U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report

Independent Evaluation Pursuant to the Government Information Security Reform Act Fiscal Year 2002

The Bureau of Prisons' Inmate Telephone System II

November 2002

03-04

INDEPENDENT EVALUATION PURSUANT TO THE GOVERNMENT INFORMATION SECURITY REFORM ACT FISCAL YEAR 2002

THE FEDERAL BUREAU OF PRISONS' INMATE TELEPHONE SYSTEM II

OFFICE OF THE INSPECTOR GENERAL EXECUTIVE SUMMARY

The Federal Bureau of Prisons (BOP) is tasked with protecting society by confining offenders in the controlled environments of prisons and community-based facilities that are safe, humane, cost-efficient, and appropriately secure; and providing work and other self-improvement opportunities to assist offenders in becoming law-abiding citizens.

The Inmate Telephone System II (ITS II) is a system that allows inmates at a federal correctional facility to place telephone calls while providing BOP staff with the ability to control their access, make records of the calls, adjust inmates' commissary account, and bill for the calls.

The Office of the Inspector General (OIG) selected ITS II as one of five sensitive but unclassified (SBU) systems to review pursuant to the Government Information Security Reform Act (GISRA) for the fiscal year (FY) 2002. The OIG is required by GISRA to perform an independent evaluation of the Department of Justice's (Department) information security program and practices. This report contains the results of the ITS II audit. Separate reports will be issued for each of the other systems evaluated pursuant to GISRA, including three systems that process classified information.

Under the direction of the OIG and in accordance with Government Auditing Standards, PricewaterhouseCoopers LLP (PwC) performed the audit of ITS II. The audit took place from May through July 2002 and consisted of interviews, on-site observations, and reviews of Department and component documentation to assess ITS II's compliance with GISRA and related information security policies, procedures, standards, and guidelines.[1] We[2] used commercial-off-the-shelf and proprietary tools to conduct vulnerability

[1] In a September 1997 audit, report number 97-26, the OIG recommended that the Department develop effective computer security program guidance. The Department then revised its policy and released DOJ Order 2640.2D, "Information Technology Security" in July 2001, which was used in the analysis of this year's review.

[2] In this report, "we" refers either to the OIG or to PwC working under the direction of the OIG.

tests and analyses of significant operating system integrity and security controls.

During the course of our work for this review, we found improvements or satisfactory operations within the ITS II information security controls that are being reported. Specifically:

- BOP is in the process of having ITS II recertified.
- BOP is in the process of addressing findings identified in the June 2002 security test and evaluation (ST&E) report.
- BOP staff have signed the Rules of Behavior.
- BOP facilities are controlled by security guards. In addition, all BOP employees and contractor staff must have an access badge or be escorted by BOP personnel to gain entry to BOP facilities.

Despite these improvements, we assessed management, operational, and technical controls at a medium to high risk to the protection of the ITS II from unauthorized use, loss, or modification. Specifically, we identified vulnerabilities in 13 of the 17 control areas. Two of the 13 vulnerabilities were identified as high risks to the protection of ITS II as indicated in the following chart.

CONTROL AREAS[3]	VULNERABILITIES NOTED
Management Controls	
1. Risk Management	
2. Review of Security Controls	
3. Life Cycle	√
4. Authorize Processing (Certification and Accreditation)	√
5. System Security Plan	√
Operational Controls	
6. Personnel Security	√
7. Physical and Environmental Protection	√
8. Production, Input/Output Controls	√
9. Contingency Planning	√
10. Hardware and Systems Software Maintenance	√
11. Data Integrity	√
12. Documentation	
13. Security Awareness, Training, and Education	
14. Incident Response Capability	√
Technical Controls	
15. Identification and Authentication	√*
16. Logical Access Controls	√*
17. Audit Trails	√

Source: The OIG's FY 2002 GISRA audit of ITS II

√* Significant vulnerability in which risk was noted as high. A high-risk vulnerability is defined as one where extremely grave circumstances can occur by allowing a remote or local attacker to violate the security protection of a system through user or root account access, gaining complete control of a system and compromising critical information.

As a result of the findings identified in this report, we are providing 28 recommendations for improving ITS II to ensure that BOP management:

- Incorporate security requirements into the development and acquisition phases of the BOP system development life cycle (SDLC).

- Incorporate formal procedures to document certification/testing activities, update system documentation when security controls are added, retest security controls, and have the system recertified after changes have been made.

[3] Control Areas as described in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-26, "Security Self-Assessment Guide for Information Technology Systems."

- Incorporate the in-place operating controls as outlined in the June 2002 ST&E report and complete the "Conditions of Certification" outlined in the ITS II certification statement.

- Incorporate the guidelines for developing security plans outlined in the NIST SP 800-18 into the current ITS II security plan and incorporate the plan into the overall strategic plan for the BOP.

- Conduct an analysis on the current staff shortages by determining the current security and system administrator skills on the BOP team and determine what skills the BOP needs to close the "gap."

- Distribute the BOP's documented procedures on how to maintain ITS II user accounts to ITS II security staff and contractor personnel. Additionally, enforce the procedures as required by the BOP's Directive 1237.11.

- Implement all of the recommendations outlined in the June 2002 ST&E report, specifically those outlined in section 4.12.

- Establish a formal documented process to control the transfer of BOP media and data.

- Distribute the contingency plan to appropriate individuals, including contractor staff and periodically test the contingency plan.

- Develop a configuration standard for all systems that incorporates the most restrictive security settings possible.

- Develop policies and procedures surrounding the use of intrusion detection software and integrity validation software, and implement these policies and procedures on critical servers.

- Develop a stronger policy for incident handling, response, and personnel support.

- Enforce current Department password policies and procedures and install and activate a password filter on all servers to enforce parameters that enforce restrictions on passwords.

- Develop, implement, and monitor documented policy establishing specific security standards and settings for access controls.

- Develop, implement, and monitor documented policy establishing specific security standards and settings for user authentication and access.

- Implement the system key utility, restrict services to run in a secured context, and remove all unnecessary services.

- Develop, implement, and monitor documented policy establishing specific security standards and settings for network controls.

- Develop, implement, and monitor documented policy establishing specific security standards and settings for user and group management controls.

- Develop, implement, and monitor documented policy establishing specific security standards and settings for account integrity management.

- Develop, implement, and monitor documented policy establishing specific security standards and settings for file system access.

- Develop, implement, and monitor documented policy establishing specific security standards and settings for maintenance controls.

- Develop, implement, and monitor documented policy establishing specific security standards and settings for Windows NT registry settings.

- Obtain the latest security patches from the operating system vendor.

- Develop, implement, and monitor documented policy establishing specific security standards and settings for router configurations.

- Implement Cisco's fail-over capabilities on critical external routers.

- Develop, implement, and monitor documented policy establishing specific security standards and settings for command line access.

- Develop documented procedures for logging and monitoring system activity and require that audit logs be reviewed periodically.

We concluded that these vulnerabilities occurred because BOP management did not fully develop, document, or enforce agency-wide policies in accordance with current Department policies and procedures. Additionally, we believe the Department did not enforce their security policies and procedures to ensure ITS II is protected from unauthorized use, loss, or modification through its certification and accreditation process. If not corrected, these security vulnerabilities threaten ITS II and its data with the potential for unauthorized use, loss, or modification.

TABLE OF CONTENTS

OBJECTIVE, SCOPE, AND METHODOLOGY

The fiscal year (FY) 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 policies are 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).

The objective of the audit was to determine the Department of Justice's (Department) compliance with the requirements of GISRA. The Inmate Telephone System II (ITS II) was selected as one of the subset of systems to be tested to determine the effectiveness of the Department's overall security program for FY 2002. In determining if the Department is compliant with GISRA requirements, PricewaterhouseCoopers LLP (PwC) assessed whether adequate computer security controls existed to protect the ITS II from unauthorized use, loss, or modification.

Under the direction of the OIG and in accordance with Government Auditing Standards, PwC performed the audit of ITS II. The audit took place from May through July 2002. During our audit, we met with the Federal Bureau of Prisons (BOP) officials from the ITS II System Control Center. We reviewed documentation that included the BOP's information technology (IT) documents, organizational structures, OMB GISRA reporting information, and prior OIG and Department reports to assess the ITS II compliance with GISRA and related information security policies, procedures, standards, and guidelines. We performed test work at BOP Headquarters in Washington, D.C.

For the interviews conducted, we used the questionnaire contained in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-26, "Security Self-Assessment Guide for Information Technology Systems." This questionnaire contains specific control objectives and suggested techniques against which the security of a system or group of interconnected systems can be measured. The questionnaire contains 17 areas under 3 general controls (management, operational, and technical). The areas contain 36 critical elements and 225 supporting security control objectives and techniques (questions) about the system. The critical elements are derived primarily from OMB Circular A-130 and are integral to an effective IT security program. The control objectives and techniques support the critical elements. If a number of the control objectives and techniques are not implemented, the critical elements have not been met.

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 NIST. These authorities prescribe a review that evaluates the adequacy of management, operational, and technical controls over control areas listed in Appendix I.

INMATE TELEPHONE SYSTEM II (ITS II) NETWORK ENVIRONMENT

The ITS was developed in 1988. In an August 1999 review performed by the OIG, we found that a significant number of federal inmates use prison telephones to commit serious crimes while incarcerated – including murder, drug trafficking, and fraud. BOP management acknowledged the shortcomings of its inmate telephone system and indicated that a more sophisticated version of the inmate telephone system called (ITS II), was being developed to provide more options for restricting and controlling inmate access to prison telephones.

While the former inmate telephone system was self-contained at each institution and was incapable of sharing data through a central database, ITS II is designed to allow the BOP to access inmate telephone information from all BOP institutions simultaneously. ITS II provides the BOP with the ability to control their access, make records of the calls, adjust the inmates' commissary account, and bill inmates for the calls. ITS II also allows the BOP's Central Office to monitor and record telephone conversations of any inmate in the country.

ITS II provides wide-area network circuits, routers, Ethernet switches, and network management for ITS II computer systems and networking equipment. The ITS II consists of UNIX and Windows NT platforms.

SUMMARY RESULTS OF THE AUDIT

We obtained audit evidence to determine whether adequate computer security controls existed to protect ITS II from unauthorized use, loss, or modification. Our testing consisted of assessing management, operational, and technical controls for 17 critical areas for the ITS II. Our testing disclosed vulnerabilities within 13 of the 17 areas. Two of the 13 vulnerabilities were within technical controls and were identified as high risks to the protection of ITS II.

We concluded that these vulnerabilities occurred because ITS II management did not fully develop, document, or enforce agency-wide policies in accordance with current Department policies and procedures. Additionally, we believe the Department did not enforce their security policies and procedures to ensure ITS II is protected from unauthorized use, loss, or modification through its certification and accreditation process. If not corrected, these security vulnerabilities threaten ITS II and its data with the potential for unauthorized use, loss, or modification.

