SELECT APPLICATION CONTROLS REVIEW OF THE FEDERAL BUREAU OF PRISONS'S SENTRY DATABASE SYSTEM

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

Audit Report 03-25
July 2003

SELECT APPLICATION CONTROLS REVIEW OF THE FEDERAL BUREAU OF PRISONS'S SENTRY DATABASE SYSTEM

EXECUTIVE SUMMARY

SENTRY is the Federal Bureau of Prisons's (BOP) primary mission support database. The system collects, maintains, and tracks critical inmate information, including inmate location, medical history, behavior history, and release data. SENTRY processes over 1 million transactions each day and tracks more than 165,000 inmates. Roughly 85 percent of these inmates are housed within the BOP facilities, with the remaining inmates confined in other government facilities (state or local) or privately operated facilities through contracts with the BOP. As of March 2003, over 24,000 personal computers at approximately 200 facilities could access SENTRY.

The purpose of this audit was to assess the application controls for the BOP's SENTRY database to determine whether inmate data entered in SENTRY is valid, properly authorized, and completely and accurately processed.[1] Our criteria for conducting the review was the Federal Information System Controls Audit Manual (FISCAM).[2] We reviewed the accuracy and timeliness of SENTRY's input, processing, and output controls and judgmentally selected 3 of the BOP's 29 Community Corrections Offices (CCO) to conduct onsite reviews of their operational workflow (Annapolis Junction, Maryland; Philadelphia, Pennsylvania; and Chicago, Illinois). These sites were selected because they process large volumes of inmate data into SENTRY.

Our application review of SENTRY identified weaknesses in 4 of the 27 FISCAM control areas that we tested. We do not consider our findings in these areas to be major weaknesses and assessed SENTRY overall at a low risk to the protection of its data from unauthorized use, loss, or

[1] As part of our testing of the BOP's Annual Financial Statement for fiscal year 2002, we conducted a general control review of SENTRY's operating environment. General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. If general controls are weak, they diminish the reliability of controls associated with individual applications. Our general control review identified weaknesses in one of the six general control areas that we tested (the system development/change control process).

[2] FISCAM was developed by the General Accounting Office (GAO) and describes the computer-related controls that should be considered when assessing the integrity, confidentiality, and availability of computerized data. According to FISCAM, both general and application controls must be effective to help ensure the reliability, appropriate confidentiality, and availability of critical automated information. See Appendix III for a detailed description of the FISCAM application control areas tested.

modification.[3] Our findings were in the following four areas:

- Supervisory reviews (input process),
- Secured/restricted terminals (audit logs),
- Limited transactions access control, and
- Computer matching of transaction data.

Specifically, we identified data input errors resulting in incorrect inmate offense/charge codes, incorrect inmate's commitment date, incorrect date of offense, and offense fines not entered into SENTRY. We also found that the BOP did not adequately monitor audit log exception reports. Moreover, our review of SENTRY's access controls disclosed that the combination of authorization profiles and terminal access authority did not function as required because users with limited access profiles were able to process transactions above their level of access when logged onto terminals designated for users with higher authorization. We also tested completeness controls and found that the BOP's SENTRY General Use Manual failed to include a required step while updating inmate information.

We concluded that these weaknesses occurred because BOP management did not fully develop, document, or enforce the BOP policies in accordance with current Department of Justice (Department) policies and procedures. If not corrected, these security vulnerabilities could impair the BOP's ability to fully ensure the integrity, confidentiality, and availability of data contained in SENTRY.

This report contains recommendations for improving application controls for SENTRY in the Findings and Recommendations section. In general, we recommend that BOP management ensure that:

- The BOP's inmate data entry form is updated to reflect current BOP procedures and needs,
- The BOP's "SENTRY System Security Guide," requires routine generation and review of exception reports,

[3] The National Institute of Standards and Technology (NIST) defines risk as the possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity. Additionally, NIST categorizes the information into three basic protection requirements of high, medium, and low in accordance to the system's sensitivity level. Specifically, low risk would be detrimental if the information is compromised causing minor loss and needing only administrative action.

