



U.S. Department of Justice

Office of the Inspector General

August 17, 2010

Subject: Freedom of Information/Privacy Act Request (FOIA)

I am writing in response to your March 4, 2006 request seeking audit reports produced by the Office of the Inspector General.

Enclosed please find two audit reports responsive to your request. After consulting with the DEA, it has been determined that portions of these reports are exempt from FOIA release pursuant to 5 U.S.C. §552(b)(6).

With regard to the remaining requested audit reports, the OIG is continuing to consult with other components regarding the releasability of the reports. We will inform you when we reach a final determination regarding those reports.

If you are dissatisfied with my action on this request, you may appeal by writing to the Director, Office of Information Policy (OIP), U.S. Department of Justice, 1425 New York Avenue, Suite 11050, Washington, D.C. 20530. Your appeal must be received by OIP within 60 days of the date of this letter. Both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal." In the event you are dissatisfied with the results of any such appeal, judicial review will thereafter be available to you in the United States District Court for the judicial district in which you reside or have your principal place of business, or in the District of Columbia, which is also where the records you seek are located.

Sincerely,

A handwritten signature in cursive script that reads "Deborah M. Waller".

Deborah Marie Waller

FOI/PA Specialist

Office of the General Counsel



LIMITED

OFFICIAL

USE

The attached information must be protected and not released to unauthorized individuals. Use of this cover sheet is in accordance with the Department of Justice regulation on the control of Limited Official Use information.

Audit Report



Summary of the
Independent Evaluation
Pursuant to the
Government Information
Security Reform Act
Fiscal Year 2001

Classified Systems

June 2002

02-21

LIMITED OFFICIAL USE

This report contains information that, if distributed widely, could compromise the law enforcement operations of the U.S. Department of Justice (DOJ). The information is considered Limited Official Use, as defined by DOJ Order 2620.7. Therefore, the report must be properly safeguarded to prevent publication or other improper disclosure.

**SUMMARY OF THE INDEPENDENT EVALUATION PURSUANT TO THE
GOVERNMENT INFORMATION SECURITY REFORM ACT
FISCAL YEAR 2001**

CLASSIFIED SYSTEMS

**OFFICE OF THE INSPECTOR GENERAL
EXECUTIVE SUMMARY**

The Government Information Security Reform Act (GISRA) required the Office of the Inspector General (OIG) to perform an independent evaluation of the U.S. Department of Justice's (Department's) information security program and practices. This report summarizes the results of the evaluation for the Department's classified systems for FY 2001. Separate reports were issued for each of the individual systems evaluated. The OIG is also issuing a report summarizing the results of the Department's sensitive but unclassified systems.

The OIG took an ambitious approach to fulfill the GISRA requirement by performing individual audits on a subset of Department systems. The OIG, in conjunction with Department management, selected four classified and five sensitive but unclassified systems to audit from the universe of Department systems for fiscal year 2001. Systems selected were mission critical and representative of differing system configurations (both client/server and mainframe) and operating systems (UNIX, Novell, and Windows NT).

Under the direction of the OIG and in accordance with Government Auditing Standards, KPMG LLP conducted the assessment of the Department's overall computer security program and practices for classified systems by performing individual audits on the four classified systems: the Drug Enforcement Administration's Merlin and El Paso Intelligence Center Information System (EIS), and the Federal Bureau of Investigation's administrative and investigative mainframes (A&IM)¹.

The audits consisted of interviews, on-site observations, and reviews of Department and component documentation to assess the system and component compliance with GISRA and related information security policies, procedures, standards, and guidelines. Commercial off-the-shelf and proprietary software were used to conduct security tests and analyses of significant operating system integrity and security concerns.

¹ The FBI's administrative and investigative mainframes are two separate systems that were reported jointly.

The classified system audits revealed vulnerabilities with management, operational, and technical controls. The auditors assessed the vulnerabilities at a high to moderate risk to the protection of each system and the data stored on it from unauthorized use, loss, or modification. Specifically, vulnerabilities were noted in the following areas:

Audit Results of Classified Systems				
Areas of Vulnerability	Control Type	System		
		MERLIN	EIS	A&IM
Security Policies and Procedures	Management	✓	✓	✓
Department Oversight	Management	✓	✓	✓
Physical Controls	Operational	✓		*
Backup and Restoration Controls	Operational	✓	✓	✓
Software Upgrade Controls	Operational	✓		✓
Personnel Controls	Operational	✓		
Password Management	Technical	✓	✓	✓
Logon Management	Technical	✓	✓	✓
Account Integrity Management	Technical	✓	✓	✓
System Auditing Management	Technical	✓	✓	✓

* We found physical controls in place at the facilities visited, but also found a significant individual deficiency at the FBI headquarters that warranted specific reporting.

We concluded that the vulnerabilities with technical controls, assessed by conducting penetration tests², were the most significant. All four systems had password vulnerabilities and were compromised during penetration testing. Overall, the vulnerabilities identified were more voluminous and material for the Department's classified systems than for its sensitive but unclassified systems. The audit disclosed that the Department did not make the same commitment to testing its classified systems as it did on its sensitive but unclassified systems.

The audits also found that Department-level and component security policies and procedures were either insufficient or unenforced. The auditors concluded that the Department did not provide timely and effective oversight of classified systems. For example, the Department took nearly four years to revise its overall security policy, DOJ Order 2640.2D, "Information Technology Security," after we reported it as ineffective in September 1997. The Department also did not regularly test its classified systems, hold

² A penetration test is a security test in which evaluators attempt to circumvent the security features of a system and gain entry based on their understanding of the system design and implementation.

components responsible for taking corrective action on previously identified vulnerabilities, or enforce its own policy on certification and accreditation.

To address these deficiencies, we recommend granting responsibility to a single point of contact in the office of the Assistant Attorney General for Administration to oversee, standardize, implement, and maintain strict baseline Department-wide security controls over both classified and sensitive but unclassified systems. This contact also would serve as a liaison between the Information Management and Security Staff, the Security and Emergency Planning Staff, and the Assistant Attorney General for Administration. To ensure uniform system security, we also recommend more specific guidance through revisions to the Department's security policy and the development of additional procedures. Our recommendations include:

- enforce Department security policies at each component such as passwords, account lockout, and system auditing management;
- ensure that all components have current, documented, and tested contingency plans;
- develop a comprehensive corrective action plan to address weaknesses previously identified;
- ensure periodic computer security training is provided for each platform supported;
- ensure systems' security is monitored sufficiently, efficiently, and consistently, including:
 - a) automated monitoring of security policy compliance and auditing of security relevant events;
 - b) requiring intrusion detection testing and application and operating system patches be kept current.
- ensure that periodic updates supplement DOJ Order 2640.2D based on observed component needs, the evolving computer security environment, and industry best practices.