FINDINGS AND RECOMMENDATIONS

Our review disclosed that security controls need improvement to fully protect the ITS II from unauthorized use, loss, or modification. Specifically we found vulnerabilities in the areas of life cycle; authorize processing; system security plan; personnel security; physical and environmental protection; production, input/output controls; contingency planning; hardware and systems software maintenance; data integrity; incident response capability; identification and authentication; logical access controls; and audit trails.

I. Management Controls. Management controls are techniques and concerns that are normally addressed by management in the organization's computer security program. In general, they focus on the management of the computer security program and the management of risk within the organization.

Management Controls	Vulnerabilities Noted
Risk Management	
Review of Security Controls	
Life Cycle	√
Authorize Processing (Certification and Accreditation)	√
System Security Plan	√

As a result of testing management controls, we confirmed that controls were adequate for ITS II's risk management and review of security controls. Vulnerabilities were identified within the following management control areas:

A. Life Cycle. Security is an important part of the system life cycle, and security is best managed if planned for the entire IT system life cycle. There are many models for the IT system life cycle but most contain five basic phases: initiation, development/acquisition, implementation, operation, and disposal.

Issue: Inadequate System Development Life Cycle (SDLC)

Condition:

The BOP has not incorporated security requirements into its ITS II SDLC procedures. During the acquisition and development phases of ITS II, the

SDLC did not require the BOP to address security issues that may have arisen.

Cause:

The BOP ITS II management failed to fully implement its SDLC methodology.

Criteria:

DOJ Order 2640.2D, *Information Technology Security*, states that components shall develop and implement a risk-based security process to provide security throughout the life cycle of all systems supporting their operations and assets.

Risk:

Without security requirements being outlined for the development and acquisition phases of the SDLC, complications in the development process can arise that could cause system vulnerabilities to be present in the final production system.

Recommendation:

1. We recommend that the BOP Director ensure that BOP management incorporate security requirements into the development and acquisition phases of the SDLC.

Issue: Inadequate Change Control Procedures

Condition:

ITS II does not have adequate change control procedures in place to: (a) document certification testing activities, (b) update system documentation when security controls are added, (c) retest security controls, or (d) recertify the system after changes have been made.

Cause:

BOP management failed to fully implement the SDLC methodology.

Criteria:

DOJ Order 2640.2D requires that a configuration management process be in place to maintain control of changes to any system.

Risk:

The absence of adequate change control procedures in the SDLC can lead to numerous complications if or when changes are made to ITS II. This can include system failures, system vulnerabilities, and other system flaws. In addition, any changes made for security purposes will not be documented.

Recommendation:

2. We recommend that the BOP Director ensure that BOP management incorporate documented procedures to document certification testing activities, update system documentation when security controls are added, retest security controls, and recertify the system after changes have been made.

B. Authorize Processing (Certification and Accreditation). Authorize processing (also referred to as certification and accreditation) provides a form of assurance of the security of the system. Computer security assurance is the degree of confidence one has that the security measures, both technical and operational, work as intended to protect the system and the information it processes. Certification is a formal process for testing components or systems against a specified set of security requirements while accreditation is a management official's formal acceptance of the adequacy of a system's security. Computer security accreditation forces managers and technical staff to work together to find workable, cost-effective solutions of security needs, technical constraints, operational constraints, and mission or business requirements.

Issue: Operating Controls Not In Place

Condition:

Although ITS II was certified and accredited, we found that BOP management did not improve operating controls outlined in a security test and evaluation (ST&E) report completed by a contractor in June 2002. The report identified 13 areas of weaknesses and correlating recommendations for improving operating controls over ITS II. In addition, areas such as virus controls, password controls, and user level access controls outlined in a December 2000 certification statement as conditions for certification had not been met.

Cause:

BOP management did not update the system resources to fully improve security over the network.

Criteria:

DOJ Order 2640.2D requires that each component shall evaluate their IT security programs and system protection mechanisms and report deficiencies to the Chief Information Officer annually.

Risk:

Without in-place controls operating as intended, ITS II is vulnerable to security breaches that could lead to a denial of service or a full compromise of the system.

Recommendation:

3. We recommend that the BOP Director ensure that BOP management update operating controls as outlined in the June 2002 ST&E report, and complete the "Conditions of Certification" outlined in the ITS II certification statement.

Issue: Rules of Behavior

Condition:

The BOP developed Rules of Behavior (BOP Directive 1237-12) that BOP approved to provide guidance on how to use BOP systems. BOP staff signed the Rules of Behavior; however, the ITS II contractor personnel have not. Therefore, contractor personnel are not necessarily aware of the BOP's procedures and guidelines for administering and operating ITS II.

Cause:

BOP management did not follow Department procedures requiring contractor's acknowledgement of the Rules of Behavior document.

Criteria:

NIST SP 800-18, *A Guide For Developing Private Security Plans For Information Technology*, states that a set of Rules of Behavior must be established for each system and should be made available to every user

prior to receiving authorization for access to the system. It is recommended that the rules contain a signature page for each user to acknowledge receipt.

Risk:

Contractor personnel not signing the *Rules of Behavior* document could have several negative effects. For example, users could potentially find themselves in a situation where they are unsure of how to act given the circumstances and could choose an action that goes against the BOP policy. Additionally, the BOP could be unable to hold contractors and vendors accountable for their actions should they affect the BOP or ITS II negatively.

Recommendation:

4. We recommend that the BOP Director ensure that BOP management requires all users, including vendor and contractor personnel, to read and sign the *Rules of Behavior* document (BOP Directive 1237-12) to ensure users are aware of its contents.

C. System Security Plan. A system security plan provides an overview of the security requirements of the system and describes the controls in place or planned for meeting those requirements. The plan delineates responsibilities and expected behavior for all individuals who access the system.

Issue: Security Plan

Condition:

While the BOP has developed a system security plan for ITS II, BOP did not address critical elements. For example, the BOP has not incorporated all aspects of NIST SP 800-18, into the security plan. In addition, the plan for ITS II was not incorporated into the BOP's overall strategic information resources management (IRM) plan.

Cause:

The current system security plan was developed by the main ITS II contractor, and was based on the contractor’s standards, not those of the BOP or the Department.

Criteria:

DOJ Order 2640.2D Section 5 states:
"Components shall ensure the certification and accreditation of all systems under their operational control.

c. For each classified and sensitive but unclassified (SBU) system the certification official shall:

(1) Ensure a system security plan is prepared and maintained throughout the system life cycle.

(2) Ensure a system test and evaluation is conducted and the results of such tests are documented."

Risk:

Without incorporating NIST SP 800-18 standards into the security plan and not incorporating the security plan into the BOP's overall strategic plan could result in aspects of the security plan being incomplete or not in accordance with overall BOP security guidelines. This could lead to a less secure system overall.

Recommendation:

5. We recommend that the BOP Director ensure that BOP management incorporate the guidelines for developing security plans outlined in NIST SP 800-18 into the current ITS II security plan and incorporate the plan into the overall IRM strategic plan for the BOP.

II. Operational Controls. Operational controls address security controls that are implemented and executed by people. These controls are put in place to improve the security of a particular system. They often require technical or specialized expertise and rely upon management activities as well as technical controls.

Operational Controls	Vulnerabilities Noted
Personnel Security	√
Physical and Environmental Protection	√
Production, Input/Output Controls	√
Contingency Planning	√
Hardware and Systems Software Maintenance	√
Data Integrity	√
Documentation	
Security Awareness, Training, and Education	
Incident Response Capability	√

Our testing confirmed that operational controls were adequate within the areas of documentation and security awareness, training, and education for ITS II. However, our testing also identified vulnerabilities within other critical areas of operational controls. The specific details identifying these vulnerabilities are listed below.

A. Personnel Security. Personnel security involves the use of computer systems by human users, designers, implementers, and managers. A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their jobs.

Issue: Segregation of Duties

Condition:

Currently, the BOP system administration and system security responsibilities are not adequately separated to ensure least privilege and individual accountability. In addition, different individuals do not always perform distinct systems support functions.

Cause:

According to BOP personnel, due to staff constraints, system maintenance, user maintenance, and security and network administration activities all fall under one person for the BOP and one person for the contractor. In addition, staffing constraints have resulted in one person acting as both a maintenance manager and a researcher and developer.

Criteria:

DOJ Order 2640.2D, Chapter 2, Section 23 (a) and (c), states: "Department IT systems shall have assignment and segregation of system responsibilities defined and documented…. At a minimum, there shall be a clearly defined role for a security administrator and a system administrator." Additionally, "Controls [compliant with Department access control policies] shall be in place to ensure that the user [and administrators] has access to only the resources required to accomplish their duties and no more."

Risk:

Tasking the same individuals to be responsible for development, system administration, and security administration could potentially allow an individual to commit fraudulent activity and "cover-up" his/her tracks without the BOP detecting the activity. In addition, individuals could

potentially implement "backdoors" that would allow access once the individual has left the BOP.

Recommendation:

6. We recommend that the BOP Director ensure that BOP management:

    a. conduct an analysis on the current staff shortages by determining the current security and system administrator skills on the BOP team and determine what skills the BOP needs to close the "gap." If additional staff is required, hire additional personnel who are trained and experienced security and/or system administrators;

    b. ensure that those individuals who currently function as both security administrators and system administrators are moved to positions where these responsibilities do not conflict; and

    c. ensure that developers are not tasked with either system or security administration.

Issue: Hiring, Transfer, and Termination Documentation

Condition:

Not all BOP ITS II security staff and contractor personnel are aware of the BOP's user account maintenance policy, which provides procedures for how to handle ITS II user accounts when employees are hired, transferred or terminated.

Cause:

According to the BOP security staff, the policy had not been communicated to them or ITS II contractor personnel.

Criteria:

BOP Directive 1237-11, states: "Users shall be trained in protection of computer hardware, software, and information. This includes all persons employed by or working with the Department of Justice receiving direct or indirect compensation or none at all (Public Health Service staff, contractors, volunteers, interns, persons representing or detailed from other Government agencies, etc.). They shall be made thoroughly aware of security and contingency plans for systems they use."

Risk:

Without the awareness of the documented procedures for user account maintenance, accounts may be added to the ITS II without authorized approval and accounts of employees that have transferred or been terminated may not be removed in a timely manner.

Recommendation:

7. We recommend that the BOP Director ensure that BOP management:

    a. distribute the BOP's documented procedures on how to maintain BOP ITS II user accounts to ITS II security staff and contractor personnel; and

    b. enforce procedures in accordance with the BOP Directive 1237.11 and Department policy.

B. Physical and Environmental Protection. Physical security and environmental security are the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment.

