Act's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced? Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?*

EPA's Administrator took steps to set forth the Security Act's responsibilities, as well as authorities for the Agency's Chief Information Officer (CIO) and program officials. For example, in December 2001, EPA issued a revised Delegations Manual identifying CIO responsibilities and authority. As Chair of the Quality Information Council, the CIO actively participated during strategic management activities and operational planning efforts. In addition, the CIO advised EPA's Administrator, via the advisement letter and Capital Planning and Investment Control (CPIC) proposals, on information resource implications of strategic planning decisions and on the design, development, and implementation of information resources.

In June 2002, the CIO redelegated the following responsibilities to various OEI Directors:

- serve as Chair of the Agency's Data Integrity Collection Board;
- establish policies and procedures for the management and security of records, files and data;
- establish and maintain a continuing program for the management and security of records data and files;
- establish policies and procedures for the management and security of information systems and technology;
- approve the acquisition of information technology (IT) resources; and
- establish and maintain a continuing program for the management and security of information systems and technology.

Also, the CIO monitors compliance with policies, procedures, and guidance through the annual assessment, which provides an update on the status of the Agency's security program. The annual assessment is reported to the Office of Management and Budget (OMB) each September. As a follow-on activity to this annual assessment, the Agency identifies where improvements in the security program can be made, develops detailed plans of action and milestones to implement these improvements, and reports progress to OMB on a quarterly basis.

As long as EPA strictly adheres to its CPIC policy, a major operating component of the agency cannot make a major IT investment decision without review by and concurrence of the Agency's CIO. In May 2002, EPA issued an interim policy that outlined the approval policy for IT investments. By June 2002,

management superceded the interim policy with a final IT CPIC policy under EPA Order 2100.2A1. The Order established the policy for assuring that IT resources are invested and managed to achieve high value outcomes at acceptable costs. The policy requires EPA Offices to submit proposals for IT investment(s) to the CIO. If approved, these investments will be funded from the submitting Office's budget. The CIO, in conjunction with the Chief Financial Officer, Senior Procurement Executive, and senior program officials on the IT Investment Board, selects those investments recommended for funding in the Agency's budget. After the selection process is completed, the CIO sends an advisement letter to the Administrator that lists the approved IT investments. The advisement letter also summarizes the number of total IT investment proposals reviewed, the number recommended for funding, and the number of proposals withdrawn from consideration. We found that the approved investment proposals submitted to OMB in November 2001 were the same ones approved by the CIO in her September 2001 advisement memorandum. The OIG believes additional improvements can be made to EPA's CPIC and IT procurement processes and will issue findings in a report entitled *EPA's Management of Information Technology Resources Under the Clinger-Cohen Act*.

Question B.2 *How does the head of the agency ensure that the agency's information security plan is practiced throughout the life cycle of each agency system? During the reporting period, did the agency head take any specific and direct actions to oversee the performance of 1) agency program officials and 2) the CIO to verify that such officials are ensuring that security plans are up-to-date and practiced throughout the lifecycle of each system?*

The Agency head delegated to the CIO the responsibility of establishing and maintaining a continuing program for the management and security of records, files, data, and information systems and technology. In June 2002, the CIO redelegate the task of ensuring system security plans are up-to-date and practiced throughout the life cycle of each system to OEI's Director for Technology Operations and Planning (OTOP).

EPA's current Life Cycle Management policy is outdated. In EPA's 2001 GISRA Report, OEI indicated it would be updating the life cycle policies and guidance. The updating of such policies is not complete. However, OEI indicated that it has a process underway to identify those IT policies needing to be created, updated, or canceled in order to address gaps between what EPA's current IT policy collection is and what it should be from a best practices perspective. OEI expects to issue a multi-year plan for addressing the gaps and updating EPA's IT policy by November 2002.