- Exception reports are provided timely to the Information Security Officer,

- SENTRY's workstation controls are properly configured to access only authorized areas of the system, and

- The BOP's SENTRY General Use Manual is updated to reflect proper procedures for entering initial records into SENTRY.

The details of our work are contained in the Findings and Recommendations section of the report. Our objectives, scope, and methodology appear in Appendix I.

TABLE OF CONTENTS

SELECT APPLICATION CONTROLS REVIEW OF THE FEDERAL BUREAU OF PRISONS'S SENTRY DATABASE SYSTEM

BACKGROUND

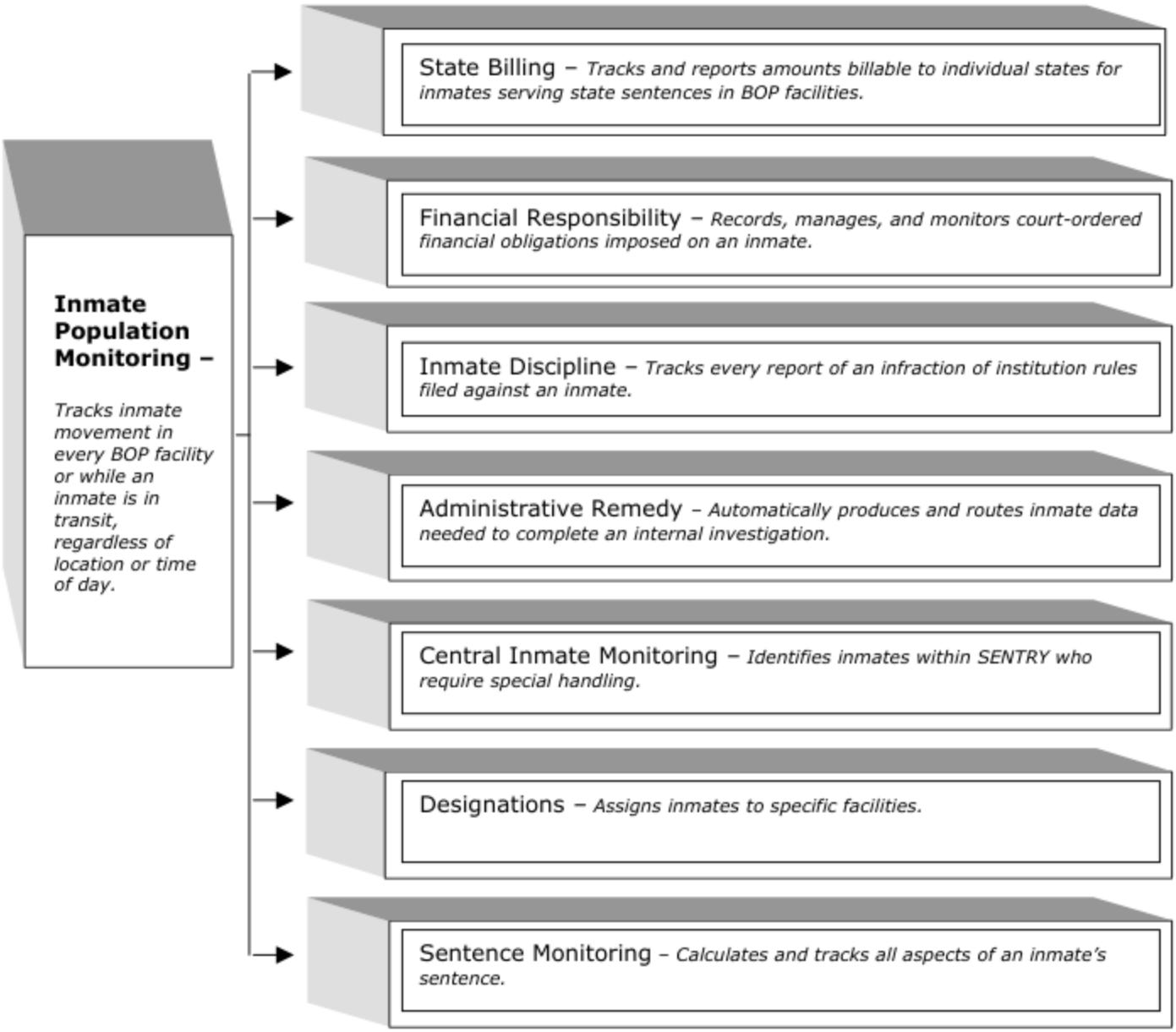
SENTRY, the Federal Bureau of Prisons's (BOP) primary mission support database, processes more than 1 million transactions each day and provides data files to a number of external organizations, including the United States Pardon Attorney, United States Marshals Service (USMS), Federal Bureau of Investigation, and United States Parole Commission. The BOP deployed its SENTRY database in 1978. It currently assists in monitoring and tracking approximately 165,000 federal inmates.