Issue: Physical Access

Condition:

The BOP does not have adequate physical security controls in place for ITS II. The ST&E report identified physical security weaknesses relating to 13 areas under NIST SP 800-26, which are being used for this GISRA review. These deficiencies included weaknesses in areas such as physical access to ITS II systems (routers, switches, and wiring closets), documentation of employee access to sensitive areas, reporting of suspicious activities, unauthorized viewing of computer monitors, and fire suppression and prevention.

Cause:

The BOP security management has not taken all appropriate steps to meet the Department and BOP requirements for physical security.

Criteria:

DOJ Order 2640.2D, states: "Department IT systems shall be physically protected commensurate with the highest classification or sensitivity of the information." In addition, BOP Directive 1237-11 Section 5 also outlines requirements for physical security.

Risk:

Without adequate physical security controls, unauthorized physical access to ITS II can be obtained and damage can be done to the systems. In addition, the systems may not be properly protected from disaster events such as fires and floods.

Recommendation:

8. We recommend that the BOP Director ensure that BOP management implement all of the recommendations outlined in the June 2002 ST&E report, specifically those outlined in section 4.12.

C. Production, Input/Output Controls. There are many aspects to supporting IT operations. Topics range from user help desk to procedures for storing handling and destroying media.

Issue: Sensitive Media

Condition:

To date, the BOP did not develop documented procedures for handling sensitive media. No formal process has been established to ensure that only authorized individuals can pick up, receive, or deliver input and output information and media. In addition, no documented process has been established to ensure adequate audit trails are used and maintained for inventory management, and labeling of sensitive media.

Cause:

According to BOP, an inadequate number of trained security personnel are on the ITS II security team to handle the associated responsibilities for developing the formal policies and procedure for handling sensitive media and perform the daily tasks required to maintain a secure computing environment.

Criteria:

BOP Directive 1237.11, states: "Be responsible for security of individual and shared office space containing computers, sensitive printouts, and electronic storage devices/media…. Take reasonable precautions to avoid loss of or damage to Government property and information."

DOJ Order 2640.2D Chapter 2 Section 19, states: "Department IT systems shall: maintain an audit trail of activity sufficient to reconstruct security relevant events."

Risk:

Without these procedures in place, unauthorized individuals could potentially gain access to sensitive BOP data. The lack of adequate audit trails for inventory management could also allow someone with access to the BOP hardware and software to either accidentally or intentionally misplace system components. In addition, contractor staff may not be made aware of the BOP's procedures for handling sensitive media once they have been created.

Recommendation:

9. We recommend that the BOP Director ensure that BOP management document a process to control the transfer of media and BOP data. In addition, the BOP management should ensure that audit trails are kept and retained for extended periods of time, capturing relevant information such as name, date, media description, and authorization.

D. Contingency Planning. Contingency planning can ensure continued operations by minimizing the risk of events that could disrupt normal operations and having an approach in place to respond to those events should they occur.

Issue: Contingency Plan Implementation

Condition:

The current BOP contingency plan has not been distributed to all ITS II personnel. In addition, the current contingency plan for ITS II is not periodically tested and ITS II staff have not been trained in their roles and responsibilities concerning the contingency plan.

Cause:

The BOP ITS II management have not distributed the contingency plan to appropriate BOP personnel. The BOP management does not know if the plan has been distributed to the vendor's (Dyncorp) personnel.

Criteria:

BOP Directive 1237-11, states: "Users shall be trained in protection of computer hardware, software, and information…. They shall be made thoroughly aware of security and contingency plans for systems they use."

DOJ Order 2640.2D Chapter 1 Section 9, states: "Components shall plan for how they will perform their missions in the event their IT systems are unavailable and how they will recover these IT systems in the event of loss or failure. Components shall:…. Test contingency/business resumption plans annually or as soon as possible after a significant change to the environment that would alter the in-place assessed risk."

Risk:

By not properly distributing the contingency plan, the BOP's security staff may not be fully informed with the plan's details, and contractor staff may not be aware of the appropriate steps to take should a system recovery become necessary. Not testing the plan could allow deficiencies or weaknesses in the plan to go unnoticed for correction until an actual emergency situation. This also leaves the BOP personnel unfamiliar with the steps to take in the event of a disaster and unaware of who is responsible for completing each step as outlined in the plan.

Recommendation:

10. We recommend that the BOP Director ensure that BOP management:

    a. distribute the contingency plan to appropriate individuals, including contractor staff; and

    b. periodically test the Contingency plan and their employees and contractor staff in their roles and responsibilities.

E. Hardware and Systems Software Maintenance. Hardware and systems software maintenance controls are used to monitor and provide a historical record of installations and upgrades.

Issue: Security Configuration

Condition:

The ITS II operating systems were not properly configured to prevent circumvention of the security software and application controls. We observed weak passwords on ITS II (Windows NT administrator level accounts with passwords set to the account name and administrator level accounts without passwords), and numerous vulnerabilities were identified by the contractor in its ST&E report. We also identified numerous vulnerabilities in ITS II diagnostic reviews. In addition, the default settings of security features for ITS II are not as restrictive as possible (Windows NT systems allowed enumeration of users, file permissions were not restrictive, and Simple Network Management Protocol (SNMP) community strings were weak).

Cause:

These conditions exist due to the lack of a formal configuration standard for the ITS II system.

Criteria:

DOJ 2640.2D CHAPTER 2 Section 16, states: "Access controls shall be in place and operational for all Department IT systems to:…. Protect the system, its data and applications, from unauthorized disclosure, modification, or erasure."

Risk:

Without properly configured security settings on operating systems, attackers can compromise the ITS II.

Recommendation:

11. We recommend that the BOP Director ensure that BOP management develop a configuration standard for all systems that incorporate the most restrictive security settings possible. In addition, the BOP should implement all the recommendations outlined in the ST&E report.

F. Data Integrity. Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality and integrity.

Issue: Integrity and Validation Controls

Condition:

Currently, the integrity and validation controls for the ITS II are not adequate. No Intrusion Detection System (IDS) has been installed on ITS II and no integrity verification programs are being used.

Cause:

The BOP does not have policy on the use of an IDS and integrity verification programs. Additionally, the BOP lacks policy on system penetration testing.

Criteria:

DOJ Order 2640.2D Chapter 2 Section 16, states: "Access controls shall be in place and operational for all Department IT systems to:.… Protect the system, its data and applications, from unauthorized disclosure, modification, or erasure."

Risk:

The lack of these controls creates an inability to ensure data integrity and to validate data. This could potentially cause BOP to be vulnerable to unauthorized data modifications. The lack of an IDS also leaves administrators without the benefit of advanced notice of unusual network or system activity. Without the warning an IDS can provide, it is more difficult to respond effectively to suspicious activity.

Recommendation:

12. We recommend that the BOP Director ensure that BOP management develop policies and procedures surrounding the use of intrusion detection software and integrity validation software and implement these policies and procedures on critical servers.

G. Incident Response Capability. Computer security incidents are an adverse event in a computer system or network. Such incidents are becoming more common and their impact is far-reaching.

Issue: Incident Handling

Condition:

In reviewing ITS II, we found the BOP's response, handling, and support procedures for security incidents are not adequate. BOP does not have a formal incident response capability implemented and information concerning incidents does not appear to be disseminated to appropriate personnel or organizations.

Cause:

The BOP does not have a policy addressing incident handling and response, or that addresses how personnel shall be trained to respond.

Criteria:

DOJ Order 2640.2D Chapter 1 Section 5, states: "For SBU systems, security incidents that meet the criteria established by the DOJ Computer Emergency Response Team (DOJCERT) shall be reported by the component to DOJCERT within time frames established by DOJCERT. For classified systems, the component shall immediately report to the Department Security Officer (DSO) any incident involving the loss, compromise, or other event affecting the security of a classified system."

Risk:

Incidents that the BOP may encounter run the risk of not being properly handled. The correct or appropriate resolution may not be reached and responsible individuals may not be informed of the incident. Also, by not sharing incident information with other organizations, a common attack or virus outbreak with a known resolution will not be as easily solved for BOP or other affected organizations.

Recommendation:

13. We recommend that the BOP Director ensure that BOP management develop a policy for incident handling, response, and personnel support.

III. Technical Controls. Technical controls focus on security controls that the computer system executes and depend upon the proper functioning of the system to be effective. Technical controls require significant operational considerations and should be consistent with the management of security within the organization.

Technical Controls	Vulnerabilities Noted
Identification and Authentication	√*
Logical Access Controls	√*
Audit Trails	√

√* Significant vulnerabilities in which risk was noted as high. A high-risk vulnerability is defined as one where extremely grave circumstances can occur by allowing a remote or local attacker to violate the security protection of a system through user or root account access, gaining complete control of a system and compromising critical information.

A. Identification and Authentication. Identification and authentication are technical measures that prevent unauthorized people or processes from entering an IT system. Identification, most commonly used for access control, is the means in which users claim their identities to a system. Authentication is verification that a person's claimed identity is valid and is usually implemented through the use of passwords.

Issue: Password Management

A password is a unique string of characters that must be provided before a logon or 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. The BOP password controls were found to be inadequate.

Condition:

- The password policy on the BOPCOF server allows blank passwords.
- The minimum password age policy is set too low allowing password changes too soon on both BOPCOF and BOPCO1 servers.
- The password history is set to less than 10 on both BOPCOF and BOPCO1 servers.
- The service pack enhancement Passfilt is not being used on the BOPCOF server.

- The resource kit utility, 'passprop', is not being utilized on both BOPCOF and BOPCO1 servers.

- The account lockout feature is not adequately set on BOPCOF and BOPCO1 servers.

- The Administrator account password is blank on the BOPCOF server.

- Nineteen users have the "password never expires" setting on the BOPCO1 server and two users have this setting on the BOPCOF server.

- The PASSLENGTH variable is set to six characters on the BOP UNIX server.

- The MAXWEEKS variable is set to 0 weeks.

- An EEPROM password has not been set.

Cause:

These vulnerabilities occurred because BOP management did not enforce compliance with Department password policies and procedures.

Criteria:

DOJ Order 2640.2D requires the Department's IT systems to implement eight-character password composed of at least three of the following: English uppercase, English lower case, numeric, and special characters. In addition, the Department's IT systems should comply with Department password management policy (DOJ-TS-001).

Risk:

Without strong password management controls, the BOP increases the risk that unauthorized persons could access sensitive ITS II resources, exposing information to unauthorized use, loss, or modification.

Recommendation:

14. We recommend that the BOP Director ensure that BOP management enforce formal Department password policies and procedures and install and activate a password filter on all servers to enforce parameters that enforce restrictions on passwords.

B. Logical Access Control. Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted.

Issue: Access Controls

Condition:

We found logical access controls were inadequate for restricting user activities and network access. On the network, insecure protocols are being used with the router, no formal procedures exist for changing vendor-supplied default security parameters, idle sessions are not disconnected, and no formal policy or procedures exist for firewalls.