The Agency has not developed a dedicated process for ensuring that security plans of general support systems and major applications are up-to-date and practiced throughout the life cycle of the system. EPA currently ensures the existence of many, but not all, security plans through the CPIC, the National Technology Services Division's (NTSD) Application Deployment Process, and a Security Plan Independent Review Process. However, CPIC process reviews are limited to "Major Agency Systems," and NTSD's Application Deployment Process is limited to "Major Agency Systems" or applications that contain data defined as having a "high" sensitivity level. Additionally, OEI indicated that the Security Plan Independent Review Process includes "completeness" reviews of security plans submitted with CPIC proposals, as well as a comprehensive review and testing of four system security plans which OEI expects to complete next fiscal year. At this time, the Agency does not verify the existence of security plans for those systems and applications that do not fall into these categories. In addition, and in

response to GISRA, EPA now requires all programs to perform assessments in accordance with NIST Special Publication 800-26. OEI management will compile and report the results of these assessments in the Agency's GISRA report to OMB.

Question B.3 *How has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., continuity of operations, and physical and operational security)? (Sections 3534 (a)(1)(B) and (b)(1) of the Security Act.) Does the agency have separate staffs devoted to other security programs, are such programs under the authority of different agency officials, if so what specific efforts have been taken by the agency head or other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent and complimentary across the various programs and disciplines?*

The Agency is beginning to integrate its information and IT security program with its critical infrastructure protection responsibilities. In EPA's Critical Infrastructure Protection Mitigation Plan, dated September 21, 2001, the responsibilities for assessing and addressing vulnerabilities are aligned with each office's overall mission. The plan states that within EPA, the overall infrastructure assurance responsibilities are shared by the Office of Administration and Resources Management (OARM), the Office of Solid Waste and Emergency Response (OSWER), and the Office of Water (OW). Specifically, OARM maintains responsibility for the Agency's physical and cyber infrastructure protection functions, while OSWER has emergency and remedial response obligations. OW is responsible for developing a water supply sector Critical Infrastructure Assurance Plan, and collaborating and coordinating efforts between the Federal government and the private sector. In addition, the CIO is responsible for the development and execution of the information-related elements of OEI's Mitigation Plan.

Other on-going reviews should also bring to light the effectiveness of EPA's actions thus far. For example, the OIG is currently evaluating EPA's implementation activities for protecting its critical, cyber-based infrastructure, under a review sponsored by the President's Council on Integrity and Efficiency regarding President Decision Directive (PDD) 63. Also, GAO is reviewing EPA's progress in protecting its critical cyber-based and physical infrastructures.

EPA does have separate staffs devoted to other security programs and these programs are under the authority of different Agency officials, as indicated by the Critical Infrastructure Protection Mitigation Plan. Based on the descriptions of the assigned responsibilities, the responsibilities do not appear to overlap or cause duplication of effort. Only one responsibility is shared by two offices - "Working with Human Resources to ensure requirement skills to support infrastructure protection program." The Agency assigned the Assistant Administrators for OARM and OSWER this responsibility, and we believe it represents a shared responsibility rather than a duplication of effort.

Question B.4 *Has the agency undergone a Project Matrix review? If so, describe the steps the agency has taken as a result of the review. If no, describe how the agency identifies its critical operations and assets, their interdependencies and interrelationships, and how they secure those operations and assets.*

The Agency has essentially concluded step one of the three-step Project Matrix process by developing a draft report identifying the Agency's critical assets under PDD 63. However, before the Project Matrix Step One Report can be finalized, it must undergo a quality assurance process to ensure that senior

executives agree with the findings. Once finalized, the Agency needs to complete vulnerability assessments and risk mitigation plans for its cyber-based assets. In addition, step two of the process needs to be officially authorized and implemented.