TABLE OF CONTENTS

INTRODUCTION	1
FINDINGS AND RECOMMENDATIONS	3
I. MANAGEMENT CONTROLS.....	3
Security Policies and Procedures.....	4
Department Oversight.....	5
II. OPERATIONAL CONTROLS.....	6
Physical Controls	6
Backup and Restoration Controls	7
Software Upgrade Controls	8
Personnel Controls.....	8
III. TECHNICAL CONTROLS.....	9
Password Management.....	9
Logon Management.....	10
Account Integrity Management.....	11
System Auditing Management	11
CONCLUSION AND RECOMMENDATIONS	12
APPENDIX I - BACKGROUND.....	16
APPENDIX II - OBJECTIVE, SCOPE, AND METHODOLOGY.....	18
APPENDIX III - AAG/A RESPONSE TO THE DRAFT REPORT.....	19
APPENDIX IV - OIG'S RESPONSE TO DEPARTMENT'S COMMENTS TO OVERALL REPORT	25
APPENDIX V - OIG, AUDIT DIVISION ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT	29

INTRODUCTION

The fiscal year 2001 Defense Authorization Act (Public Law 106-398) includes Title X, subtitle G, "Government Information Security Reform Act" (GISRA). GISRA became effective on November 29, 2000, and amends the Paperwork Reduction Act of 1995 by enacting a new subchapter on "Information Security." It requires federal agencies to:

- Have an annual independent evaluation of their information security and practices performed.
- Ensure information security policy is founded on a continuous risk management cycle.
- Implement controls that assess information security risks.
- Promote continuing awareness of information security risks.
- Continually monitor and evaluate information security policy.
- Control effectiveness of information security practices.
- Provide a risk assessment and report on the security needs of the agencies' systems, and include the report in their budget request to the Office of Management and Budget (OMB).

In January 2001, the OMB issued guidance on implementing GISRA. The Office of the Inspector General (OIG) began its GISRA audits in April 2001. In June 2001, the OMB issued "Reporting Instructions for the Government Information Security Reform Act," requiring the submission of an executive summary, including a section characterizing the results of the OIG independent evaluation, by September 10, 2001. The OIG coordinated its GISRA work with the Department to promote communication and avoid duplication as the Department concurrently conducted program reviews to fulfill its GISRA obligations. The OIG also held briefings to keep Department and component management apprised of the audit results.

The OIG contracted with KPMG LLP to conduct the assessment of the overall computer security program and practices for the Department's classified systems. The objective of the audits was to determine the Department's compliance with the requirements of GISRA. To accomplish this objective, individual audits were performed on four classified systems chosen by the OIG in consultation with Department management: the Drug Enforcement Administration's Merlin and El Paso Intelligence Center Information System, and the Federal Bureau of Investigation's administrative and investigative mainframes.

The auditors reviewed management, operational, and technical controls by interviewing component management personnel, reviewing system documentation, and performing testing. The audits were performed in accordance with Government Auditing Standards and were conducted between April and August 2001. The audit approach was based on the General Accounting Office's Federal Information System Control Audit Manual, the Chief Information Officer Council Framework, and guidance established by the National Institute of Standards and Technology.

The OIG has routinely performed computer information security audits within Department components. Since 1996, we have also reviewed computer security program requirements annually as part of the financial statement audit process. For the GISRA audits, special emphasis was placed on reviewing vulnerabilities previously identified and verifying that appropriate corrective measures were implemented.

The GISRA audits of classified systems revealed vulnerabilities with management, operational, and technical controls. The auditors assessed these vulnerabilities at a high to moderate risk to the protection of each system and the data stored on it from unauthorized use, loss, or modification. In assessing technical controls, penetration tests identified user accounts and passwords that allowed the auditors access to the system. These tests demonstrated that systems were susceptible to unauthorized access and that entry to seemingly harmless areas can jeopardize the security and integrity of entire systems.

The Department's Justice Management Division (JMD) Security and Emergency Planning Staff (SEPS) is responsible for providing guidance on security issues related to the Department's classified systems. This includes monitoring components' compliance with the provisions of the Department's security policy and applicable Federal statutes, policies, and regulations as they apply to classified computer systems. The Department's JMD Information Management and Security Staff, which is similarly responsible for sensitive but unclassified systems, had conducted network security penetration testing at Department components for the past four years. However, SEPS did not have a similar program established for testing classified systems.

A summary of the individual audit results previously reported is detailed in the Findings and Recommendations section of the report. Appendices I and II provides background on the systems selected and the objective, scope, and methodology for the audit.

FINDINGS AND RECOMMENDATIONS

The Department's computer security program needs improvement to fully protect its classified systems from unauthorized use, loss, or modification. Audits of four classified systems disclosed vulnerabilities in management, operational, and technical controls for each system reviewed. Department-level and component security policies and procedures were insufficient or unenforced. The Department did not adequately: (1) identify and assess risks to determine needed security measures, (2) establish and implement policies and controls to meet those needs, (3) promote awareness so that users understand the risks and the related policies and controls required to mitigate them, or (4) monitor and evaluate established policies and controls to ensure that they were both appropriate and effective.

I. MANAGEMENT CONTROLS

Management controls are techniques and concerns normally addressed by officials with responsibility for an organization's computer security program. In general, these controls manage the computer security program and the risk within the organization.

Security policies, procedures, standards, and guidelines are the primary means by which management communicates goals and requirements. To be effective, compliance must be overseen and enforced. The related policies should encompass all major systems and facilities. The policies should outline the duties of those who are responsible for overseeing security as well as those who own, use, or rely on the entity's computer resources.

The Department did not provide timely and effective oversight of classified systems, hold components responsible for taking corrective action on previously identified vulnerabilities, or enforce its own policy on certification and accreditation. Further, the Department did not make the same commitment to testing its classified systems as it did its sensitive but unclassified systems. Specifically, our audits disclosed vulnerabilities with management controls as shown below:

Area of Vulnerability	MERLIN	EPIC	A&IM
Security Policies and Procedures	✓	✓	✓
Department Oversight	✓	✓	✓

Security Policies and Procedures

The Department established uniform policy for the protection of its automated information systems with DOJ Order 2640.2C, "Telecommunications and Information System Security," dated June 25, 1993. Despite the rapid evolution of computer technology, this policy remained in effect and unchanged, governing the Department's information systems security environment for eight years. In a September 1997 audit, Report No. 97-26, "Computer Security at the Department of Justice," the OIG noted the Order's shortcomings and recommended that the Department develop effective computer security program guidance. However, the Department did not revise its policy, DOJ Order 2640.2D, "Information Technology Security," until four years later, in July 2001.

Although DOJ Order 2640.2D addresses many areas of identified system security vulnerabilities, the guidance for the protection of Department information systems remains insufficient. The Order imposes minimal standards that are broadly stated, allowing components and system security managers too much latitude in establishing system settings. To ensure uniform system security, DOJ Order 2640.2D needs more specificity in the following areas:

- password management (including task versus user accounts);
- accountability and audit trails;
- access controls;
- account integrity management, including monitoring of account disposition (dormant accounts);
- logon management;
- service accounts - changing the default password;
- assignment of user rights and advanced user rights;
- renaming guest and administrative accounts; and
- backup procedures.