Cause:

The BOP management did not develop documented policy and procedures dictating the implementation and use of access control software for the prevention of fraudulent activity.

Criteria:

DOJ Order 2640.2D Chapter 2 Section 16, states: "Access controls shall be in place and operational for all Department IT systems to:… Protect the system, its data and applications, from unauthorized disclosure, modification, or erasure."

Risk:

Without access controls in place, BOP management is unable to prevent an individual from committing fraud.

Recommendation:

15. We recommend that the BOP Director ensure that BOP management develop, implement, and monitor documented policy establishing specific security standards and settings for access controls. At a minimum, these standards and settings should:

    a. Establish policy and procedures for disabling insecure protocols.

    b. Establish policy dictating the reset of vendor default security parameters to more secure settings.

c. Configure network connections to automatically disconnect.

d. Establish standard firewall procedures for configuring the firewall.

e. Restrict access to tables defining network options, resources, and operator profiles.

Issue: User Authentication and Access

Condition:

User authentication and access is not properly controlled on the ITS II network. Specifically:

- Access scripts with embedded passwords are not prohibited.
- Service and administrator accounts have weak passwords.
- Inactive user accounts are not disabled after a specific period of time.
- Lost or compromised passwords are handled inappropriately.
- No formal procedures for replacing vendor-supplied passwords.
- Data owners do not periodically review access authorizations to determine whether they remain appropriate.

Cause:

The ITS II management did not have documented procedures for monitoring access scripts with embedded passwords, disabling inactive user accounts, handling lost or compromised passwords, replacing vendor-supplied passwords, service and administrator accounts with weak passwords, and data owners ability to review access authorizations so that only individuals with a need to know can access files.

Criteria:

DOJ Order 2640.2D Chapter 2 Section 16, states: "Access controls shall be in place and operational for all Department IT systems to: … Protect the system, its data and applications, from unauthorized disclosure, modification, or erasure."

Risk:

Without periodic review of access permissions, it is possible that individuals without a legitimate need may gain access to sensitive information.

Recommendation:

16. We recommend that the BOP Director ensure that BOP management develop, implement, and monitor documented policy establishing specific security standards and settings for user authentication and access. At a minimum, these standards and settings should:

    a. Prohibit the use of access scripts with embedded passwords.

    b. Require data owners to review access authorizations to determine whether they remain appropriate.

Issue: Server Configuration

Condition:

- The system key (SYSKEY) on the Windows NT servers was disabled. Enabling this option decreases the risk that password hashes will be cracked if obtained. A utility has been released that can extract the Windows NT password hashes even with SYSKEY enabled; therefore, this risk is only partially mitigated.

- Fifteen of the services on BOPCO1 and nine of the services on BOPCOF are running in an insecure context. If services running as LocalSystem are allowed to interact with the desktop, there is an increased risk that domain resources may be compromised by a locally logged on user who would have system access to server resources. If the service is compromised by an unauthorized user, they would be able to access any resources available to the user account under which it is running.

- BOPCO1 is running the spooler service, which for a Primary Domain Controller (PDC) is an unnecessary service. Both BOPCOF and BOPCO1 are running the "messenger" and "alerter" services. Running unnecessary applications, services or protocols opens the server to any vulnerabilities that exist within each one.

- For UNIX, the BOPNNM server is running nine extraneous services.

- On the Cisco router, finger and Cisco discovery protocol are running.

Cause:

The BOP management did not develop documented procedures regarding the implementation of the system key utility. In addition, services such as LocalSystem, in "interactive" mode, and "spooler" are running on the server.

Criteria:

DOJ Order 2640.2D Chapter 2 Section 16, states: "Access controls shall be in place and operational for all Department IT systems to:…. Protect the system, its data and applications, from unauthorized disclosure, modification, or erasure."

NIST Interagency Reports (NISTIR) 5153 Section 3.2.2, states: "Each resource delivered with the system shall have the most restrictive access rights possible to permit the intended use of that resource."

Risk:

These services pose a risk to the system in that many are known to either present system users' information or have known vulnerabilities.

Recommendation:

17. We recommend that the BOP Director ensure that BOP management:

    a. implement the system key utility and restrict services so that they are running in a secure context; and

    b. ensure the removal of all unnecessary services.

Issue: Networking Controls

Networking controls access the system from the network. These controls are a front-line defense for the system against intruders.

Condition:

Specifically, we found:

- Of the two Windows NT servers tested, the auditors discovered both BOPCO1 and BOPCOF allow users to login with cached login information. This means the user name information of the last user is already provided at the login prompt. With this information provided,

an attacker already has 50 percent of the login information required to gain access to the system.

- Routing updates sent by a router may advertise internal network topologies to groups or third parties that may be untrusted. In addition, interfaces that routinely advertise routing information may impede network efficiency, especially if neighboring routers are using other routing protocols or using static routes.

Cause:

The BOP management did not develop documented procedures for networking controls.

Criteria:

DOJ Order 2640.2D Chapter 2 Section 16, states: "Access controls shall be in place and operational for all Department IT systems to:…. Protect the system, its data and applications, from unauthorized disclosure, modification, or erasure."

Risk:

Without formal networking control procedures, ITS II user logon information is vulnerable in the event of an unauthorized user gaining access to the system.

Recommendation:

18. We recommend that the BOP Director ensure that BOP management develop, implement, and monitor documented policy establishing specific security standards and settings for networking controls. At a minimum, these standards and settings should include:

    a. The registry key on Windows NT servers, HKLM\Software\Microsoft\WindowsNT\CurrentVersion \Winlogon\CachedLogonsCount, should be set to 0.

    b. The command on routers in global configuration mode: Passive-interface type number where "type" refers to the interface type and "number" is the interface number.

Issue: User and Group Management Controls

Management of users and groups is key to controlling access to the system. Proper user and group management can help to enhance overall system security.

Condition:

Specifically, we found:

- Accounts that have not been logged into for an extended period of time have not been disabled on both BOPCOF and BOPCO1. Having outstanding accounts that are no longer needed increases the risk of unauthorized access.

- The default administrator accounts need to be renamed and given strong passwords on BOPCOF and BOPCO1. The 'Administrator' accounts are known to exist on all Windows NT systems. Consequently, they are among the first accounts that an intruder will attempt to use. The 'Administrator' account on Windows NT has all system rights and therefore should be the most protected account on the system. If these accounts are not renamed, an attacker would only need to guess the password. Depending on other system settings, this might be easy to achieve in a relatively short period of time without being detected.

- The BOPCOF\Domain Users group is a member of the Local Administrators group. The resulting effect is Domain users, which are members of the local administrators group, have administrator access to the server.

- The special group “Everyone” is being used on the BOPCOF and BOPCO1 servers. Access control lists for files and directories include the “Everyone” group on BOPCOF. The special group “Everyone” is anyone, to includes domain users, null session connections, and other trusted domain users. Using the special group “Everyone” is very broad and could inadvertently allow an intruder to gain access to system resources.

- An FTP users file (/etc/ftpusers) has not been created to restrict FTP access to authorized users.

Cause:

The ITS II management lack procedures for renaming the administrator and guest accounts and assigning strong passwords. In addition, account activity is not being reviewed on a regular basis.

Criteria:

NISTIR 5153 Section 3.2.2, states: "Each resource delivered with the system shall have the most restrictive access rights possible to permit the intended use of that resource."

DOJ Order 2640.2D Chapter 2 Section 16, states: "Access controls shall be in place and operational for all Department IT systems to: … Protect the system, its data and applications, from unauthorized disclosure, modification, or erasure."

Federal Bureau of Prisons (FBOP) 1237.11, *Information Security Programs,* Section 6, Paragraph b, regarding Movement of Personnel, states: "A new user ID shall be issued at a staff member's new duty station. The ISO at the transferring location shall disable the old user ID within one working day of the employee's departure and delete the ID within 30 days. For a SENTRY ID that cannot be created at the new duty station, use procedures prescribed in c.(3), following. On the UNICOR MCS system, the old user ID shall be permanently disabled, rather than deleted. For all involuntary separations and home duty assignments, the departing employee's access to all computer systems shall be immediately disabled and his/her supervisor or the ISO shall confiscate accessible media. For routine voluntary permanent separations, the employee's access shall be terminated no later than one working day following departure."

Risk:

Without the existence of the /etc/ftpusers file, any user listed in the /etc/passwd file can transfer files across the network. This increases the risk that unauthorized files are transferred across the network. In addition, the 'Administrator' account is known to exist on all Windows NT systems. Consequently, it is among the first accounts that an intruder will attempt to use. The 'Administrator' account on Windows NT has all system rights and therefore should be the most protected account on the system. If the account is not renamed, an attacker would only have to guess the password. Depending on other system settings, this might be easy to achieve in a relatively short period of time without being detected.

Recommendation:

19. We recommend that the BOP Director ensure that BOP management develop, implement, and monitor documented policy establishing specific security standards and settings for user and group management controls. At a minimum, these standards and settings should include:

    a. Review user account activity and disable or remove accounts that have been inactive for an extended period of time or are no longer needed.

    b. Develop procedures for renaming the Administrator accounts and assigning strong passwords that are a minimum of eight characters and contain alphanumeric and special characters.

    c. Remove domain users from the local administrator group.

    d. Replace references to the special group 'Everyone' with 'Domain users', 'Authenticated Users' or Domain application groups.

    e. Create the /etc/ftpusers file.

Issue: 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 reserved for users involved in programming efforts.

Typically, administrators can create two types of accounts—user and group accounts. A user account belongs to one person only; rights assigned affect only that account. A group account is a collection of users with common rights. In addition, to maintain account integrity, users must be clearly identified on the system in order to track their use of system resources. Account integrity is also strengthened by renaming Administrator and Guest accounts to make them unidentifiable to unauthorized users and making sure that users can be clearly identified in order to track their use of system resources.

Condition:

Specifically, we found:

- Unauthenticated users can access this computer from the network. Lack of a standard user rights assignment policy for Windows NT users allows the \Everyone group to access this computer from the network. The special \Everyone group includes unauthenticated users.

- On BOPCOF the Local Administrators group has "Backup files and Directories" right. There should be a segregation of duties between administrators, users, and individuals who can backup files. Individuals with this user right can bypass the access control list (ACL) of a file and read any file. This is an issue because the domain users group is also a member of the local administrators group.

- The "Change the system time" standard user right is not restricted on BOPCO1. Accuracy of the system time is a prerequisite for an audit trail because knowing who was accessing resources at a specified time could implicate a user. The entire audit, event monitoring, and logging system is based on time and therefore, requires that time not be tampered with. Security policies, such as those for account lockout and expiration, are based on the system time.