Question B.5 *How does the agency head ensure that the agency, including all components, has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities? Identify and describe the procedures for external reporting to law enforcement authorities and to the General Services Administration's Federal Computer Incident Response Center (FedCIRC).*

The Agency Head delegated to the CIO the responsibility for ensuring that EPA-documented procedures for reporting security incidents and shared information regarding common vulnerabilities exist. The CIO, in turn, delegated this responsibility to OEI's Director for Technology, Operations and Planning in June 2002.

EPA Directive 200.06, *Computer Security Incident Response*, dated January 31, 1996, is the Agency's official incident handling procedures document. In FY01, OEI indicated they were updating the Directive. Management subsequently decided to out-source the Incident Handling Program function. Due to this decision, they have given no date as to if and when they will revise Directive 200.06. OEI's Technical Information Security Staff (TISS) have been assigned the lead in developing the Incident Handling requirements that will be included in the OTOP contract.

EPA's Procedures for sharing information regarding common vulnerabilities within the agency are as follows:

1. TISS receives a FedCIRC and Computer Emergency Response Team Advisory and sends it to a supporting contractor.
2. Contractor performs analysis of the scope and impact of the advisory.
3. Contractor returns the advisory to TISS, and TISS distributes to manager of affected platform.
4. The platform manager distributes the advisory to the appropriate operational division for remedy.
5. The operational division reports back to TISS, confirming that the remedy has been taken.

The CIO does not directly report incidents to external law enforcement agencies. Instead, incidents with criminal ramifications are reported to the OIG's Computer Crimes Directorate (CCD). The CCD reports such incidents to external law enforcement authorities as they deem appropriate.

Although FedCIRC recommends real-time reporting, it has not promulgated any formal procedures for reporting security incidents. In the absence of specific criteria, TISS prepared and submitted an incident handling digest using data provided by EPA's NTSD. EPA discontinued submitting this digest at the end of September 2001, due to the lack of specific reporting requirements. As of July 2002, EPA resumed sharing a more condensed incident handling digest with FedCIRC.

Question C.1 *Have agency program officials: 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?*

A survey of EPA's program offices disclosed that only 80% of offices had completed risk assessments for all assets and operations under their control. Likewise, only 80% of EPA's program offices are either in the process of conducting or have completed testing and evaluating controls identified in the risk assessments. In our opinion, the 20% difference represents assets and systems that EPA did not label as "major applications" or "general support systems" for GISRA reporting purposes. These applications operate on the Agency's network and pose inherent security risks. As such, they should undergo risk evaluation, whether conducted by OEI or the responsible program office.

Program offices indicated they determined the level of security appropriate to protect operations and assets. However, as stated above, not all IT systems had undergone risk assessments or had approved security plans in place. We believe it is unlikely that adequate levels of security can be selected until the risk assessments are completed. As a result, major IT systems could be placed into operation without an adequate level of security and could be prone to operational manipulation due to inadequately designed internal controls. Representatives from OEI indicated that they instituted the NIST Self-Assessment tool for the fiscal 2002 review cycle, and that all program offices were to have completed the evaluation by July 2002. OEI plans to capture weaknesses from these risk assessments, incorporate them in a Plan of Actions & Milestones (POA&M), and track the milestones. Agency officials believe this approach will give them more reliable data on risk assessments.

Additionally, our fieldwork disclosed that EPA needs to do more to bring its system security plans into compliance with NIST requirements. We reviewed key data elements in EPA security plans and found that 21% of them were not comprehensively addressed to meet the standards set forth in NIST Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*. For example, some Security Plans did not:

- document the risk assessment methodology used to identify threats and vulnerabilities,
- document security activities required for its current phase, or
- describe contingency plan procedures.

This happened because EPA's security plan guidance predates revisions to NIST guidance and OMB A-130, Appendix III, which clearly describe and organize basic security plan requirements.

Question C.2 For operations and assets under their control, have agency program officials used appropriate methods (e.g., audits or inspections) to ensure that contractor provided services (e.g., network or website operations) or services provided by another agency for their program and systems are adequately secure and meet the requirements of the Security Act, OMB policy and NIST guidance, national security policy, and agency policy?