Department-level guidance regarding the adequate, efficient, and consistent monitoring of classified systems' security is also lacking. Specific areas that should be immediately addressed include:

- automating monitoring of security policy compliance;
- automating logging, auditing, review and notification of security relevant events;

- requiring intrusion detection testing; and
- requiring timely software patch application.

The auditors also found that component and system-level security policies were ineffective and applied inconsistently on all four systems audited:

- A security operating procedures guide was not finalized for one system that had been operating since early 1998.
- One component was not following its automated data processing and telecommunications security policy.
- A security plan for one system was dated January 2000, but remained unapproved by the component Security Program Manager.
- Two systems' "Rules of Behavior" were not distributed and acknowledged by the user community.
- At one component, annual computer security refresher courses were not held for employees as required. Some employees had not received annual computer security refresher training for over seven years.
- At one component, two of the five critical levels assigned to mainframe systems applications were not defined. The criticality of system applications definitions is an essential factor in risk management.

These vulnerabilities occurred because Department and component management did not develop or enforce formal data security policies and procedures.

Department Oversight

The Security Program Operating Manual (SPOM) documents the Department's requirements and procedures specific to safeguarding classified information. The Department did not provide timely and effective oversight of classified systems security by enforcing the SPOM and holding components responsible for taking corrective action on previously identified vulnerabilities. Specifically our audits revealed:

- Vulnerabilities identified in previous reviews of all four systems were not corrected. For one component, reports were not distributed to personnel responsible for correcting the vulnerabilities.
- Security vulnerabilities previously reported continued to exist for one component for as long as five years.

The Department also did not enforce its policy on certification and accreditation. All four systems operated without appropriate accreditation:

- One system network was accredited without complete certification and accreditation documentation.
- One system operated under an interim approval.
- Two systems were self-certified, but unaccredited by the designated approval authority.

Although the SPOM allows for interim approval to operate prior to accreditation, the Department did not follow up to ensure timely receipt of final accreditations.

II. OPERATIONAL CONTROLS

Operational controls address security controls that are implemented and executed by people to improve the security of a particular system, often require technical or specialized expertise, and rely upon management activities as well as technical controls. The audits identified vulnerabilities with operational controls as shown below.

Area of Vulnerability	MERLIN	EPIC	A&IM
Physical Controls	✓		*
Backup and Restoration Controls	✓	✓	✓
Software Upgrade Controls	✓		✓
Personnel Controls	✓		

* We found physical controls in place at the facilities visited, but also found a significant individual deficiency at the FBI headquarters that warranted specific reporting.

Physical Controls

Physical controls protect the computer facility – the building, systems room, computer workstations, and storage media. Moreover, physical controls protect the computing equipment and the sensitive information stored on the equipment from damage and theft. Department policy requires that sensitive computer systems facilities be secured in a manner commensurate with the risk.

For the four systems audited, we found:

- Access to an unattended telecommunications wiring closet increased the risk of unauthorized access to systems resources. Although housed in a secure facility, the wiring closet was accessible to anyone with access to the building. As a result, employee or contractor personnel could employ a tool to intercept unencrypted network traffic from multiple offices on that floor as it passed through the devices in the closet.
- The procedure at one facility for maintaining an approved personnel list for recording access to sensitive computer areas was ineffective, increasing the risk of unauthorized access to system resources.
- One component did not enforce procedures for safeguarding removable hard drives, exposing information to unauthorized disclosure, destruction, or modification. An unattended hard drive could easily be hidden in a pocket and is therefore subject to the risk of unauthorized removal from the premises.

Although the open wiring closet and the unattended hard drive were located at secure sites, relatively isolated security lapses such as these cannot be discounted because they circumvent access controls put in place to protect sensitive information. The risk of systems compromise by insiders and "trusted" personnel must also be seriously considered. The Director of the FBI's National Infrastructure Protection Center has previously stated before the Senate Judiciary Committee Subcommittee on Technology and Terrorism that "the disgruntled insider" is a principal source of computer crimes. He stated, "The 1999 Computer Security Institute/FBI report notes that 55% of respondents reported malicious activity by insiders."

Backup and Restoration Controls

System backup procedures, including backup tapes, protect information resources, minimize the risk of unplanned interruptions, allow for the recovery of critical operations when interruptions occur, and ensure on-going availability of critical systems operations. Not testing a contingency plan or effectively training employees in the restoration process jeopardizes the continuation of critical missions and business functions in the event of an emergency.

The collective vulnerabilities with backup and restoration controls noted in the four system audits are as follows:

- Critical data, operations, and resources were not identified and prioritized.

- Documented contingency plans and procedures were inadequate and untested.
- Weaknesses affecting system and network backup and restoration controls identified in previous reviews were not corrected.
- One system continuously operated at nearly full capacity, increasing the likelihood of unexpected loss due to disruptions in service.

These vulnerabilities were attributed to both the Department and components not enforcing compliance with existing policies or taking necessary steps to ensure contingency testing and recovery planning needs were addressed.

Software Upgrade Controls

Software requires frequent upgrades to mitigate system vulnerabilities. These software upgrades include applying manufacturer supplied patches to operating systems and applications to repair or correct known system vulnerabilities. Virus protection software must also be updated frequently to prevent infections that lead to disrupted service.

Three of the four systems audited had one or more of the following vulnerabilities:

- Virus protection software was outdated.
- Documented operational patch processes were bypassed or neglected.
- Patches to correct known security vulnerabilities were never installed. A similar condition was reported in a previous audit but had not been corrected.

Personnel Controls

Persons with access to computer systems must have security clearances commensurate with the highest level of information processed by the systems. The SPOM requires that persons with access to classified information must, at a minimum, be approved to access information at the secret level. For one of the four systems audited, we found:

- One person without an appropriate security clearance was allowed access to a system's Open Storage area. Although access with an escort is permissible according to DOJ Order 2640.2C, allowing uncleared persons the ability to access classified information increases the risk of unauthorized access, misuse, or abuse of classified data.

III. TECHNICAL CONTROLS

Technical controls focus on the security controls the computer system executes and depend upon the proper functioning of the system for their effectiveness. Technical controls require significant operational considerations and should be consistent with the organization's security management.

The auditors assessed the effectiveness of technical controls by using commercial-off-the-shelf and proprietary software to conduct penetration tests of the systems. Penetration tests can reveal existing security deficiencies, assess their severity, and prescribe remedies to prevent unauthorized exploitation.

The audits identified vulnerabilities with technical controls as shown in the table below:

Area of Vulnerability	MERLIN	EPIC	A&IM
Password Management	✓	✓	✓
Logon Management	✓	✓	✓
Account Integrity Management	✓	✓	✓
System Auditing Management	✓	✓	✓

These vulnerabilities existed because the Department and component security management did not formalize and develop effective security policies or enforce compliance with existing password, logon, account integrity, and system auditing management policies. The Department has conducted regular network security penetration testing on sensitive but unclassified systems for the past four years but did not have a similar program established for testing classified systems. Thus, we concluded that the technical control vulnerabilities identified for the classified systems were more egregious than the sensitive but unclassified systems because the classified systems were not subject to the same frequency of external reviews.