- The "Log on locally" standard user is not restricted on BOPCOF. Although, a security control inherent in Windows NT is that the first entry in the new log states that the old log was cleared and by whom. Only authorized individuals, such as the Security Officer or the Internal Auditor, should be given this right. Those types of individuals should be members of an auditors group.

- The "Restore file and directories" standard user right is not restricted. There should be a segregation of duties between Administrators, users, and individuals who can restore files. Individuals with this user right can bypass the ACL of a file and read or write to any file on the server.

- The "Shut down the system" standard user right is not restricted on both servers. Individuals who can shut down the Primary Domain Controller (PDC) could cause a denial of service or degrade the performance of the network performance subject to Backup Domain Controller (BDC) configurations.

- The "Take ownership of files or other objects" standard user right is not restricted on BOPCOF. This is a very powerful user right because

individuals can ignore the ACL of an object, take ownership of the object, and change the ACL.

- The 'Act as Part of the Operating System' advanced user right is not restricted on BOPCO1. The right is one of the most powerful rights within Windows NT. It allows the designated accounts to act as a trusted part of the operating system and can therefore perform any activity regardless of other rights.

- The "Log on as a service" advanced user right is not restricted on both servers. The "Log on as a Service" right allows a user to log on as a service, similar to those required by virus scanners and faxing software. These services run in the background without any interaction from any additional users. Some services have full control over the system and could be very powerful if configured in that manner.

- "Increase scheduling priority" and "profile single process" advanced user rights are assigned inappropriately on BOPCOF. These advanced user rights could be used to compromise the PDC if they are granted to the wrong individuals other than administrators. The advanced rights are very powerful and do not need to be granted to normal users.

Cause:

The BOP management did not develop a documented user rights assignment policy.

Criteria:

DOJ Order 2640.2D Chapter 2 Section 16, states: "Access controls shall be in place and operational for all Department IT systems to:…. Enable the use of resources such as data and programs necessary to fulfill job responsibilities and no more."

Risk:

Without policy and procedures in place for account integrity management, ITS II is exposed to attacks from unauthenticated users.

Recommendation:

20. We recommend that the Director of the BOP ensure that BOP management develop, implement, and monitor documented policy establishing specific security standards and settings for account integrity management. At a minimum, these standards and settings should include:

    a. "Log on locally,"

    b. "Access this computer from the network,"

    c. "Restore files and directories,"

    d. "Shut down the system,"

    e. "Take ownership of files or other objects,"

    f. "Act as part of the operating system,"

    g. "Log on as a service," and

    h. "Increase scheduling priority."

Issue: File System Access

Access to the file system can be controlled at the group or user level. Inappropriate settings for file system access can leave sensitive system information vulnerable to unauthorized disclosure or modifications.

Condition:

Specifically, we found:

- The \Everyone group has access to directories containing applications or sensitive files. The special group 'Everyone' is anyone, to include domain users, null session connections, and other trusted domain users. Using the special group 'Everyone' is very broad and could inadvertently allow an intruder to gain access to system resources.

- Users without a legitimate business requirement have access to sensitive system utilities in the \winnt directory. If user accounts are granted access to potentially sensitive utilities there is an increased risk that the user may gain information that could be used to compromise the security

of the domain, or perform actions that may affect the security and productivity of the domain.

- The BOPNNM server has an excessive number of world-writeable files and directories. Files that are world-writeable allow any user on the system the ability to modify or delete their contents. Improper permissions on home directories could potentially allow a user to obtain the level of access of another ID on the server. If the compromised ID is business-critical, then this vulnerability is high-risk and could be exploited to gain privileged access on the server.

- Network File System (NFS) shares are not adequately secured. Read, write, and export to the world permissions exist on one of the directories. NFS exported directories could potentially expose the NFS servers to greater risk. It is possible to "mis-configure" the NFS export file and potentially allow remote users from NFS clients to gain root access on the NFS server.

Cause:

The BOP security management did not develop documented procedures for exporting and sharing users' directories.

Criteria:

DOJ Order 2640.2D Chapter 2 Section 16, states: "Access controls shall be in place and operational for all Department IT systems to:…. Protect the system, its data and applications, from unauthorized disclosure, modification, or erasure."

Risk:

Without ITS II procedures in place, NFS directories exported to everyone can be mounted by any remote user without authentication. An attacker does not need to actually break into a remote system. Instead, all that is necessary is to mount a file system via NFS.

Recommendation:

21. We recommend that the BOP Director ensure that BOP management develop, implement, and monitor documented policy establishing specific security standards and settings for file system access. At a minimum, these standards and settings should:

    a. Replace references to the special group 'Everyone' with 'Domain users', 'Authenticated Users', or Domain application groups.

b. Remove access to sensitive system utilities from accounts that do not require access.

c. Review and remove unnecessary permissions on files and directories.

d. Restrict access to the network file system shares.

Issue: Maintenance Controls

For purposes of the operating system server review, maintenance controls relate to standard user profiles and the use of password protected screen savers and login warning banners.

Condition:

- On BOPCOF, a password protected screen saver is not being used.
- The Unix server does not display a system warning message when users log on the server.

Cause:

The BOP management currently is not following policy regarding password protected screen savers and system warning banners.

Criteria:

FBOP 1237.11, 6.h.2 states: "All personal computers designated as sensitive systems or "STAFF ONLY" shall have software that will, after a specified period of keyboard inactivity, blank the display and require a password for further access. The maximum time of inactivity shall be 10 minutes. All Novell or Windows NT workstations shall use software requiring the network password. This shall be adequate for a staff member to leave a workstation unattended for a short period. The Bureau standard, related requirements, and exceptions are stated in the previous subsection."

DOJ Order 2640.2D Chapter 2 Section 20, states: "All Department IT systems shall implement a system banner that provides warnings: to employees that accessing the system constitutes consent to system monitoring for law enforcement and other purposes; and to unauthorized users that their use of the system may subject them to criminal prosecution and/or criminal or civil penalties."

Risk:

By not enabling the Windows NT screen saver with password protection, risk is increased that the server will be exposed to unauthorized access when left unattended. BOP's ability to prosecute criminals may be impacted by the BOP's ability to prove they abused BOP systems with the knowledge these systems were supposed to be used only for official purposes. Also, it is a good practice to proactively inform users that they are subject to audit.

Recommendation:

22. We recommend that the Director of the BOP ensure that BOP management develop, implement, and monitor documented policy establishing specific security standards and settings for maintenance controls. At a minimum, these standards and settings should:

    a. Enable a password protected screen saver on the server.

    b. Display a system-warning message when users log on the server.

Issue: NT Registry Settings

A registry is a database used by the Windows NT operating to store configuration information. Most Windows applications write data to the registry, at least during installation.

Condition:

- Users, besides administrators, can install print drivers.
- The CD-ROM and floppy drives are accessible to users not logged on locally.
- Unauthenticated users can read the RunOnce registry key.
- Unauthenticated users can read the PerfLib, WinLogon, and LSA registry keys.
- Unauthenticated users have access to 17 registry keys that contain server configuration information.
- Unauthenticated users can query information from the server.

- A Default user name is displayed at login.
- There are no restrictions on who can define system attributes.
- Idle users are not disconnected after 15 minutes.
- Pagefile is not cleared at shutdown.
- Integrity checking is not being performed.
- The LMCompatibilityLever registry key is not securely set.
- The minimum security that is used for programs that use the NTLM Security Support Provider (SSP), or uses secure Remote Procedure Call [RPC] is not specified.
- Server Message Block (SMB) Signing is not being used.
- Users are allowed to schedule jobs on the server.
- Guests can view the system event and system application logs.

Cause:

The ITS II management did not develop documented standard configuration policy for securing Windows NT registry settings.

Criteria:

DOJ Order 2640.2D Chapter 2 Section 16, states: "Access controls shall be in place and operational for all Department IT systems to:…. Protect the system, its data and applications, from unauthorized disclosure, modification, or erasure."

Risk:

By not having the registry keys set to their most secure setting, the system is vulnerable to misuse and overall system security is weakened.

Recommendations:

23. We recommend that the BOP Director ensure that BOP management develop, implement, and monitor documented policy establishing specific security standards and settings for NT registry settings. At a

minimum, these standards and settings should include reconfiguring the registry settings to a more secure configuration.

Issue: Security Patches

Security patches contain update information for the operating system that correct bugs or vulnerabilities in the software.

Condition:

The operating system software is not kept up to date with respect to security patches.

Cause:

The ITS II management has not developed documented procedures for updating computer security patches.

Criteria:

NIST SP 800-13 Section 5.10, *Telecommunications Security Guidelines for Telecommunications Management Network*, states: "All new software features and patches shall be tested first on a development system and approved by an appropriate testing organization, prior to installation on an operational system. Tests that modify live data shall not be performed. A risk analysis shall be conducted of proposed software changes to determine their impact on network element (NE) security. Any changes to security features or security defaults shall be documented and made available to the user before the software is distributed."

Risk:

If the version of the operating system and the security patches are not current, there is an increased risk that an unauthorized user may be able to exploit weaknesses.

Recommendation:

24. We recommend that the BOP Director ensure that BOP management obtain the latest security patches from the operating system vendor. The patches should be properly installed and configured.

Issue: Router Configuration

Condition:

- Source routing can be used to bypass the router's route tables and potentially gain access to unauthorized portions of the network.

- Administrators can use the Internet protocol (IP) alias command to assign multiple IP addresses to the router. For example, in addition to the primary alias address, addresses can be specified that correspond to lines or rotary groups. Using the IP alias command in this way makes the process of connecting to a specific rotary group transparent to the user. If the IP alias command is enabled on Cisco products, transmission control protocol (TCP) connections to any destination port are considered valid connections.

- The TCP intercept feature helps prevent SYN-flooding attacks by intercepting and validating TCP connection requests. In intercept mode, the TCP intercept software intercepts SYN packets from clients to servers that match an extended access list. The software establishes a connection with the client on behalf of the destination server, and if successful, establishes the connection with the server on behalf of the client and knits the two half-connections together transparently. Thus, connection attempts from unreachable hosts will never reach the server. The software continues to intercept and forward packets throughout the duration of the connection. In the case of illegitimate requests, the software's aggressive timeouts on half-open connections and its thresholds on TCP connection requests protect destination servers while still allowing valid requests.

- Encryption is not being used on the router. Sensitive information may be the target of sniffing attacks by unauthorized users. If transactions are occurring that contain highly confidential information, it may be vulnerable to sniffing if it is not encrypted. Hash algorithms will help mitigate against a loss of data integrity should the data be manipulated in transit.

Cause:

The ITS II management has not properly configured the Cisco router.

Criteria:

DOJ Order 2640.2D Chapter 2 Section 16, states: "Access controls shall be in place and operational for all Department IT systems to:…. Protect the

system, its data and applications, from unauthorized disclosure, modification, or erasure."