As of July 22, 2002, except for the Toxic Substances Control Act (TSCA) program, we had not identified any audits or inspections accomplished by Agency program officials to ensure that contractor-provided services or services provided by another agency for their program and systems were adequately secure and met regulatory requirements.

The TSCA program regularly audits/inspects contractors to verify that security standards are enforced. However, officials from EPA's Office for Prevention, Pesticides, and Toxic Substances stated that TSCA

is unique in that a law suit and court order require them to enforce security standards deemed by many to be more stringent than necessary.

Question D.1(1) Has the agency CIO adequately maintained an agency-wide security program?

While the agency has more work to do in this key area, they have issued or updated several security-related policies and procedures this fiscal year and plan to complete additional ones next year. We view policies and procedures as a critical element to maintaining an agency-wide security program that is:

- compliant with Federal regulations and standards, and industry best practices, and
- implemented consistently throughout all parts of the organization

As such, in responding to this question, we focused on the Agency's efforts to issue or update security-related policies and procedures. The Agency identified the following security-related policies and procedures that the CIO (through EPA's Office of Environmental Information) has issued or will issue in fiscal 2002 to adequately maintain agency wide security.

Completed in FY 02:

- LAN Operating Procedures (LOPS) 2002.
- Network and Infrastructure Procedures – new and revised procedures, along with links to the documents (described in deployment papers), for the Network can be found on the Network Infrastructure Services Support Web Page.
- EPA Order 2100.2A1, entitled *Information Technology Capital Planning and Investment Control*, dated 6/17/02. It revised an interim Order issued one month earlier.
- Standard Configuration Documents (SCDs) for the following Operating Systems:
 - T Sun Solaris 8.0
 - T RedHat LINUX 7.1
 - T Tru64 5.1

We found that all of the security-related policies and procedures identified as completed this fiscal year existed and were issued or updated as management indicated. In addition, with the exception of the Network and Infrastructure Procedures, we found that all of the security-related policies and procedures identified as completed this fiscal year were directly related to security.

With regard to the Network and Infrastructure procedures, we found that the Network Infrastructure Services Support Page does not differentiate whether the reason behind a service pack deployment is to correct a security shortcoming or to add other, non-security-related enhancements. This site provides a link to the LOPS, as well as to various deployment papers and service packs for software used by EPA, such as Corel Word Perfect, Lotus Smart Suite, Netware, Norton Anti-Virus, Windows, etc. The site includes a brief description and link to recent deployment papers, but these summaries do not specify whether a security shortcoming is the purpose for the specific upgrades or service packs described.

Currently Being Revised or Developed:

SCDs for the following Operating Systems are still in progress:

- T Sun Solaris 9.0
- T RedHat LINUX 7.2 & 7.3
- T Beowulf (LINUX) SCYLD
- T AIX 5L

The following policies and procedures are also under development:

- T Personal Use Policy
- T Systems Life Cycle
- T Personal Digital Assistants
- T Background Checks for Visitors
- T Updated Standards of Behavior

We were able to verify that all but one of the SCDs identified above were included on the SCD web page as “under development & review.” As of July 18, 2002, the only SCD not listed was the one for Beowulf (LINUX) SCYLD. The web page was last updated June 17, 2002. We could not verify the status of policies and procedures under development, as no web references or draft documentation were provided.

Question D.1 (2) Has the agency CIO ensured the effective implementation of the program and evaluated the performance of major agency components?

OEI is beginning to establish some security oversight for EPA’s complex information systems network. For several years, in conjunction with the Federal Managers’ Financial Integrity Act, the OIG has formally advised EPA to centralize its security program and establish strong oversight processes to adequately address risks and ensure the security of its information resources and environmental data. We found that OEI is performing some quality assurance and oversight activities to help ensure the effective implementation of the security program and to evaluate the performance of major agency components. However, we believe the Agency needs to focus more on independent verification, validation, and enforcement of the implementation of its security program.