The system is designed to automate and assist in the monitoring of inmates consistent with implementation of the Violent Crime Control and Law Enforcement Act of 1994 (VCCLEA),[4] the Prisoner Litigation Reform Act (PLRA),[5] and other laws, which may require special treatment of inmates within the BOP prison institutions. All inmate information, which is critical to the safe and orderly operation of BOP facilities, is collected, maintained, and reported within SENTRY. This information includes inmate institution assignment, inmate population, and sentence data. A diagram detailing the various SENTRY modules and a short description of each module follow.

[4] The VCCLEA provided for new police offices, funding for prisons, and funding for prevention programs.

[5] In April 1996, the PLRA was enacted by Congress as part of the Balanced Budget Down Payment Act, which limits the prospective relief that can be provided for prison conditions as well as terminates the existing orders for prospective relief unless a court finds that prospective relief remains necessary to correct a current or ongoing violation of a federal right.

SENTRY DATABASE MODULES AND DESCRIPTIONS[6]



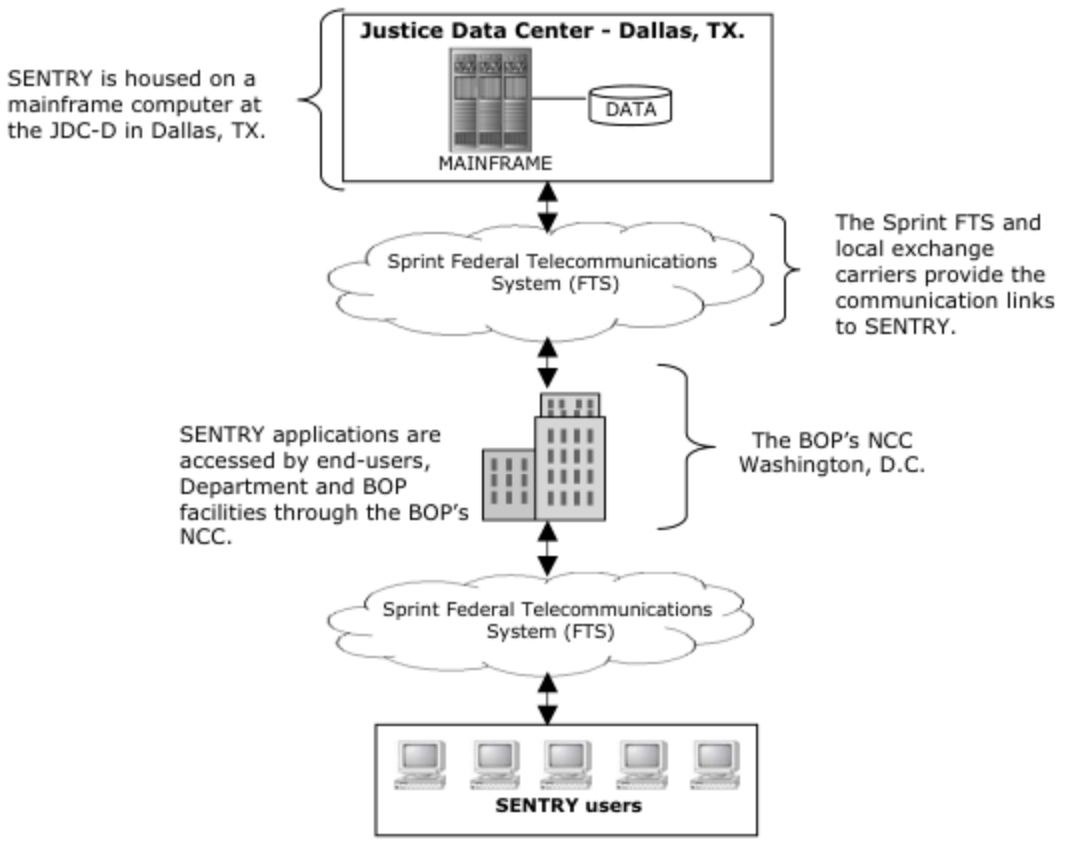
Source: The BOP's Information Technology Investment Report, March 1998.