Risk:

Without properly configuring the Cisco router, attackers can potentially gain access to unauthorized portions of the network.

Recommendation:

25. We recommend that the Director of the BOP ensure that BOP management develop, implement, and monitor documented policy establishing specific security standards and settings for router configuration. At a minimum, these standards and settings should:

    a. Issue the "no ip source-route" command in interface configuration mode.

    b. Issue the "no ip alias" command in configuration mode.

    c. Issue the command: "ip tcp intercept list yyy," (where yyy is the access list number to which the connections will be intercepted), in configuration mode.

    d. Enable encryption via the "crypto map" command.

Issue: Fail-over Capabilities

Fail-over is hardware or software backup to which the system switches to in the event of a failure.

Condition:

The Cisco's fail-over capabilities are not in place.

Cause:

The BOP ITS II security management did not develop documented configuration standards for securing BOP's Cisco routers. In addition, Cisco's hot standby router protocol (HSRP) fail-over capability has not been implemented on the router.

Criteria:

DOJ Order 2640.2D Chapter 2 Section 16, states: "Access controls shall be in place and operational for all Department IT systems to:…. Protect the system, its data and applications, from unauthorized disclosure, modification, or erasure."

Risk:

Cisco internet operating system (IOS) and hardware offers advanced fail-over capabilities in case of hardware or software failure. Mission critical routers (typically core routers) may be good candidates to take advantage of the Cisco fail-over capabilities.

Recommendation:

26. We recommend that the BOP Director ensure that BOP management implement Cisco's fail-over capabilities by configuring HSRP on critical external routers.

Issue: Command Line Access

Information on the router configuration can be retrieved or entered via command-line access.

Condition:

- Different levels of PRIV EXEC access have not been defined. It may not be necessary for all administrators or users to have full privileged access to the router. Administrators that do not require this functionality can make unauthorized changes to the configuration.

- Anyone on the BOP network can access a login prompt to the router. Allowing anyone on the network access to the login prompt increases the risk of unauthorized access to the router.

- Telnet is being used to access the router. Telnet sessions transmit information, including usernames and passwords, in clear text. If an unauthorized user were to capture this information, it may place critical network devices at risk of compromise.

- AAA (Authentication, Authorization, and Accounting) has not been implemented. AAA provides for more granular levels of accounting and access privileges. These can be helpful in complex environments

where resources are being accessed by different users in multiple ways.

- Timeout values have not been assigned to all console terminals on the router. Timeout sessions provide additional security against consoles that are left unattended. If a user can gain access to a console left unattended they can modify the router's configuration.

Cause:

The BOP management did not develop documented configuration standards for securing BOP's Cisco routers.

Criteria:

DOJ Order 2640.2D Chapter 2 Section 16, states: "Access controls shall be in place and operational for all Department IT systems to: Protect the system, its data and applications, from unauthorized disclosure, modification, or erasure."

Risk:

Allowing anyone on the network access to the login prompt increases the risk of unauthorized access to the router.

Recommendation:

27. We recommend that the Director of the BOP ensure that BOP management develop, implement, and monitor documented policy establishing specific security standards and settings for command line access. At a minimum, these standards and settings should include:

    a. Enter the following command: privilege level command, in global configuration mode.

    b. Create an appropriate access-list using the access-list command in configuration mode. Once the access list has been created, apply it to the appropriate terminal (typically vty 0 4) using the access-group <basic access list number> in command.

    c. Enable SSH on the router.

    d. Enable Authentication, Authorization, and Accounting.

e. Establish a session timeout.

C. Audit Trails. Auditing provides the ability to detect and record security-related events. It tracks the activities of users by recording information 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 in a security log on the server.

Issue: Activity Logs

Condition:

System activities are not adequately logged and reviewed on a regular basis on the BOP ITS II system.

Cause:

The ITS II management did not develop procedures for collecting, reviewing and archiving activity logs.

Criteria:

DOJ Order 2640.2D Chapter 2, Section 19, states: "Department IT systems shall:

1. Maintain an audit trail of activity sufficient to reconstruct security relevant events.

2. Include in the audit trail the identity of each entity accessing the system, time and date of the access, time and date the entity terminated access, activities performed using an administrator's identification, and activities that could modify, bypass, or negate the system's security safeguards.

3. Protect the audit trail from actions such as unauthorized access, modification, and destruction that would negate its forensic value.

4. Retain the audit trail for a period of 90 days, the minimum record retention period specified by the component, or the period specified in the system security plan, whichever is longer.

    a. Audit trails shall be reviewed in compliance with the review period specified for the audit trail in the system's security plan.

b. IT systems operating in the Dedicated Mode of Operation or in a stand-alone environment that do not implement an audit trail must be justified and documented in the risk analysis and certification process."

Risk:

Insufficient logging will result in the lack of an audit trail in the event of unauthorized access or use. Insufficient reviewing of audit logs will result in administrators not being alerted to any unauthorized activity as early as possible. Also, with good logging and monitoring, administrators are often given early warnings for hardware and software errors or problems.

Recommendation:

28. We recommend that the BOP Director ensure that BOP management develop procedures for logging and monitoring system activity and require that audit logs be reviewed periodically.

CONCLUSION

Our review disclosed that security controls need improvement to fully protect the ITS II from unauthorized use, loss, or modification. Specifically, we found security vulnerabilities in the areas of life cycle, authorize processing, system security plan, personnel security, physical and environmental protection, production, input/output controls, contingency planning, hardware and systems software maintenance, data integrity, incident response capability, identification and authentication, logical access controls, and audit trails.

We concluded that these vulnerabilities occurred because BOP management did not fully develop, document, or enforce agency-wide policies in accordance with current Department policies and procedures. Additionally, the Department did not enforce its security policies and procedures to ensure the ITS II was protected from unauthorized use, loss, or modification through its certification and accreditation process.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY GENERAL CONTROL AREAS

The review focused on evaluating the adequacy of management, operational and technical controls over the following specific control areas:

I. MANAGEMENT CONTROLS. Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management.

- **Risk Management**. Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. Assessing risk management involves evaluating the BOP's efforts to complete the following critical procedures:

  - Periodic performance of a system risk assessment had been performed.
  - Program officials understand the risk to systems under their control and had determined the acceptable level of risk.

- **Review of Security Controls.** Routine evaluations and response to identified vulnerabilities are important elements of managing security controls of a system. Determining whether review of security controls had been adequately performed requires the auditor to assess if the following critical items were completed:

  - A system security control review had been performed for both ITS II and interconnected systems.
  - Management ensured effective implementation of corrective actions.

- **Life Cycle.** Like other aspects of an IT system, security is best managed if planned for throughout the IT system life cycle. There are many models for the IT system life cycle but most contain five basic phases: initiation, development/acquisition, implementation, operation, and disposal. Assessing a system's life cycle involves identifying if the following critical items are in place for the ITS II:

  - A system development life cycle methodology.
  - System change controls as programs progress through testing to final approval.

- **Authorize Processing (Certification and Accreditation).** Authorize processing (also referred to as certification and accreditation) provides a form of assurance of the security of the system. To determine whether the ITS II had been appropriately authorized to process data involves analyzing critical documents that identify whether:

    - The system had been certified/recertified and authorized to process (accredited).
    - The system is operating on an interim authority in accordance with specified agency procedures.

- **System Security Plan.** A system security plan provides an overview of the security requirements of the system and describes the controls in place or planned for meeting those requirements. The plan delineates responsibilities and expected behavior of all individuals who access the system. Assessing whether the ITS II has an adequate system security plan requires identifying if the following critical elements were met:

    - A system security plan had been documented for the system and all interconnected systems if the boundary controls are ineffective.
    - The plan is kept current.

II. OPERATIONAL CONTROLS. Operational controls address security controls that are implemented and executed by people. These controls are put in place to improve the security of a particular system. They often require technical or specialized expertise and rely upon management activities as well as technical controls.

- **Personnel Security.** Many important issues in computer security involve human users, designers, implementers, and managers. A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their jobs. Assessing personnel security involves evaluating the BOP efforts to complete the following critical procedures:

    - Duties are separated to ensure least privilege and individual accountability.
    - Appropriate background screening is completed.

- **Physical and Environmental Protection.** Physical security and environmental security are the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. Assessing physical and environmental protection involves evaluating the BOP efforts to complete the following critical procedures:

    - Adequate physical security controls have been implemented and are commensurate with the risks of physical damage or access.
    - Data is protected from interception.
    - Mobile and portable systems are protected.

- **Production, Input/Output Controls.** There are many aspects to supporting IT operations. Topics range from a user help desk to procedures for storing, handling, and destroying media. Assessing production, input/output controls involves evaluating the BOP efforts to complete the following critical procedures:

    - User support is being provided to ITS II users.
    - Media controls are in place for the ITS II.

- **Contingency Planning.** Contingency planning ensures continued operations by minimizing the risk of events that could disrupt normal operations and having an approach in place to respond to those events should they occur. Assessing contingency planning involves evaluating the BOP's efforts to complete the following critical procedures:

    - Identify the most critical and sensitive operations and their supporting computer resources.
    - Develop and document a comprehensive contingency plan.
    - Have tested contingency/disaster recovery plans in place.

- **Hardware and System Software Maintenance**. These are controls used to monitor the installation of, and updates to, hardware and software to ensure that the system functions as expected and that a historical record is maintained of changes. Some of these controls are also covered in the Life Cycle Section. Assessing hardware and system software maintenance involves evaluating the BOP efforts to complete the following critical procedures:

    - Access is limited to system software and hardware.
    - All new and revised hardware and software are authorized, tested and approved before implementation.

- Systems are managed to reduce vulnerabilities.

- **Data Integrity.** Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality and integrity. Assessing data integrity involves evaluating the BOP efforts to complete the following critical procedures:

  - Virus detection and elimination software is installed and activated.
  - Data integrity and validation controls are used to provide assurance that the information has not been altered and the system functions as intended.

- **Documentation.** The documentation contains descriptions of the hardware, software, policies, standards, procedures, and approvals related to the system and formalize the system's security controls. Assessing documentation involves evaluating the BOP's efforts to complete the following critical procedures:

  - There is sufficient documentation that explains how software/hardware is to be used.
  - There are documented formal security and operational procedures.

- **Security Awareness, Training, and Education.** People are a crucial factor in ensuring the security of computer systems and valuable information resources. Security awareness, training, and education enhance security by improving awareness of the need to protect system resources. Additionally, training develops skills and knowledge so computer users can perform their jobs more securely and build in-depth knowledge. Assessing security awareness, training, and education involves evaluating the BOP efforts to complete the following critical procedures:

  - Employees have received adequate training to fulfill their security responsibilities.

- **Incident Response Capability.** Computer security incidents are an adverse event in a computer system or network. Such incidents are becoming more common and their impact is far-reaching. The following questions are organized according to two critical elements. Assessing incident response capability involves evaluating the BOP efforts to complete the following critical procedures:

- There is a capability to provide help to users when a security incident occurs in the system.
- Incident related information is shared with appropriate organizations.