OEI has accomplished very few oversight activities that independently verify and validate the implementation of the security program thus far this fiscal year. Three of the four FY02 oversight activities completed, as of July 30, 2002, were desk reviews of activities performed or information provided by program and regional offices. The three oversight activities were:

- performing completeness reviews of security plans for all CPIC systems.
- reviewing answers to security questions in CPIC systems and providing feedback on each submission as well as recommendations for improving responses.
- reviewing corrective action milestones submitted by program offices and regions to ensure they adequately addressed the identified weaknesses.

The fourth oversight activity focused on independent verification and validation. This activity was the monthly scan of UNIX and NT servers at the National Computer Center. Although OEI had completed very few oversight activities of this type by the end of our field work, they had identified five oversight activities which they are phasing in or planning to complete between July 30, 2002 and the end of FY03:

- **Testing a sample of EPA's Unix Servers.** OEI expects to issue a draft report by September 27, 2002, but has not indicated when the final report will be completed.
- **External Penetration Testing of Network.** Testing includes scans from external sites and war dialing. The draft report was issued on July 19, 2002. OEI did not include any planned date for the completion of the final report.
- **Quarterly Reports on Netware Servers.** Quarterly scans of attached servers determine their individual compliance with OEI-developed standards. OEI will issue quarterly status reports (score cards) to Assistant Administrators (AA) and Regional Administrators (RA). OEI is currently phasing-in this process to allow program and regional offices to get acclimated to the process and to provide a larger window for achieving full compliance.

The Agency is already seeing improvement in its compliance with the OEI-developed standards for Netware servers. We compared OEI's summary of EPA's weighted and curved compliance rates in January/February 2002 to the rates achieved in May/June 2002, and found that the Agency showed improvement in meeting Netware Server Standards. OEI applied several interim conditions while it phased in the quarterly reporting process:

- added reports to monitor standards not previously monitored.
 - weighted the percentage of compliance for new reports at half the weight of ongoing reports, thereby allowing offices to become acclimated to the process. ¹
 - graded on a curve to allow offices more leeway to work on bringing systems into compliance. For example, OEI counted a server as being compliant regarding system audit logs if it logged at least 40% of the events required in the OEI-developed standards.
 - only ran Bindview reports against approximately 95% of its Netware servers, and did not reconcile the list of servers against which they ran Bindview to the list of all of the Netware servers in the Agency's Novell Directory Services Tree. ²
- **Quarterly Scan of NT Servers.** In October 2002, OEI plans to begin performing a quarterly scan of all attached NT servers to determine compliance with OEI-developed standards.
 - **Comprehensive Review and Testing of Four System Security Plans.** OEI plans to complete this activity next fiscal year.

Concerns regarding Oversight Reviews: To improve feedback received through its oversight processes, we believe the Agency needs to set higher criteria for contractor-performed evaluations. For example, OEI hired a contractor to perform the Completeness Review of Security Plans for all the CPIC systems. OEI asked the contractor to perform the review based solely on the Agency's Information Security Planning Guidance (ISPG), dated June 17, 1997. OEI did not require the contractor to use

¹ Starting in August 2002, OEI stated it stopped weighting the compliance percentage.

² Since conclusion of audit field work, OEI stated it will run Bindview reports against all resources identified in the tree.

current Federal regulations, standards, and industry best practices as criteria. As such, the contractor's findings would not provide a completely accurate picture of the Agency's compliance with Federal requirements. As the contractor pointed out in their recommendations to the Agency, the ISPG needs to be brought into compliance with NIST.

We compared the OEI-developed Netware Standards: Netware Security Checklist to the latest LOPs (2002 version) and found that the LOPs does not contain all OEI-developed standards. OEI states that other Agency documents augment the LOPs, but we did not find evidence to support that all standards were formalized requirements within other approved Agency policies, directives, or orders. As such, regional and program offices are not required to conform their Netware security settings, even if future quality assurance reviews were to identify specific shortcomings.