Password Management

A password is a unique string of characters that must be provided before access is authorized to a computer system. Passwords are security measures used to restrict logons to user accounts and access to computer systems and resources. Department policy requires security safeguards to ensure that each person with access to a computer system is individually accountable for his or her actions on the system, and that each user has a unique user-id and password. Password vulnerabilities permit access to unauthorized personnel and expose system resources to theft, loss, or modification.

For the four systems audited, we found:

- All four systems were compromised during penetration testing. Network services and devices with easily guessed passwords were compromised on one system; an administrator account with an easily guessed password provided access to two systems, enabling auditors to identify additional user accounts and passwords; and auditors were able to logon to a system after determining that a system administrator's password was identical to the user name.
- All four systems included one or more of the following password vulnerabilities: accounts without passwords; easily guessed passwords; no minimum password length requirement; passwords that did not expire; or passwords equivalent to the account name. These password vulnerabilities increase the likelihood that passwords will be guessed.
- Three systems had password management vulnerabilities similar to those identified in previous reviews.

Logon Management

The first line of defense against unauthorized user access is an interactive logon process. The process usually begins with a warning banner, informing the user of the proper use of computers on the network. Next, the user is presented with a request for the user's information such as the user name, password, and the server or domain the user intends to access. If the user's information is entered incorrectly, the system returns a logon failure message and, after a predetermined number of failed attempts, locks out the user for a specified period of time. If the user's information is entered correctly, the system authenticates the user by matching the user's information with an account in the system's security database.

For the four systems audited, we found:

- All four systems utilized inadequate user authorization procedures or lacked periodic reviews to verify the appropriateness of user access, resulting in potential access by someone who no longer had a legitimate need to access the system.
- All four systems had inactive accounts, increasing administrative overhead burden.

- Three of the four systems had the lockout option inappropriately set, permitting an unlimited number of logon attempts and increasing the likelihood of unauthorized system access through password guessing.
- On two of the four systems, auditors were able to gain access to a network server, an application, and a network switch, increasing the risk of unauthorized access to system resources.
- Three of the four systems had logon management vulnerabilities similar to those identified in previous reviews.

Account Integrity Management

A system administrator manages user and account rights to ensure that account information conforms to system security policy. A system of user rights and advanced user rights control account integrity. User rights define what a user can do on the system. These rights may include the right to logon directly at a computer (local logon) or the right to logon to a computer over the network (remote logon). Advanced user rights are generally reserved for users involved in programming efforts.

For the four systems audited, we found:

- Three systems did not have a formal, well-defined software change control mechanism, which could permit inaccurate or unauthorized program changes.
- Three of the four systems had account integrity vulnerabilities similar to those identified in previous reviews.
- All four systems granted user rights in excess of the user's responsibilities, resulting in segregation of duty conflicts and increasing the potential that fraudulent activity will go undetected.
- One system had multiple servers running services that allowed unrestricted access to sensitive services and information, increasing the likelihood of unauthorized access to system resources using known security vulnerabilities of those services.

System Auditing Management

Auditing can provide the ability to detect and record security-related events. It tracks the activities of users by recording information in a security log on the server about specific types of events, such as logon and logoff, file and object access, use of user rights, user and group management, security policy changes, restart, shutdown, and system events.

We found that the system auditing performed on all four systems was deficient and audit logs were not periodically reviewed. Specifically, our GISRA audits disclosed:

- Two systems had system auditing management vulnerabilities similar to those identified in previous OIG audits.
- Two systems did not have auditing enabled for all volumes and containers.
- One system had insufficient computing resources, restricting its capability to perform auditing.
- One system did not capture an audit trail for changes to sensitive Windows NT registry file directories.

CONCLUSION AND RECOMMENDATIONS

The GISRA audits of classified systems revealed vulnerabilities with management, operational, and technical controls. The auditors assessed these vulnerabilities at a high to moderate risk to the protection of each system and the data stored on it from unauthorized use, loss, or modification. Specifically, vulnerabilities were noted in the following areas:

Audit Results of Classified Systems				
Areas of Vulnerability	Control Type	System		
		MERLIN	EIS	A&IM
Security Policies and Procedures	Management	✓	✓	✓
Department Oversight	Management	✓	✓	✓
Physical Controls	Operational	✓		*
Backup and Restoration Controls	Operational	✓	✓	✓
Software Upgrade Controls	Operational	✓		✓
Personnel Controls	Operational	✓		
Password Management	Technical	✓	✓	✓
Logon Management	Technical	✓	✓	✓
Account Integrity Management	Technical	✓	✓	✓
System Auditing Management	Technical	✓	✓	✓

* We found physical controls in place at the facilities visited, but also found a significant individual deficiency at the FBI headquarters that warranted specific reporting.

Overall, our audits found that Department-level and component security policies and procedures were either insufficient or unenforced. The Department did not provide timely and effective oversight of classified

systems, regularly test its classified systems, hold components responsible for taking corrective action on previously identified vulnerabilities, enforce its own policy on certification and accreditation, or inform users of the risk and the controls to mitigate them.

~~Based on the security deficiencies and concerns disclosed as well as the repeat nature of many of them, we recommend a proactive approach to improving security controls over classified Department systems. Our recommendations are intended to create a framework of checks and balances within the Department to prevent, or quickly detect and address, security control deficiencies at the component level.~~

We conclude that a central office with responsibility for system security is needed to identify trends and enforce uniform standards. We believe that a central office would concentrate resources (time, money, and expertise) to identify and correct system security vulnerabilities most significant to the Department more effectively. Moreover, baseline security safeguards and controls should not vary according to the classification of system data, although data sensitivity might warrant additional or increased measures of protection.

Senior management benefits from having a single point of contact responsible for overseeing activities that standardize, implement, and maintain strict, baseline Department-wide security controls over both types of systems. This office would also serve as a liaison between the Information Management and Security Staff, the Security and Emergency Planning Staff, and the Assistant Attorney General for Administration (AAG/A).

Therefore, we recommend that the AAG/A:

1. Establish a Department Information Technology (IT) Central Security Compliance Office for classified and sensitive but unclassified systems with the responsibility for:
 - a. Monitoring security-related activities by testing controls at each component having classified systems (performing penetration tests and providing those results to the affected components).
 - b. Reviewing the number and types of security deficiencies identified in each component's periodic reports.
 - c. Evaluating each component's compliance with Department security policies, especially in areas of reported weaknesses, and establishing processes and procedures to enforce existing policy such as passwords, account lockout, and system auditing management.