[6] SENTRY also includes a Property Management Module that tracks BOP's accountable property and automatically computes the depreciation of capitalized property; however it is not directly applicable to the Inmate Population Monitoring Module.

SENTRY Database System Environment

SENTRY resides on a BOP mainframe[7] computer located at the Justice Data Center in Dallas, Texas (JDC-D) operated by the Department of Justice (Department) Justice Management Division's (JMD) Computer Services. Over 24,000 personal computers are in place - at approximately 200 facilities in the Department and BOP - to grant access to SENTRY by way of the BOP's Washington, D.C., Network Control Center (NCC).[8] These remote sites include federal correctional facilities, regional offices, Community Corrections Offices (CCO), and other selected offices. The following diagram depicts SENTRY's network configuration:

SENTRY Network Configuration



Source: The Office of the Inspector General's (OIG) analysis of the SENTRY Network Configuration.

[7] A mainframe is a large system capable of handling tens of thousands of online terminals. Large-scale mainframes support multiple gigabytes of main memory and terabytes of disk storage. Large mainframes use smaller computers as front-end processors that connect to communications networks.

[8] See Appendix IV for a listing of SENTRY's authorized users.

SENTRY utilizes a client/server application. This is a network architecture in which each computer or process on the network is either a client or a server. Servers are powerful computers or processes dedicated to managing disk drives, printers, or network traffic. Clients are personal computers (PCs) or workstations on which users run applications. Clients rely on servers for resources, such as files, devices, and even processing power. The client part of the program is referred to as the front-end processor and the server part is referred to as the back-end.

SENTRY is comprised of approximately 700 program routines written in COBOL,[9] which is used to process data to a database management system (DBMS). SENTRY allows concurrent sharing of data among multiple users. The DBMS maintains the indices that are necessary to translate application program data requirements into the information used by the mainframe's operating system to read or write data to SENTRY. The DBMS application used for SENTRY is the Computer Associate's (CA) Integrated Data Management System (IDMS). The IDMS's function is to process transmitted data between SENTRY and the mainframe operating system. The IDMS writes and retrieves data to and from the physical storage area of the mainframe when SENTRY is accessed.

SENTRY communications are relayed by way of the BOP's Wide Area Network (WAN) circuits. The SENTRY mainframe is accessed by way of Systems Network Architecture (SNA) gateways,[10] which ensure that all SENTRY circuits include end-to-end encryption. Each BOP facility connects directly to the BOP's NCC via the Sprint Federal Telecommunications System (FTS) network. The Sprint FTS and the local exchange carriers provide the communication links for SENTRY. However, the BOP migrated its data communications to the Justice Consolidated Network (JCN),[11] which also is implemented primarily through the Sprint FTS contract. The FTS currently provides intercity telecommunications services for federal government agencies.

---

[9] COBOL (Common Business Oriented Language) is a popular high-level programming language used for business applications that runs on large computers.

[10] SNAs are IBM's mainframe network standards consisting of a centralized architecture with a host computer controlling many terminals. Enhancements have adapted SNA to today's peer-to-peer communications and distributed computing environment. Gateways perform protocol conversion between different types of networks or applications to facilitate communication between different systems.

[11] The OIG previously audited JCN (see OIG Audit Report Number 03-13, "Independent Evaluation Pursuant to the Government Information Security Reform Act," fiscal year 2002, the Justice Consolidated Network, February 2002).