Suggestions for Improvement: OEI should:

- (1) ensure that both in-house and contractor-performed reviews determine compliance using the following criteria:
 - current Federal regulations and standards,
 - industry best practices, and
 - additional requirements that EPA has instituted.
- (2) formally establish OEI-developed Netware Standards as official standards.

Quality Reviews for Risk-Based Performance Measures: OEI is currently developing risk-based performance measures that focus on outcomes rather than outputs. OEI provided a draft framework which they plan to use; however, it was still in the vision stage and did not contain specific details. Therefore, we did not have enough information to express an opinion on EPA's intended performance measures.

Our review, however, disclosed one concern regarding the process itself. In our opinion, EPA's process relies heavily on self-assessments and self-certifications, rather than on independent verification and validation. We believe that for the process to be successful in accurately measuring performance, it must include these additional components. Although such aspects were not part of the draft framework, OEI stated that it will apply some sort of quality assurance component. However, due to limited resources, OEI stated that it only will be able to verify a small portion of what it receives. OEI plans to accomplish its quality assurance plan in FY03.

Question D.1 (3) *Has the agency CIO ensured the training of agency employees with significant security responsibilities?*

The Agency cannot be assured that personnel with significant security responsibilities are sufficiently trained because management has not yet identified which EPA employees have such responsibilities. Once these personnel have been identified, EPA needs to assess security training needs based on assigned responsibilities. We noted that OEI does not track how many EPA employees receive specialized security training; program offices are expected to obtain and track this data.

The Agency provided web-based security awareness training to all EPA employees in August 2001. Although the Agency can track which employees have completed this training, OEI officials could not

verify to us that all EPA employees have taken the training. At this point, EPA does not have standardized procedures to ensure that new employees receive security awareness training.

OEI has plans for several security training initiatives. For example, OEI has a subscription with the Department of Transportation's Virtual University (TVU) to a library of IT security-related courses. Per OEI, these courses are aligned with NIST Special Publication 800-16. Approximately 50 EPA employees have begun taking these courses. For the balance of the calendar year, OEI plans to deploy: (1) the 2002 version of Information Security Awareness Training for all employees, (2) IT training sessions for executives and managers, and (3) security training (focused on NIST 800-16 requirements) for Information Security Officers (ISOs) through the TVU and the IRM College of the National Defense University. Also, in August 2002, OEI provided security training to ISOs during the annual ISO Forum.

Suggestion for Improvement:

To establish a robust and effective security training program, OEI should:

- identify personnel with significant security responsibilities, and
- assess security training needs for those personnel.

Question D.2 For operations and assets under their control (e.g., network operations), has the agency CIO used appropriate methods (e.g., audits or inspections) to ensure that contractor provided services (e.g., network or website operations) or services provided by another agency are adequately secure and meet the requirements of the Security Act, OMB policy and NIST guidance, national security policy, and agency policy?

The CIO has responsibility for a variety of contract services which support the Agency's enterprise network operations, network security, and systems development activities:

- National Computer Center (NCC),
- National Wide Area Network,
- Headquarters Local Area Network,
- TRI Reporting Center,
- Systems Development Center, and
- Central Data Exchange.

During fiscal 2002, the CIO took the following actions to ensure contractor-provided services were adequately secured and met the requirements of the Security Act:

- conducted modem-based penetration testing using a "war-dialer" technique at two key EPA locations: EPA Headquarters and the NCC;
- conducted Internet-based penetration testing against network assets located at the NCC;
- conducted a "completeness" review of security plans for major applications and general support systems identified in the CPIC proposals; and
- implemented a program to regularly monitor Novell Netware security settings and provide feedback to responsible EPA officials.