- d. Assisting component Security Program Managers in assessing security risks, identifying hardware/software security deficiencies, and providing policy and procedural guidance as needed.
2. Charge the Department IT Central Security Compliance Office with ensuring that all components have current, documented, and tested contingency plans.
 3. Charge the Department IT Central Security Compliance Office with developing a comprehensive corrective action plan to fully and timely address all Department-wide IT control weaknesses previously identified in security reviews and audits. Additionally, measures should be prescribed and oversight provided to ensure that component corrective action plans are prepared and that vulnerabilities are corrected. Eliminating repeat findings should be a priority.
 4. Require each component Security Program Manager to:
 - a. Have full knowledge of and familiarization with current Department information technology security policies and procedures, including DOJ Order 2640.2D and other departmental policies related to classified and unclassified systems.
 - b. Report component compliance with Department security policy requirements.
 - c. Ensure a security administrator is designated within each component for reviewing system security posture in accordance with Department security policy. In the case of multiple platforms or operating systems supporting component systems, an administrator should be designated to represent each unique platform.
 - d. Ensure periodic computer security training is provided for each platform supported and require attendance by the designated security administrators.
 - e. Develop and enforce security policies or apply industry best practices, to assess and counter evolving computer security vulnerabilities.
 5. Require each component Security Program Manager to periodically report to the Department IT Central Security Compliance Office on the compliance of individual systems within their component relative to requirements outlined in Department security policies and procedures. Upon its review of the reports, the Department IT Central Security Compliance Office should bring areas of concern to the attention of the AAG/A.

6. Establish and implement guidance to ensure systems' security is monitored sufficiently, efficiently, and consistently. Specific areas that need to be addressed include:
 - a. automated monitoring of security policy compliance;
 - b. automated logging, auditing, review and notification of security relevant events;
 - c. requiring intrusion detection testing; and
 - d. requiring application and operating system patches be kept current.

JMD stated that they have addressed some of the above areas after the completion of our audit fieldwork. Moreover, although DOJ Order 2640.2D addresses many areas of identified system security vulnerabilities, it still lacks sufficient guidance in several areas. The policy should be specific to each operating system (Windows NT, Novell, and UNIX) so that the requirements are not misunderstood or inappropriately applied; that is, some procedures may apply to Windows NT systems but not to UNIX systems. Further, procedures should be developed to provide more specific guidance when necessary.

Therefore, we recommend that the AAG/A:

7. Ensure the periodic update and supplementing of DOJ Order 2640.2D based on observed component needs, the evolving computer security environment, and industry best practices. We recommend that the AAG/A promptly review the adequacy of guidance for the following areas:
 - a. password management (including task versus user accounts);
 - b. accountability and audit trails;
 - c. access controls;
 - d. account integrity management, including monitoring of account disposition (dormant accounts);
 - e. logon management;
 - f. service accounts - changing the default password;
 - g. assignment of user rights and advanced user rights;
 - h. renaming guest and administrative accounts; and
 - i. backup procedures.

BACKGROUND

KPMG LLP conducted the assessment of the Department's overall computer security program and practices for classified systems by performing Individual audits on four classified systems: the Drug Enforcement Administration's Merlin and El Paso Intelligence Center Information System (EIS) and the Federal Bureau of Investigation's administrative mainframe and investigative mainframe.

The Drug Enforcement Administration (DEA)

The mission of the DEA is to enforce controlled substances laws and regulations of the United States and investigate organizations and individuals that grow, manufacture, or distribute controlled substances. The DEA also recommends and supports non-enforcement programs that attempt to reduce the availability of illicit controlled substances worldwide.

Merlin

Merlin is a classified system at the secret level used by DEA intelligence analysts and agents to access and analyze classified information obtained from sources within DEA and other federal agencies. Merlin is an interactive tool used on cases and major investigations. Merlin is essential to the real time transmission of classified information within DEA. The system was designed to help improve coordination, speed analysis, enable data integration, and support the production of charts, graphs, and other analytical products. Approximately 600 users within DEA headquarters in Arlington, Virginia, and at DEA field offices access Merlin. A compromise of the system can jeopardize an investigation or agent safety. The Merlin Data Center is located in a certified Open Storage Area. Open Storage Areas are constructed when the volume of bulk classified material is such that the use of security containers is not practical.

EIS

The mission of the El Paso Intelligence Center (EPIC) is to support United States law enforcement and interdiction activities through the timely analysis and dissemination of intelligence on illicit drug and alien movements and criminal organizations responsible for these illegal activities. EPIC is under the direct line authority of the DEA and is comprised of senior law enforcement representatives from 15 federal and several state agencies. Overall coordination and management of activities at EPIC is the responsibility of the EPIC Director.

The EPIC Information System (EIS) processes multiple types of data including historical intelligence, tactical, administrative, and office automation ranging in sensitivity from law enforcement sensitive to secret high.³ The EIS is partitioned into classified and unclassified sections that operate separately from one another. The EIS is a mission critical operation that limited EPIC personnel accesses 24 hours a day, seven days a week. The EIS was designed to collect, process, and disseminate intelligence information concerning illicit drug activity, currency movement, alien smuggling, weapons trafficking, and other illegal related activities.

The Federal Bureau of Investigation (FBI)

The FBI Headquarters Data Center and the Information Resources Division Investigative Application Facility (IRDIAF) provide the mainframe systems support for the FBI. The mainframes host critical applications that support the FBI headquarters and field offices through the FBI wide area network and local area network (WAN/LAN). The FBI WAN/LAN provides systems users with secure communications.

Administrative Mainframe

Administrative applications are essential to the FBI's mission and allow the FBI to process forfeited and seized property for civil and judicial cases, perform background investigations, generate crime statistics, manage the Criminal Informant Program, and administer agent firearms qualification requirements. Additionally, the FBI uses them to manage its personnel, financial, and fiscal resources. The mainframe housing the administrative applications is located in the FBI Headquarters Data Center.

Investigative Mainframe

The IRDIAF, located in the FBI's Clarksburg, West Virginia, Data Center, houses the mainframe that maintains the FBI's investigative applications. Investigative applications assist special agents and support analysts in their daily activities supportive of the FBI mission to: uphold the law through the investigation of violations of federal criminal law; protect the United States from foreign intelligence and terrorist activities; and provide leadership and law enforcement assistance to federal, state, local, international agencies.

³ "Secret high" is a DEA sensitivity rating.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of the audits was to determine the Department's compliance with the requirements of the Government Information Security Reform Act (GISRA). In doing so, we assessed whether adequate computer security controls existed to protect Department systems from unauthorized use, loss, or modification. To accomplish the objective, we reviewed management, operational, and technical controls for a subset of Department systems. This report summarizes the audit results of the four classified systems reviewed.

We interviewed component and system management personnel, reviewed system documentation, and performed testing to determine compliance with Department and component security policies and procedures. The audits were performed in accordance with Government Auditing Standards and took place from April through August 2001. The effectiveness of security controls was assessed by using commercial off-the-shelf and proprietary software to conduct penetration tests of the system.

The audit approach was based on the General Accounting Office's Federal Information System Controls Audit Manual, the Chief Information Officer Council Framework, OMB Circular A-130, and guidance established by the National Institute of Standards and Technology.