III. TECHNICAL CONTROLS. Technical controls focus on security controls that the computer system executes and depend upon the proper functioning of the system to be effective. Technical controls require significant operational considerations and should be consistent with the management of security within the organization.

- **Identification and Authentication.** Identification and authentication is a technical measure that prevents unauthorized people or processes from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. Authentication is verification that a person's claimed identity is valid and it is usually implemented through the use of passwords. Assessing identification and authentication involves evaluating the BOP's efforts to complete the following critical procedures:

  - Users are individually authenticated via passwords and other devices.
  - Access controls are enforcing segregation of duties.

- **Logical Access Controls.** Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. Assessing logical access controls involves evaluating the BOP's efforts to complete the following critical procedures:

  - Logical access controls restrict users to authorized transactions and functions.
  - There are logical controls over network access.
  - There are controls implemented to protect the integrity of the application and the confidence of the public when the public accesses the system.

- **Audit Trails.** Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems. Assessing audit trails

involves evaluating the BOP's efforts to complete the following critical procedures:

- Activity involving access to and modification of sensitive or critical files is logged and monitored and possible security violations are investigated.

APPENDIX II

U.S. Department of Justice

Federal Bureau of Prisons

Office of the Director

Washington, DC 20534

October 25, 2002

MEMORANDUM FOR GUY K. ZIMMERMAN
ASSISTANT INSPECTOR GENERAL
FOR AUDIT

FROM: Kathleen Hawk Sawyer, Director
Federal Bureau of Prisons

SUBJECT: Response to the Office of the Inspector General's (OIG) Draft Audit Report: The Bureau of Prisons Inmate Telephone System Independent Evaluation Pursuant to the Government Information Security Reform Act Fiscal Year 2002

The Bureau of Prisons (BOP) appreciates the opportunity to respond to the recommendations from the OIG's draft report entitled The Bureau of Prisons Inmate Telephone System Independent Evaluation Pursuant to the Government Information Security Reform Act Fiscal Year 2002. The BOP understands the risks associated with computer systems and communication networks and works diligently to reduce security vulnerabilities associated with them. This report makes several recommendations that will assist us in reducing these risks.

The OIG points out several areas of vulnerability and two areas of high risk. The OIG also documented areas of improvements or satisfactory operations within the ITS II information security controls. The BOP would like to point out that these areas of improvement and satisfactory operations were a direct result of proactive steps taken by the BOP prior to the OIG's investigation. As noted in the OIG's report, the "BOP is in the process of addressing findings identified in the June 2002 Security Test and Evaluation (ST&E)." The BOP was in the process of finalizing its report on system vulnerabilities and creating a corrective plan of action when the OIG began its audit in May 2002. These findings were provided to the OIG during their audit and were reflected throughout their report. The BOP

appreciates the OIG's additional recommendations and will incorporate them into the existing project plan. The BOP will continue to seek methods of improving its system security and strive to build and maintain an exceptional system security program for the ITS II system.

The BOP, recognizing the importance of maintaining a secure ITS system, hereby submits its responses for each recommendation identified in the OIG's report.

Recommendation #1 - We recommend that the BOP Director ensure that BOP management incorporates security requirements into the development and acquisition phases of the SDLC.

Response: The BOP agrees with this recommendation. The BOP will incorporate security requirements into the development and acquisition phases of the BOP system development life cycle (SDLC). Completion is anticipated by March 2003.

Recommendation #2 - We recommend that the BOP Director ensure that the BOP management incorporate formal procedures to document certification testing activities, update system documentation when security controls are added, retest security controls, and recertify the system after changes have been made.

Response: The BOP agrees with this recommendation. The BOP will incorporate formal procedures to document certification/testing activities, update system documentation when security controls are added, retest security controls, and have the system recertified after changes have been made. Completion is anticipated by March 2003.

Recommendation #3 - We recommend that the BOP Director ensure that the BOP management update operating controls as outlined in the June 2002 ST&E report, and complete the "Conditions of Certification" outlined in the ITS II certification statement.

Response: The BOP agrees with this recommendation. The BOP is in the process of incorporating the in-place operating controls as outlined in the June 2002 ST&E report and completing the "Conditions of Certification" outlined in the ITS II certification statement. Completion is anticipated by April 2003.

Recommendation #4 - We recommend that the BOP Director ensure that BOP management requires all users, including vendor and contractor personnel, to read and sign the Rules of Behavior

document (BOP Directive 1237-12) to ensure users are aware of its contents.

Response: The BOP agrees with this recommendation. The BOP will revise procedures to incorporate vendors and contractors. The BOP is currently in the process of rewriting the Rules of Behavior for the vendor. The BOP anticipates having an updated copy completed and signed by all vendor staff by December 2002.

Recommendation #5 - We recommend that the BOP Director ensure that the BOP management incorporate the guidelines for developing security plans outlined in the NIST SP 800-18 into the current ITS II security plan and incorporate the plan into the overall IRM strategic plan for the BOP.

Response: The BOP agrees with this recommendation. The BOP is currently rewriting the security plan using the NIST SP 800-18 as the guideline. Completion is anticipated by February 2003.

Recommendation #6 - We recommend that the BOP Director ensure that the BOP management:

a. Conduct an analysis on the current staff shortages by determining the current security and system administrator skills on the BOP team and determine what skills the BOP needs to close the "gap." If additional staff is required, hire additional personnel who are trained and experienced security and/or system administrators;

b. Ensure that those individuals who currently function as both security administrators and system administrators are moved to positions where these responsibilities do not conflict; and

c. Ensure that developers are not tasked with either system or security administration.

Response: The BOP agrees with this recommendation. The BOP will analyze current staff shortages by determining the current security and system administrator skills on the BOP team and determine what additional skills and positions are needed. Completion is anticipated by March 2003.

Recommendation #7 - Distribute the BOP's documented procedures on how to maintain BOP ITS II user accounts to ITS II security staff and contractor personnel.

a. Enforce procedures in accordance with the BOP Directive 1237.11 and Department policy.

Response: The BOP agrees with this recommendation. The BOP will distribute documented procedures on ITS II user accounts to ITS II security staff and contractor personnel. Additionally, the BOP will enforce the procedures as required by the BOP's Directive 1237.11. The BOP anticipates that all training will be completed by February 2003.

Recommendation #8 - We recommend that the BOP Director ensure that the BOP management implement all of the recommendations outlined in the June 2002 ST&E report, specifically those outlined in section 4.13.

Response: The BOP believes OIG intended to reference section 4.12, Physical Security instead of section 4.13, Computer Incident Response Capability. The BOP agrees with the recommendation with a reference to 4.12 Physical Security. The BOP will implement the recommendations outlined in section 4.12 of the June 2002 ST&E report. Completion is anticipated by February 2003.

Recommendation #9 - We recommend that the BOP Director ensure that BOP management document a process to control the transfer of media and BOP data. In addition, the BOP management should ensure the audit trails are kept and retained for extended periods of time, capturing relevant information such as name, date, media description, and authorization.

Response: The BOP agrees with this recommendation. The BOP will develop and document a formal procedure to control the transfer of BOP media and data. The BOP anticipates that the documentation will be completed by January 2003.

Recommendation #10 - We recommend that the BOP Director ensure the contingency plan is distributed to appropriate individuals, including contractor staff. The plan should be periodically tested and employees and contractor staff trained on their roles and responsibilities.

Response: The BOP agrees with the recommendation to distribute the contingency plan to the appropriate individuals. We are currently modifying the existing contingency plan and will distribute it to all required staff by January 2003. The BOP tested the contingency plan in January 2002 at our alternate COF and will continue to test the plan as necessary.

Recommendation #11 - We recommend that the BOP Director ensure that the BOP management develop a configuration standard for all systems that incorporate the most restrictive security settings possible. In addition, the BOP should implement all the recommendations outlined in the ST&E report.

Response: The BOP agrees with this recommendation. The BOP will develop a configuration standard for all systems that incorporates the most restrictive security settings possible. The BOP anticipates this process will be completed by March 2003.

Recommendation #12 - We recommend that the BOP Director ensure that the BOP management develop policies and procedures surrounding the use of intrusion detection software and integrity validation software and implement these policies and procedures on critical servers.

Response: The BOP agrees with this recommendation. The BOP will develop procedures surrounding the use of intrusion detection software and integrity validation software, and implement these policies and procedures at each of the vendor locations by February 2003.

Recommendation #13 - We recommend that the BOP Director ensure that the BOP management develop a policy for incident handling, response, and personnel support.

Response: The BOP agrees with this recommendation. The BOP will develop stronger incident handling, response, and personnel support procedures. Completion is anticipated by January 2003.

Recommendation #14 - We recommend that the BOP Director ensure that the BOP management enforce formal Department password policies and procedures and install and activate a password filter on all servers to enforce parameters that enforce restrictions on passwords.

Response: The BOP agrees with this recommendation. The BOP will enforce current Department password policies and procedures and install and activate a password filter on all servers to enforce parameters that enforce restrictions on passwords. Completion is anticipated by December 2002.

Recommendation #15 - We recommend that the BOP Director ensure that the BOP management develop, implement, and monitor documented policy establishing specific security standards and

settings for access controls. At a minimum, these standards and settings should:

a. Establish policy and procedures for disabling insecure protocols.

b. Establish policy dictating the reset of vendor default security parameters to more secure settings.

c. Configure network connections to automatically disconnect.

d. Establish standard firewall procedures for configuring the firewall.

e. Restrict access to tables defining network options, resources, and operator profiles.

Response: The BOP agrees with this recommendation. The BOP will develop, implement, and monitor documented procedures establishing specific security standards and settings for access controls. Completion is anticipated by February 2003. However, the BOP would like to request specific information about the findings to assist in the corrective action necessary to eliminate these issues.

Recommendation #16 - We recommend that the BOP Director ensure that the BOP management develop, implement, and monitor documented policy establishing specific security standards and settings for user authentication and access. At a minimum, these standards and settings should:

a. Prohibit the use of access scripts with embedded passwords.

b. Require data owners to review access authorizations to determine whether they remain appropriate.

Response: The BOP agrees with this recommendation. The BOP will develop, implement, and monitor documented procedures establishing specific security standards and settings for user authentication and access. Completion is anticipated by March 2003.

Recommendation #17 - We recommend that the BOP Director ensure that the BOP management implement the system key utility and restrict services so that they are running in a secured context. In addition, ensure the removal of all unnecessary services.

Response: The BOP agrees with this recommendation. The BOP will implement the system key utility, restrict services to run in a secured context, and remove all unnecessary services. Completion is anticipated by February 2003. However, the BOP would like to request specific information regarding the services OIG believes are "unnecessary" that were identified on the NT, UNIX, and Cisco platforms, in order to remove these services.