FINDINGS AND RECOMMENDATIONS

Our application review of SENTRY identified weaknesses in 4 of the 27 FISCAM control areas that we tested.[12] In our judgment, these are not major weaknesses in SENTRY. We consider the system overall to be at a low risk to the protection of its data from unauthorized use, loss, or modification. Specifically, we found weaknesses in the areas of supervisory reviews (input process), secured/restricted terminals (audit logs), limited transactions for access controls, and computer matching of transaction data. We concluded that these weaknesses occurred because BOP management did not fully develop, document, or enforce the BOP policies in accordance with current Department policies and procedures. If not corrected, these weaknesses could impair the BOP's ability to fully ensure the integrity, confidentiality, and availability of data contained in SENTRY.

I. Authorization Controls (Input)

Authorization controls involve the process of granting or denying access to a network resource, converting the data to an automated form, and entering the data into the application in an accurate, complete, and timely manner. Testing of authorization controls includes examining the data input process and determining if controls exist for ensuring:

- Data are authorized prior to being entered;
- Access restrictions exist to prevent unauthorized personnel from obtaining blank source documents to record unauthorized information and insert the document into production with authorized documents;
- Supervisory or independent reviews of the source document occurs before its data is entered into the automated system;
- Data entry terminals are only accessible to authorized users for authorized purposes;

[12] Although we performed a full application review of SENTRY, this audit report does not include an evaluation of SENTRY's general controls. As part of the OIG's Federal Bureau of Prisons Annual Financial Statement for fiscal year 2002, we evaluated the general controls over select SENTRY systems. In that report, weaknesses were identified in the area of application software development/change control, which represents one of General Accounting Office's (GAO) six FISCAM general controls.

- Users are limited to what transactions they can enter;
- Master files are configured to assist with identifying unauthorized transactions;
- Exception reports are generated and reviewed before transactions are posted; and
- Duties are appropriately segregated among staff.

Our audit of the BOP's authorization controls for SENTRY found that authorization controls were in place within the areas of controlled and authorized source documents;[13] unauthorized transactions; and reported exceptions. However, we identified weaknesses with respect to SENTRY's input process, review of audit logs, and access controls.

Supervisory Reviews (Input Process)

During the input process, a supervisory (or independent) review of the data should occur before it is entered into the automated system. This control is used to ensure that unauthorized transactions are not being entered and that exceptions are reviewed and corrected before transactions are posted. Since SENTRY is used for collecting, maintaining, and reporting inmate information vital to the operation of the BOP facilities, it is critically important to maintain the integrity and quality of the data that lies within it. The BOP's Information Technology Investment Report (Section 2.2), dated March 1998, requires accurate entry of data to help provide assurance that data integrity is being maintained.

We performed survey work of the BOP's mandatory procedures for SENTRY's input process at one field office (Chicago, Illinois), and we performed detailed testing at two regional offices (Philadelphia, Pennsylvania; and Annapolis Junction, Maryland). To review for authorization and correct entry into SENTRY, we selected a total of 48 inmate files from the Philadelphia and Annapolis Junction offices. From each case file, we examined the mandatory source documents (the Court's Judgment and Commitment Order (J&C), the USMS Judgment and Individual Custody and Detention Report,[14] and the United States Probation Office's pre-sentence investigation report) and compared them to the information

[13] Controlled and authorized source document controls are implemented to ensure that access to blank documents is restricted to authorized personnel.

[14] This form is referred to as Form USM-129.

entered into SENTRY. These three source documents are received by the CCO and are used to complete the initial processing of an inmate assignment.[15]

We selected a total of 23 case files for review at the BOP's Philadelphia CCO. Two of the 23 case files identified data entry errors. One case file contained an incorrect "offense/charge code" ("391") for "attempt and conspiracy" versus a correct code ("381") for "create, manufacture, distribute or dispense controlled narcotic drug." The second case file revealed an incorrect inmate's commitment date. A source document (J&C) showed a commitment date of "09/19/02," yet the date entered in SENTRY's database was "09/18/02."