AAG/A RESPONSE TO THE DRAFT REPORT



U. S. Department of Justice

Washington, D.C. 20530

APR 12 2002

MEMORANDUM

TO: Glenn A. Fine
Inspector General

FROM: Robert F. Diegelman
Acting Assistant Attorney General
for Administration

Vance Hitch
Chief Information Officer

SUBJECT: Comments on the Office of Inspector General's Draft Audit
Reports – Summary of Classified and Unclassified Systems

This is in response to the Office of the Inspector General's (IG) request for comments on draft Fiscal Year 2001 audit reports of classified and sensitive but unclassified information systems pursuant to the Government Information Security Reform Act (GISRA).

As you know, the Attorney General (AG) recently appointed a new Chief Information Officer (CIO). We have had several meetings concerning the Department's information technology (IT) security program, and we acknowledge the need to improve the Department's IT security program. The IG report addresses certain deficiencies that need correction, especially in the areas of system-specific technical and operational security controls, and we intend to strengthen computer security throughout the Department. For purposes of this response, we have divided our comments into three sections: comments on the Draft Audit Report for Sensitive But Unclassified IT Systems, comments on the Draft Audit Report for Classified IT Systems; and responses to the IG recommendations.

Draft Audit Report for Sensitive But Unclassified IT Systems

We have reviewed the draft audit report, Summary of Sensitive But Unclassified Systems, and have no comments.

Glenn A. Fine

Draft Audit Report for Classified IT Systems

We have reviewed the draft audit report and, as a preliminary matter, we note that no one from the Security and Emergency Planning Staff (SEPS) was interviewed as part of this audit. SEPS has security oversight of classified IT systems and reports to the Assistant Attorney General for Administration (AAG/A) through the Deputy Assistant Attorney General for Law and Policy and, therefore, must be consulted in assessing any classified systems' compliance with the GISRA and related information security policies.

In addition, we are providing the following comments for clarification to the findings of the draft summary report.

1. **IG Finding:** Management did not conduct penetration testing on its classified systems.

Comment: At the request of the Department, the National Security Agency (NSA) conducted penetration testing on two of the four IG-audited classified systems, and SEPS personnel conducted security testing on a third. Although the testing took place immediately prior to the audit's reporting period, this finding implies that the four audited systems were completely untested. Penetration testing on the same systems two years in a row would not normally be a prudent use of resources, especially where it is known that additional testing will be conducted as part of an IG audit.

2. **IG Finding:** The Department did not provide timely and effective oversight of classified systems.

Comment: During the audit period and as a direct result of its oversight activities, SEPS identified thirty-six previously undisclosed Federal Bureau of Investigation (FBI) classified IT systems, discovered several missing FBI classified laptops, disapproved one of the audited systems certification and accreditation documentation, and ordered the FBI to cease Sensitive Compartmented Information (SCI) processing on an administrative mainframe because of an insufficient partition. Prior to the audit period, at the recommendation of the Department Security Officer, the AAG/A shut down the Drug Enforcement Administration (DEA) Merlin IT System, a system audited by the IG, due to an unacceptable risk to classified information, as well as an FBI white collar case management system.

The draft audit also finds that the Department did not enforce its own policy on certification and accreditation of classified systems. In fact, all systems identified to SEPS by the components were certified and accredited at the time of the audit. The systems that were not accredited were FBI systems that were uncovered through SEPS' oversight during the audit period. And, both the Justice Management Division leadership and SEPS insisted that these "new" systems be expeditiously certified and accredited; that

Glenn A. Fine

insistence resulted in the creation of a separate FBI certification and accreditation section in order to meet the deadlines imposed by the Department.

Of the four FBI systems that were audited, two were certified and accredited during the audit period, one was not granted full accreditation by SEPS because of vulnerabilities discovered during a site visit, and the fourth, contrary to the audit report, did in fact have a contingency plan.

All of these activities demonstrate an oversight program that, while constrained by resources, nevertheless is effective and does hold components responsible for taking corrective actions on identified vulnerabilities.

3. **IG Finding:** The Department took nearly four years to revise its overall IT security policy after it was reported as ineffective in September 1997.

Comment: In February 1998, in response to the 1997 IG findings, SEPS promulgated a revised policy on classified IT systems in its Security Program Operating Manual, which was disseminated to all Security Program Managers.

IG Recommendations

Recommendation 1. *Establish a Department Information Technology (IT) Central Security Compliance Office for classified and sensitive but unclassified systems with the responsibility for:*

- a. *Monitoring security-related activities by testing controls at each component having classified systems (performing penetration tests and providing those results to the affected components);*
- b. *Reviewing the number and types of security deficiencies identified in each component's periodic reports;*
- c. *Evaluating each component's compliance with Department security policies, especially in areas of reported weaknesses, and establishing processes and procedures to enforce existing policy such as passwords, account lockout, and system auditing management;*
- d. *Assisting component Security Program Managers in assessing security risks, identifying hardware/software security deficiencies, and providing policy and procedural guidance as needed.*

Agree With Reservation. The Department acknowledges the need to improve IT security management and oversight activities. The Department's new Strategic Plan, dated November

Glenn A. Fine

2001, identifies a specific goal to "[i]mprove the integrity and security of computer systems and make more effective use of information technology." In addition, following the horrific events of September 11th 2001, the AG initiated a series of goals and management initiatives that reflect the changed priorities of the Department. Goal 10, *Utilize Technology to Improve Government*, required the development of a comprehensive IT plan to support strategic goals and improve information management. The CIO is developing an IT Strategic Plan (as specifically tasked by the AG in his Department-wide November 8, 2001 reorganization and restructuring memorandum) that will identify IT security as a major initiative in the Department. Based on the recommendations in your reports, Office of Management and Budget guidance, and the IT Strategic Plan, we are fully assessing the Department's current organization and resources regarding IT security and, following that review, will develop the best solution to achieve improved computer security within the Department. We expect to make a decision before the end of the fiscal year.

Recommendation 2. *Charge the Department IT Central Security Compliance Office with ensuring that all components have current, documented, and tested contingency plans.*

Agree. Current policy requires all systems to have a current, documented, and tested contingency plan. The Department identified a performance measure in FY 01 to specifically address contingency planning. With regard to the recommendation to charge a newly created office with this responsibility, we defer this decision pending action on Recommendation 1.

Recommendation 3. *Charge the Department IT Central Security Compliance Office with developing a comprehensive corrective plan to fully and timely address all Department-wide IT control weaknesses previously identified in security review and audits. Additionally, measures should be prescribed and oversight provided to ensure that component corrective action plans are prepared and that vulnerabilities are corrected. Eliminating repeat findings should be a priority.*

Agree. The Department's new IT Strategic Plan will identify IT security as a major initiative. An action plan for classified systems will be developed within 60 days. Furthermore, we have implemented data bases to track both classified and unclassified system vulnerabilities. With regard to the recommendation to charge a newly created office with this responsibility, we defer this decision pending action on Recommendation 1.