In our opinion, the CIO's actions seem appropriate for ensuring contractor services comply with the Security Act. However, at the end of field work, the penetration testing results were not finalized, so we

could not review OEI's POA&M associated with identified weaknesses. In our opinion, the CIO must work to finalize these results, and establish and monitor POA&Ms for identified weaknesses. Additionally, the CIO should develop and implement strategies to address concerns regarding oversight reviews identified in section D1.(2).

Question D.3 *Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were security requirements and costs reported on every FY03 capital asset plan (as well as in the exhibit 53) submitted by the agency to OMB? If no, why not?*

The Agency has not fully integrated security into the Agency's CPIC process. Although EPA has made significant improvements, weaknesses remain in the areas of policy guidance, quality assurance, and systems inventory.

- EPA's recently-enacted CPIC policy does not reference existing Agency security requirements. Although EPA's policy addresses security through a high-level reference to OMB Circular A-130, *Information Resources Management*, it does not reference existing Agency security policies. As it is written, the current CPIC policy does not include guidance with respect to integrating security into the CPIC process.
- EPA reported security costs for all projects on OMB Exhibit 53; however, EPA did not report security requirements on every FY03 capital asset plan submitted by the Agency to OMB. Of the 46 capital asset plans submitted to OMB, 11 (24%) lacked an approved security plan and 3 (7%) referenced security plans that had not been updated within the past three years. OEI explained that, at the time of submission, risk assessments had not been completed for the 11 proposals without security plans. In response to the draft report, OEI emphasized that the outstanding risk assessments have been completed, and stated that all 39 systems in the fiscal 2004 capital asset plan have security plans.
- In response to an OIG draft report entitled *EPA's Management of Information Technology Resources Under the Clinger-Cohen Act*, dated July 2, 2002, OEI indicated it will resolve the systems inventory issue by establishing an Information Resources Registry System that will contain all major and significant systems. The Agency expects to (1) complete prototype software for the Registry by the end of FY02, and (2) populate the database with actual data by the end of FY03.

STATUS OF GAO SECURITY RECOMMENDATIONS

We conducted follow-up work to determine EPA's progress in implementing recommendations contained in GAO's report: GAO/AIMD-00-122, *Information Security - Fundamental Weaknesses Place EPA Data and Operations at Risk*, dated June 2000. To date, we have reviewed 31 recommendations relating to the Unix Operating System and all 13 recommendations regarding Novell systems.

Status of Unix Recommendations:

During this review cycle, we evaluated 31 GAO recommendations related to Unix. We met with agency officials, analyzed system configuration files, and reviewed applicable network management policies and

procedures. Additionally, we selected a sample of servers critical to EPA's top-level architecture (i.e., Firewall, Intrusion Detection System, Domain Name Service, and Network Management Servers) and conducted limited confirmation testing using readily available network assessment tools.

In our opinion, EPA has taken appropriate steps to implement the GAO Unix recommendations. Based on system file reviews and confirmation tests, we found:

- servers were properly configured according to the vendor's instructions and GAO's recommendations.
- no security holes.

GAO recommendation number 71 required EPA to improve its incident handling practices. We found that EPA has made improvements in its incident handling practices, although we did not assess the efficiency and effectiveness of those practices. For example, EPA established sufficient policies to provide the overall direction for the incident handling program, and its ISOs have an understanding of their duties for reporting security incidents.

Status of Novell Recommendations :

As part of the 2001 GISRA review, we reviewed three of the 13 Novell (i.e., Netware) recommendations from GAO. These recommendations were fully implemented. During our 2002 GISRA review, we evaluated the status of the 10 remaining Novell recommendations. We reviewed a judgmental sample of EPA's regional and program offices to determine if management implemented GAO's recommendations or, at least, planned to establish compensating controls.

We used Bindview reports generated by OEI to assess the Agency's compliance with 6 of the 10 GAO recommendations. EPA uses Bindview reports in support of their overall network security program and these reports depict compliancy profiles with the majority of the OEI-developed Netware security standards, as well as most of GAO's recommendations. At that point in time, compliance was still being graded on a curve, as explained in our response to Question D.1(2) above.