At the BOP's Annapolis Junction CCO, we reviewed 25 case files. We identified data entry errors for three case files. At this office, we again found an inmate "description of offense" code incorrectly entered. In this case, an incorrect offense code of "381" was entered instead of the code "382" "marijuana charge" as indicated on the source document (PSI report). Additionally, we found a different inmate's record was entered in SENTRY with an incorrect "date of offense." The source document (J&C) contained only the month and year. However, the date entered into SENTRY was "12-31-1999." Lastly, some information contained in an inmate's case file was not entered into SENTRY. The source document (J&C) indicated that the inmate paid offense fines of $500 and assessments fines of $50. However, this information was not entered in the "Felony Assessment & Fines" data fields in SENTRY.

The errors identified above were disclosed to the BOP and corrected in the presence of our auditors. While the input errors we identified were relatively minor, they represent a weakness in internal controls because the severity of an input error could result in a more serious outcome. For example, the repercussions of an incorrect offense/charge code could result in transporting an inmate to an inappropriate facility.

In our judgment, these errors occurred because: 1) the BOP does not enforce the use of the BOP's form BP-337 as a primary document for inputting data into SENTRY, and 2) the BOP's primary form BP-337 does not identify which source documents are to be used to complete mandatory information into SENTRY. Additionally, the multiple source documents used to complete the BP-337 sometimes contain conflicting information or lack mandatory information. Since the BOP Community Corrections Management

[15] The BOP transfers information obtained from the courts, the USMS, or other law enforcement documents to a single document (the Male/Female Inmate Load and Designations Form BP-337). The BOP uses the BP-337 as the source document for entering consolidated data into SENTRY.

Operational Procedures, Policy Standards (PS) 5100.07, does not require the BP-337 to be completed for all data input into SENTRY from a single source document (or state which source document should be used to complete the various sections of the BP-337), this causes confusion as to which source document to use to obtain the mandatory information.

Recommendations:

We recommend the BOP Director ensure that BOP management:

1. Enforce the BOP (PS) 5100.07, which states that all CCOs are to use the BP-337 for inputting initial inmate data as the sole source document.

2. Redesign the BP-337 so that mandatory information needed for tracking BOP inmates can be documented.

3. Modify the BP-337 to indicate which source document should be used to complete each field within this form.

Secured/Restricted Terminals (Audit Logs)

Audit logs (commonly known as audit trails) maintain a record of activity by system or application processes. Audit logs provide a means to help establish several security–related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification.

Automated controls, such as an audit log that produces exception reports, help to ensure data integrity and can alert management to possible misuses of the system. We found that the BOP end-users and management depend on manual verification of transactions by performing cross-edit checks of source documents to verify data integrity and completeness of transactions entered into SENTRY.

Currently, the BOP tracks all of SENTRY's input and output activities through an automated audit log, which contains system data such as the identity of the person and device having access to the database, the date and time of user logon/logoff activities, and data processed. At present, the BOP uses these audit logs for the sole purpose of monitoring SENTRY's operational performance.

Although the SENTRY audit logs used to monitor system performance are capable of generating ad hoc exception reports, the BOP does not

routinely produce these reports from the logs. Additionally, we found that the BOP's "SENTRY System Security Guide," dated June 23, 2000, does not require a periodic review of exception logs. Without requiring a periodic review of audit logs, unauthorized activities can go unnoticed, uninvestigated, or unresolved.

Department of Justice Order 2640.2D, Chapter 2, "Security Requirements" (Accountability and Audit Trails), requires that audit logs be maintained and reviewed for activities that could modify, bypass, or negate the system's security safeguards.

In our judgment, these weaknesses exist because the BOP failed to implement a process for routinely identifying exceptions using audit logs.

Recommendations:

We recommend the BOP Director ensure that BOP management:

4. Update the BOP's "SENTRY System Security Guide," dated June 23, 2000, to require the routine generation and review of exception reports; and

5. Provide the Information Security Officer with the exception reports generated from the audit logs in the time period specified by the BOP's "SENTRY System Security Guide."

Limited Transactions (Access Controls)

Limited transaction controls restrict the access of legitimate users to the specific systems, programs, and files needed to complete work assignments and to prevent unauthorized users from gaining access to computing resources. Limiting transactions include utilizing system access controls and ensuring assigned personnel duties are properly segregated.