Recommendation 4. *Require each component Security Program Manager to:*

- a. *Have full knowledge of and familiarization with current Department information technology security policies and procedures, including DOJ Order 2640.2D and other departmental policies related to classified and unclassified systems.*
- b. *Report component compliance with Department security policy requirements.*

Glenn A. Fine

- c. *Ensure a security administrator is designated within each component for reviewing system security posture in accordance with Department security policy. In the case of multiple platforms or operating systems supporting component systems, an administrator should be designated to represent each unique platform.*
- d. *Ensure periodic computer security training is provided for each platform supported and require attendance by the designated security administrators.*
- e. *Develop and enforce security policies or apply industry best practices, to assess and counter evolving computer security vulnerabilities.*

Agree. Although most elements of this recommendation are already in place, it will be fully implemented within 90 days, including a meeting of Security Program Managers devoted exclusively to IT security and the IG audit recommendations. The roles and responsibilities of Security Program Managers will be fully spelled out in implementing guidance to Department of Justice (DOJ) Order 2640.2D, "Information Technology Security."

Recommendation 5. *Require each component Security Program Manager to periodically report to the Department IT Central Security Compliance Office on the compliance of individual systems within their component relative to requirements outlined in Department security policies and procedures. Upon its review of the reports, the Department IT Central Security Compliance Office should bring areas of concern to the attention of the AAG/A.*

Agree. This recommendation is already implemented in DOJ Order 2640.2D. Areas of concern will be brought to the attention of both the AAG/A and the Department CIO. With regard to your recommendation to charge a newly created office with this responsibility, we defer this decision pending action on Recommendation 1.

Recommendation 6. *Establish and implement guidance to ensure systems' security is monitored sufficiently, efficiently, and consistently. Specific areas that need to be addressed include:*

- a. *Automated monitoring of security practice compliance;*
- b. *Automated logging, auditing, and review and notification of security relevant events;*
- c. *Requiring intrusion detection systems; and*
- d. *Requiring application and operating system patches be kept current.*

Glenn A. Fine

Agree. The Department is already preparing and plans to promulgate implementing guidance to DOJ Order 2640.2D, "Information Technology Security." The guidance for classified IT systems will be promulgated by July 1, 2002.

Recommendation 7. *Ensure the periodic update and supplementing of DOJ Order 2640.2D based on observed component needs, the evolving computer security environment, and industry best practices. We recommend that the AAG/A promptly review the adequacy of guidance for the following areas:*

- a. *Password management (including task versus user accounts);*
- b. *Accountability and audit trails;*
- c. *Access controls;*
- d. *Account integrity management, including monitoring of account disposition (dormant accounts);*
- e. *Logon management;*
- f. *Service accounts – changing the default password;*
- g. *Assignment of user rights and advanced user rights;*
- h. *Renaming guest and administrative accounts; and*
- i. *Backup procedures.*

Agree. We will periodically update the DOJ Order to address changing environments and component needs. Additional implementing directives will be developed to include more detailed guidance for classified IT and SBU IT security in the areas set forth in this recommendation.

* * * *

We strongly recommend that our comments be included in your final reports. If you have any questions or require additional information, please feel free to contact us.

cc: Guy K. Zimmerman
Assistant Inspector General for Audit
Office of the Inspector General

**OIG'S RESPONSE TO DEPARTMENT'S
COMMENTS TO OVERALL REPORT**

In addition to commenting on each specific recommendation discussed in APPENDIX V, the Department's response stated that the OIG did not interview anyone from the Security and Emergency Planning Staff (SEPS) as part of the audit. That assertion is not completely accurate. Throughout the audit, SEPS participated in periodic meetings the OIG held with the Department. In those meetings the OIG discussed: which systems would be selected for audit, scope of the work, audit methodology, certification and accreditation (C&A) process, status of audit work, preliminary findings, and final results of audit work. The conclusions stated in the reports were based upon the four major systems selected for audit -- systems that were selected with the participation and advice of SEPS. The OIG asked SEPS to provide information and policy statements applicable to their responsibilities, which were incorporated into the audits. Although the OIG did not conduct formal interviews of SEPS personnel, SEPS's views about the audit findings were heard and considered, even though the OIG ultimately disagreed with some of SEPS's views.

The Department's response also provided three bolded comments regarding the report. The following responds to each bolded comment.

1. Management did not conduct penetration testing on its classified systems.

The Department's response stated that it requested the National Security Agency (NSA) to conduct penetration testing on two systems the OIG audited and that SEPS personnel conducted "security testing" on a third. The response further states that the OIG's report "implies that the four audited systems were completely untested."

First, in the detailed OIG reports on the individual systems, the OIG did report where NSA had performed penetration testing, although the results of that testing were not received in time to include it in the evaluation. The OIG found, however, that the components and Department had not prepared corrective action plans in response to the NSA penetration testing, and without such plans the benefit from testing is minimal. In addition, the OIG found that the NSA report on penetration tests of one system was not properly circulated and appropriate personnel were not required to address the issues noted.

The Department also recites that SEPS performed "security testing" on a third system. The exact nature of the testing was not further described in the Department's response. The OIG has since been informed that the testing did not include penetration testing. During the audit of this third system, no evidence was found that testing occurred, that it was formally reported and disseminated to the program manager, or that recommendations and corrective action were being tracked.

Moreover, the OIG's report does not assert that the Department conducted *no* penetration testing, as the response implies. Rather, the report states the Department did not make the *same commitment* to testing its classified systems as it did its sensitive but unclassified systems (SBU). The OIG stated that the Department has conducted regular network security penetration testing on SBU systems for the past four years but that it did not have a similar program established for testing classified systems. Justification explaining why classified systems received less intense testing than SBU systems was not provided to the OIG. Therefore, the OIG concluded that, at a minimum, classified systems should have received equal attention from the Department.

2. The Department did not provide timely and effective oversight of classified systems.

The Department in its response cited a broad range of results as evidence that its oversight program is effective and holds components responsible for taking corrective actions on identified vulnerabilities. For example, the Department stated, "Of the four FBI systems that were audited, two were certified and accredited..." and all systems identified to SEPS by the components were certified and accredited at the time of the OIG's audits. By its response, the Department implied that SEPS fulfilled its obligations to enforce its policy on C&A for those systems that it knew about.

The OIG disagrees. The OIG did not audit four FBI systems. Of the four systems audited, two were FBI's and two were DEA's. At the time of the audit, the OIG was informed of the Department's activities, but do not believe they change the audit report findings. The OIG's report criticized the Department for not providing timely and effective oversight of classified systems security by enforcing the Security Program Operating Manual (SPOM) and by holding components responsible for taking corrective actions on previously identified vulnerabilities. Further, the report states that the Department did not enforce its policy on C&A and that all four systems operated without full certification and accreditation.

Specifically, the report notes that vulnerabilities identified in previous reviews of all four systems were not corrected. For example, a past report of deficiencies in one component's system was not distributed to personnel responsible for correcting the vulnerabilities, and security vulnerabilities previously reported continued to exist in another component for as long as five years.