In May 2002, OEI officials conducted assessments of the Agency's program and regional offices' compliance with OEI-developed Netware Security Standards. OEI concluded program and regional offices were 85.4% complaint with prescribed standards. We further analyzed these results for three program offices and three regional offices having the lowest compliance rates with the OEI-developed Netware standards. We limited our review to compliance with GAO recommendations and used the Bindview reports directly related to these recommendations. Our review indicated the six offices reached a compliance rate of 78.5% ³with GAO recommendations. OEI officials stated that any non-compliance by an individual office reflected on that particular office and should not be used to judge the merit of OEI's implementation program.

³For GAO recommendation 95, the percentage represents the compliance rate associated with the AuditCon feature enable for applicable servers, containers, and volumes, but does not represent compliance with logging of GAO recommended auditing events.

For the four recommendations where EPA chose not to implement GAO's recommendations, the Agency indicated they have established or planned to establish compensating controls to mitigate the associated risks. We did not test the adequacy of these controls or individual implementation plans.

EPA has improved network security among the regions and program offices by providing OEI-developed Netware standards and by monitoring most of these standards. OEI's standards for Netware include the majority of GAO's Novell recommendations. However, as discussed in our response to question D.1(2), these standards have not been formalized as an Agency requirement. The Agency's assessment of compliance with these standards, as captured in January/February 2002 and in May/June 2002, shows an increased overall compliance.

Suggestions for Improvement: OEI should:

- formalize standards into Agency policy and procedures, and assign accountability and identify consequences for non-compliance.
- perform follow-up monitoring for program and regional offices with poor compliance rates to ensure their respective management take corrective action within 30 days of notification. For substantive problems, planned corrective actions should be formalized under OEI's POA&M.

PLAN OF ACTION AND MILESTONES

To facilitate creation of the Agency plan of action, OEI's TISS prepared a standard approach for identifying, compiling, and tracking corrective actions. As a first step, TISS compiled a list of weaknesses for each Region and Program from the following sources:

- FY01 annual assessments,
- risk assessments completed during last 18 months,
- independent testing conducted on EPA's network-attached resources, and
- security plan reviews conducted last fiscal year.

TISS aggregated the list of detailed weaknesses into approximately 12 broad categories and developed standardized work plans for each category. Each EPA program and region was asked to: (1) verify the list of weaknesses; (2) add any additional weaknesses; (3) identify weaknesses already corrected; and (4) fill in dates for completing milestones of weaknesses not yet corrected. AA/RA's were asked to sign off on their respective Action Plan and submit it to the CIO with an electronic copy to TISS.

TISS captured the Agency's POA&Ms in a central project management database. TISS established a project management infrastructure that will assist the Agency in consolidating the individual POA&Ms into a comprehensive Agency action plan. A contractor, under TISS's direction, maintains a central database with all the work plans. TISS was requiring monthly updates from each program and regional office, but switched to quarterly updates after July 2002, to be consistent with OMB's schedule.

OMB requested that IGs verify that agency POA&Ms identify all known security weaknesses. As such, we randomly selected a contractor-performed review to verify that the weaknesses identified were included in the Agency's POA&M. We found that the Agency had not included the weaknesses identified in this review.

Suggestions for Improvement:

We believe that the collection and maintenance process needs to be modified to ensure that:

- all known weaknesses associated with any reviews performed by, for, or on behalf of the Agency are included.
- all known weaknesses, whether they are associated with a component of the Agency or the Agency as a whole, are included.

In addition, we believe that the process needs to include quality assurance/oversight to ensure that the corrective actions reported as completed are effective. We also believe that the Agency needs additional full-time staff with backgrounds in IT Security to adequately oversee the maintenance, monitoring, and oversight of the Agency's POA&Ms.