Access controls are designed to limit or detect access to computer programs, data, and equipment to protect these resources from unauthorized modification, disclosure, loss, or impairment. They also serve as a key control for ensuring that staff duties and responsibilities are implemented in a way that safeguards programs. Logical access controls involve the use of computer hardware and security software programs to prevent or detect unauthorized access by requiring users to input unique user identifications, passwords, or other identifiers that are linked to predetermined access privileges. Additionally, controls are designed to reduce the risk of errors or fraud from occurring and going undetected.

Policies outlining the supervision and assignment of responsibilities to groups and related individuals should be documented, communicated, and enforced. Such controls keep individuals from subverting a critical process.

The BOP's "SENTRY System Security Plan," dated February 25, 2000, requires restricting access to SENTRY through the use of software and hardware profiles. The BOP access controls are intended to implement two lines of defense — one at the application level, the other at the workstation level. The use of a user identification/password requires validation and authentication at the application level. At the workstation level, workstations are configured to identify their location and authorization functional capabilities to SENTRY's system platform. Additionally, each workstation is required to be configured in a manner that limits access to SENTRY according to users' identification and profiles. These limitations are required to restrict access to menus, fields, and records within SENTRY. According to the BOP's Information Technology Investment Report, dated March 31, 1998, some transactions also require SENTRY users to utilize special access codes in addition to their user identification/password.

Our review of SENTRY's access controls disclosed that the combination of authorization profiles and terminal access authority did not function as required. Users with limited access profiles were able to process transactions above their level of access when logged onto terminals designated for users with higher authorization. This control weakness was identified when a user was requested to demonstrate the BOP's access controls in place. The user logged onto his assigned workstation and was unable to access inmates' restricted medical records. However, when the same user logged onto a different workstation assigned to another user with higher authorization, the user was granted access to sensitive medical records without proper authorization.

Additionally, our audit disclosed that the BOP does not have documentation defining who should have access to sensitive medical records. At the time of our audit, we found that a Community Corrections Trainee was permitted to view an inmate's sensitive medical history records within SENTRY. Duties that are not appropriately segregated significantly increase the risk of releasing private information.

For SENTRY workstations that are configured to operate at a high level of security, access controls should be in place to prevent users with lower levels of authorization from accessing restricted data. The failure to ensure that access controls are properly implemented could cause critical mistakes such as modifications of inmates' medical records, transfer records, or release dates.

Department of Justice Order 2640.2D requires access controls to ensure system users can only access the resources necessary to accomplish their duties and no more. Additionally, OMB Circular A-130 requires agencies to implement the practice of "least privilege," whereby user access to systems is restricted to the minimum level possible.

Recommendation:

We recommend the BOP Director ensure that BOP management:

6. Enforce the BOP's existing access control policy by properly configuring SENTRY's workstation controls to ensure that users with system authorization are restricted to areas of the system that they have been authorized to access, and no more.

II. Completeness Controls (Processing)

Completeness controls are designed to ensure that all authorized transactions are processed and completed prior to being entered into the computer. These controls include the use of record counts and control totals, computer sequence checking, computer matching of transaction data with data in a master or suspense file, and checking of reports for transaction data.

Our audit of the BOP's completeness controls for SENTRY found controls were in place for record counts and control totals, computer sequence checking, checking reports for transaction data, completeness of data processed in the processing cycle, and completeness of data processed for the total cycle. However, we identified weaknesses with respect to SENTRY's computer matching of transaction data.

Computer Matching of Transaction Data

The BOP's Community Corrections Management Operational Procedures, Policy Standards 1237.12 requires all systems, whether automated or manual, to quickly, accurately, and reliably provide information. Additionally, it requires that only authorized and accurate information be entered into databases. When incorrect transactions are processed, controls should be in place to ensure that these items are investigated and resolved in a timely manner.

We tested the BOP's completeness controls for SENTRY and found that the BOP's SENTRY "General Use Manual" (GUM) did not reflect current system settings. The manual provides instructions for inputting initial inmate records into SENTRY. However, when we attempted to simulate the addition of a new inmate into SENTRY (by following instructions indicated in the GUM) we noted that the manual failed to include the required step of updating an inmate identification number screen prior to initiating the addition of an inmate.