For the four systems audited, the OIG found that one system was accredited without complete certification and accreditation documentation (DEA, Merlin), one system operated under an interim approval (DEA, EPIC), and two systems were self-certified but unaccredited by the designated approval authority (FBI, Investigative and Administrative mainframes). In our opinion, the fact that different conditions existed for the four systems audited shows a lack of enforcement of the certification and accreditation procedures by the Department.

In short, as the following points demonstrate, none of the four systems audited was fully certified and accredited:

- During the audit, the FBI's two systems operated under an interim approval because they could not achieve and had not achieved full accreditation. The individual report recommended that the FBI obtain a full accreditation for the systems. In its response, the FBI agreed that the two systems were not certified and accredited, stating that it had yet to request a full accreditation due to outstanding action items that needed resolution.
- The Department's response stated that the system identified by the OIG as lacking a contingency plan did in fact have such plan. The basis for the Department's assertion is still unclear to the OIG. The DEA's response to the draft audit report agreed with the OIG's finding that the system did not have a contingency plan. The DEA also advised the OIG that the draft contingency plan was still being reviewed as of December 31, 2001 - several months after the completion of our audit work.
- The Department stated it did not accredit one system due to vulnerabilities it had identified. The OIG's contention is that the Department granted the system an interim approval to operate, and upon its expiration granted an extension even though DOJ Order 2640.2C states that computer systems must be accredited prior to processing classified information. The DEA agreed it needed to fulfill the necessary conditions to fully accredit the system as soon as possible and stated that it was finalizing a new certification and

accreditation effort for the system environment. The OIG report criticizes the Department for not following up to ensure that a final accreditation is actually achieved and that it is achieved promptly. On December 31, 2001, the extension to the interim approval to operate expired. In its most recent response, dated May 13, 2002, DEA did not indicate whether or not the Interim approval to operate had again been extended.

Interim approval to operate is intended to be a temporary condition while certification requirements are being met, not a substitute for the full C&A requirements. The interim approval does not require a contingency plan, a security guide, or a report on certification testing, which are required for full certification and accreditation. For example, without a documented and tested contingency plan, as was the case for one system, that component and the Department cannot be assured that component staff are prepared to continue operations in the event of a system failure or disaster.

3. The Department took nearly four years to revise its overall Information Technology security policy after it was reported as ineffective in September 1997.

The Department stated that SEPS promulgated a revised policy on classified Information Technology (IT) systems in February 1998 in its SPOM. In fact, the OIG used and referenced the SPOM throughout the audits. However, the OIG criticized the Department for not responding to the November 1997 audit until July 2001. The February 1998 SPOM was not a response to the findings and deficiencies reported in the November 1997 audit. Moreover, the SPOM does not set forth policy applicable to the Department's overall IT security policy and only addresses classified systems. The issuance of the SPOM in February 1998, while valuable, did not resolve the need for a timely revised overall IT security policy.

**OIG, AUDIT DIVISION ANALYSIS AND SUMMARY
OF ACTIONS NECESSARY TO CLOSE THE REPORT**

The OIG resolved recommendations 1, 2, and 3 because the Department agreed to consider the findings and recommendations while developing its strategic plan. The OIG believes, however, that it is important for the Department to make a prompt decision on how these problems will be addressed organizationally and procedurally. Implementation of any decisions will take additional time to achieve, and considerable time could pass before remedial action is achieved. Accordingly, with respect to recommendations 1, 2, and 3, the Department should advise the OIG in 60 days of its plan and schedule if it proposes an alternative to our recommendations. Otherwise, the OIG will consider reclassifying the recommendations as unresolved.

The Department's responses to the report's seven individual recommendations, including the status and action needed to close each, are detailed below.

Recommendation Number:

- 1. Resolved.** In its response, the Department acknowledged the need to improve information technology security management and oversight activities. The Department did not agree to implement the specific actions the OIG recommended, but did commit that it would consider the recommendations in its forthcoming strategic plan to achieve improved computer security within the Department. To close this recommendation, the Department should establish a Department Information Technology Central Security Compliance Office or propose alternative corrective action to ensure centralized responsibility for monitoring security-related activities by performing penetration tests on classified systems; reviewing security deficiencies identified in each component's periodic reports; evaluating each component's compliance with Department security policies; and assisting Security Program Managers in accessing security risks and providing guidance as needed.
- 2. Resolved.** The Department agreed, stating that current policy requires all systems to have a current, documented, and tested contingency plan. However, the Department deferred a decision on who to charge with this responsibility pending action on Recommendation 1. The OIG believes that the Department needs to quickly decide this issue and implement contingency plans. These plans should be the responsibility of the

component that "owns" the system, and they should accomplish that process without delay. Even if accountability for ensuring that such action occurs may later shift if the Department reorganizes its IT functions, the OIG sees no reason why a component official should not assume responsibility for overseeing the contingency planning process until then. To close this recommendation, the Department should provide the OIG with documentation evidencing the assignment of the responsibility to ensure that all components have current, documented, and tested contingency plans.

- 3. Resolved.** The Department stated that its new IT Strategic Plan will identify IT security as a major initiative and that an action plan for classified systems will be developed within 60 days. Further, the Department stated that it has implemented databases to track both classified and unclassified system vulnerabilities. To close this recommendation, the Department should provide the OIG with documentation formally assigning the recommended responsibility and detailing prescribed measures and oversight to ensure that component corrective action plans are prepared and vulnerabilities are corrected. The Department should also provide the OIG with a copy of its comprehensive Department-wide corrective action plan (for both classified and SBU systems).
- 4. Resolved.** The Department stated that most of the elements of the recommendation are already in place and that it will be fully implemented within 90 days. To close this recommendation, the Department should provide the OIG with the documented policy or procedures by which it will ensure and require performance of each of the recommendation's four elements.
- 5. Resolved.** The Department stated that requiring each component Security Program Manager to periodically report to the Department on the compliance of individual systems relative to Department security policies and procedures is already implemented in DOJ Order 2640.2D, Chapter 5, Roles and Responsibilities for the Component Head or their Designee. To close this recommendation, the Department should provide the OIG with a copy of the implementing procedure detailing how this occurs and designating responsibility for receipt of Security Program Managers compliance reports reporting areas of concern to the attention of the Assistant Attorney General for Administration.

- 6. Resolved.** The Department stated that it is preparing and plans to promulgate implementing guidance to DOJ Order 2640.2D, with the guidance for classified IT systems expected by July 1, 2002. To close this recommendation, the Department should provide the OIG a copy of the guidance specifically addressing the four elements named in the recommendation and ensuring that both SBU and classified systems' security is monitored sufficiently and consistently.
- 7. Resolved.** The Department stated that it will periodically update the DOJ Order 2640.D to address changing environment and component needs and develop additional implementing directives to include more detailed guidance for classified and SBU system security in the areas set forth in this recommendation. To close this recommendation, the Department should provide the OIG with copies of supplementing guidance developed for each of the nine areas cited in the recommendation.