Recommendation #18 - We recommend that the BOP Director ensure that BOP management develop, implement, and monitor documented policy establishing specific security standards and settings for networking controls. At a minimum, these standards and settings should include:

a. The registry key on Windows NT servers, HKLM\Software\Microsoft\WindowsNT\CurrentVersion\ Winlogon CachedLogonsCount, should be set to 0.

b. The command on routers in global configuration mode: Passive-interface type number where "type" refers to the interface type and "number" is the interface number.

Response: The BOP agrees with this recommendation. The BOP will develop, implement, and monitor documented procedures establishing specific security standards and settings for network controls. Completion is anticipated by February 2003.

Recommendation #19 - We recommend that the BOP Director ensure that the BOP management develop, implement, and monitor documented policy establishing specific security standards and settings for user and group management controls. At a minimum, these standards and settings should include:

a. Review user account activity and disable or remove accounts that have been inactive for an extended period of time or are no longer needed.

b. Develop procedures for renaming the Administrator and Guest accounts and assigning strong passwords that are a minimum of eight characters and contain alphanumeric and special characters.

c. Remove domain users from the local administrator group.

d. Replace references to the special group 'Everyone' with 'Domain Users', 'Authenticated Users' or Domain application groups.

e. Create the /etc/ftpusers file.

Response: The BOP agrees with this recommendation. The BOP will develop, implement, and monitor documented procedures establishing specific security standards and settings for user and group management controls. Completion is anticipated by March 2003.

Recommendation #20 - We recommend that the BOP Director ensure that the BOP management develop, implement, and monitor documented policy establishing specific security standards and settings for account integrity management. At a minimum, these standards and settings should include:

a. "Log on locally,"

b. "Access this computer from the network,"

c. "Restore Files and Directories,"

d. "Shut down the system,"

e. "Take ownership of files or other objects,"

f. "Act as part of the operating system,"

g. "Log on as a service," and

h. "Increase Scheduling Priority."

Response: The BOP agrees with this recommendation. The BOP will develop, implement, and monitor documented procedures establishing specific security standards and settings for account integrity management. Completion is anticipated by March 2003.

Recommendation #21 - We recommend that the Director of the BOP ensure that the BOP management develop, implement, and monitor documented policy establishing specific security standards and settings for file system access. At a minimum, these standards and settings should:

a. Replace references to the special group 'Everyone' with 'Domain users', 'Authenticated Users', or Domain application groups.

b. Remove access to sensitive system utilities from accounts that do not require access.

c. Review and remove unnecessary permissions on files and directories.

d. Restrict access to the network file system shares.

Response: The BOP agrees with this recommendation. The BOP will develop, implement, and monitor documented procedures establishing specific security standards and settings for file system access. Completion is anticipated by February 2003.

Recommendation #22 - We recommend that the BOP Director ensure that BOP management develop, implement, and monitor documented policy establishing specific security standards and settings for maintenance controls. At a minimum, these standards and settings should:

a. Enable a password protected screen saver on the server.

b. Display a system-warning message when users log on the server.

Response: The BOP agrees with this recommendation. The BOP will develop, implement, and monitor documented procedures establishing specific security standards and settings for maintenance controls. Completion is anticipated by February 2003.

Recommendation #23 - We recommend that the BOP Director ensure that the BOP management develop, implement, and monitor documented policy establishing specific security standards and settings for NT registry settings. At a minimum, these standards and settings should include reconfiguring the registry settings to a more secure configuration.

Response: The BOP agrees with this recommendation. The BOP will develop, implement, and monitor documented procedures establishing specific security standards and settings for Windows NT registry settings. Completion is anticipated by January 2003.

Recommendation #24 - We recommend that the BOP Director ensure that the BOP management obtains the latest security patches from the operating system vendor. The patches should be properly installed and configured.

Response: The BOP agrees with this recommendation. The BOP will obtain the latest security patches from the operating system

vendors and test for compatibility with the system. Completion is anticipated by December 2003.

Recommendation #25 - We recommend that the Director of the BOP ensure that the BOP management develop, implement, and monitor documented policy establishing specific security standards and settings for router configuration. At a minimum, these standards and settings should:

a. Issue the "no ip source-route" command in interface configuration mode.

b. Issue the "no ip alias" command in configuration mode.

c. Issue the command: "ip tcp intercept list yyy," (where yyy is the access list number to which the connections will be intercepted), in configuration mode.

d. Enable encryption via the "crypto map" command.

Response: The BOP agrees with this recommendation. The BOP will develop, implement, and monitor documented procedures establishing specific security standards and settings for router configurations. Completion is anticipated by February 2003.

Recommendation #26 - We recommend that the BOP Director ensure that the BOP management implement Cisco's fail-over capabilities by configuring HSRP on critical external routers.

Response: The BOP does not agree with this recommendation. The ITS network currently has fail-over procedures in place and the BOP feels this change will not benefit the operation or security of the system.

Recommendation #27 - We recommend that the Director of the BOP ensure that the BOP management develop, implement, and monitor documented policy establishing specific security standards and settings for command line access. At a minimum, these standards and settings should include:

a. Enter the following command: privilege level command, in global configuration mode.

b. Create an appropriate access-list using the access-list command in configuration mode. Once the access list has been created, apply it to the appropriate terminal (typically vty 0 4) using the access-group <basic access list number> in command.

c. Enable SSH on the router.

d. Enable Authentication, Authorization, and Accounting.

e. Establish a session timeout.

Response: The BOP agrees with this recommendation. The BOP will develop, implement, and monitor documented procedures establishing specific security standards and settings for command line access. Completion is anticipated by January 2003.

Recommendation #28 - We recommend that the BOP Director ensure that the BOP management develop procedures for logging and monitoring system activity and require that audit logs be reviewed periodically.

Response: The BOP agrees with this recommendation. The BOP will develop documented procedures for logging and monitoring system activity and require that audit logs be reviewed periodically. The BOP anticipates completing this requirement by February 2003.

If you have any questions regarding this response, please contact Michael W. Garrett, Senior Deputy Assistant Director, Program Review Division, at (202) 616-2099.

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

Recommendation Number:

1. **Resolved.** In order to close this recommendation, the Bureau of Prisons (BOP) needs to incorporate security requirements into the development and acquisition phases of the SDLC.

2. **Resolved.** In order to close this recommendation, the BOP needs to incorporate procedures to document certification testing activities, update system documentation when security controls are added, retest security controls, and recertify the system after changes have been made.

3. **Resolved.** In order to close this recommendation, the BOP needs to update operating controls as outlined in the June 2002 Security Test and Evaluation (ST&E) report, and complete the "Conditions of Certification" outlined in the Inmate Telephone System II (ITS II) certification statement.

4. **Resolved.** In order to close this recommendation, the BOP needs to require all users, including vendor and contractor personnel, to read and sign the Rules of Behavior document (BOP Directive 1237-12) to ensure users are aware of its contents.

5. **Resolved.** In order to close this recommendation, the BOP needs to incorporate guidelines for developing security plans outlined in the National Institute of Standard Technology (NIST) Special Publication (SP) 800-18 into the current ITS II security plan and incorporate the plan into the overall IRM strategic plan for the BOP.

6. **Resolved.** In order to close this recommendation, the BOP needs to conduct an analysis on the current staff shortages by determining the current security and system administrator skills on the current BOP team and ensure that those individuals are moved to positions that do not conflict.

7. **Resolved.** In order to close this recommendation, the BOP needs to enforce procedures in accordance with the BOP Directive 1237.11 and Department policy for the distribution of the BOP's documented procedures on how to maintain ITS II user accounts to ITS II security staff and contractor personnel.

8. **Resolved.** In order to close this recommendation, the BOP needs to implement all of the recommendations outlined in the June 2002 ST&E report, specifically those outlined in section 4.12.

9. **Resolved.** In order to close this recommendation, the BOP needs to document a process to control the transfer of media and BOP data.

10. **Resolved.** In order to close this recommendation, the BOP needs to ensure the contingency plan is distributed to appropriate individuals, including contractor staff.

11. **Resolved.** In order to close this recommendation, the BOP needs to develop a configuration standard for all systems that incorporates the most restrictive security settings possible.

12. **Resolved.** In order to close this recommendation, the BOP needs to develop policies and procedures surrounding the use of intrusion detection software and integrity validation software.

13. **Resolved.** In order to close this recommendation, the BOP needs to develop a policy for incident handling, response, and personnel support.

14. **Resolved.** In order to close this recommendation, the BOP needs to enforce Department password policies and procedures and install and activate a password filter on all servers to enforce parameters that enforce restrictions on passwords.

15. **Resolved.** In order to close this recommendation, the BOP needs to develop and monitor documented procedures establishing specific security standards and settings for access controls.

16. **Resolved.** In order to close this recommendation, the BOP needs to develop and monitor documented procedures establishing specific security standards and settings for user authentication and access.

17. **Resolved.** In order to close this recommendation, the BOP needs to implement the system key utility and restrict services so that they are running in a secured context.

18. **Resolved.** In order to close this recommendation, the BOP needs to develop, implement, and monitor documented procedures establishing specific security standards and settings for network controls.

19. **Resolved.** In order to close this recommendation, the BOP needs to develop, implement, and monitor documented procedures establishing specific security standards and settings for user and group management controls.

20. **Resolved.** In order to close this recommendation, the BOP needs to develop, implement, and monitor documented procedures establishing specific security standards and settings for account integrity management.

21. **Resolved.** In order to close this recommendation, the BOP needs to develop, implement, and monitor documented procedures establishing specific security standards and settings for file system access.

22. **Resolved.** In order to close this recommendation, the BOP needs to develop, implement, and monitor documented procedures establishing specific security standards and settings for maintenance controls.

23. **Resolved.** In order to close this recommendation, the BOP needs to develop, implement, and monitor documented procedures establishing specific security standards and settings for Windows NT registry settings.

24. **Resolved.** In order to close this recommendation, the BOP needs to obtain the latest security patches from the operating system vendor.

25. **Resolved.** In order to close this recommendation, the BOP needs to develop, implement, and monitor documented procedures establishing specific security standards and settings for router configuration.

26. **Unresolved.** In order to resolve this recommendation, the BOP needs to comply with the recommendation to implement Cisco's fail-over capabilities by configuring hot standby router protocol (HSRP) on critical external routers. In addition, the BOP needs to provide the OIG with documentation reflecting the current fail-over capabilities for Cisco routers residing on the ITS II network.

27. **Resolved.** In order to close this recommendation, the BOP needs to develop, implement, and monitor documented procedures establishing specific security standards and settings for command line access.

28. **Resolved.** In order to close this recommendation, the BOP needs to develop procedures for logging and monitoring system activity and require that audit logs be reviewed.