Recommendation:

We recommend the BOP Director ensure that BOP management:

7. Update SENTRY's General Use Manual to reflect proper procedures for entering initial inmate records into SENTRY.

III. Accuracy Controls (Output)

Accuracy controls are implemented to ensure that data recording is valid and accurate in order to produce reliable results. The implementation of these controls includes procedures that are well designed for data entry, easy to follow data entry screens, limit and reasonableness checks, and validation of override actions for appropriateness and correctness. Without accuracy controls, invalid data may enter the system and produce unreliable results.

Our testing of the BOP's SENTRY accuracy controls confirmed that controls were in place for source documents, preformatted screens, key verification, automated entry devices, programmed validation, tests of critical calculations, restricting overriding data validation, controlled rejected transactions, reported of erroneous data, control output, and review of processing reports.

IV. Controls Over Integrity of Processing and Data Files

Controls over integrity of processing and data files are used to ensure that the current version of production programs and data files is used during system processing. The implementation of these controls includes: (1) executing program routines that can verify the proper version of computer files, (2) protecting against concurrent file updates, and (3) checking for internal file header labels to prevent the system end-user from bypassing system controls.

The NIST Federal Information Processing Standards Publication 73, Section 3.1.3, states that checking of input data during processing and validation of data that is generated by the application system are essential for assuring data integrity. Errors should be detected and corrected as soon as possible in order to prevent the propagation of invalid data throughout the system and the potential contamination of the system database.

We confirmed that controls were in place for SENTRY to check for the appropriate program. BOP end-users are only permitted access to the production environment and are locked into the production software version of SENTRY. Further, we found that record locks were in place within the database disallowing two end-users from updating the same record simultaneously. Finally, we found that SENTRY is not updated through batch processing, therefore, a test to determine whether SENTRY programs can or cannot bypass file header labels did not apply.

CONCLUSION

Our application review of SENTRY identified weaknesses in 4 of the 27 FISCAM control areas that we tested. We do not consider our findings in these areas to be major weaknesses, and we assessed SENTRY overall at a low risk to the protection of its data from unauthorized use, loss, or modification.[16] Application control weaknesses were identified in the areas of supervisory reviews, audit logs, access controls, and computer matching of transaction data. Specifically, we identified weaknesses in the inputting of incorrect offense/charge codes, incorrect inmate's commitment date, incorrect date of offense, and offense fines not entered into SENTRY. These input errors represent a weakness in internal controls that should be corrected. We also found that the BOP failed to monitor audit log exception reports. Without requiring a periodic review of audit logs, unauthorized activities could go unnoticed, uninvestigated, or unresolved. Moreover, our review of SENTRY's access controls disclosed that the combination of authorization profiles and terminal access authority did not function as required. Users with limited access profiles were able to process transactions above their level of access when logged onto terminals designated for users with higher authorization. We also tested the completeness of controls for SENTRY and found that the BOP's SENTRY GUM failed to include a required step while updating inmate information.

[16] Although we performed a full application review of SENTRY, this audit report does not include an evaluation of SENTRY's general controls. As part of the OIG's Federal Bureau of Prisons Annual Financial Statement for fiscal year 2002, we evaluated the general controls over select SENTRY systems. In that report, weaknesses were identified in the area of application software development/change control, which represents one of the six FISCAM general control areas.

We concluded that these weaknesses occurred because BOP management did not fully develop, document, or enforce the BOP policies in accordance with current Department policies and procedures. If not corrected, these weaknesses could impair the BOP's ability to ensure the integrity, confidentiality, and availability of data contained in SENTRY.

OTHER REPORTABLE MATTER

OMB Circular A-130, Appendix III, Section A 3.b.2 (d), requires that a contingency plan be established and periodically tested to perform the agency function supported by the application in the event of failure of its automated support.

GAO's FISCAM recommends the frequency of contingency plan testing should vary depending on the criticality of the entity's operations. Additionally, FISCAM states that generally, contingency plans should be fully tested about once every year or two, whenever significant changes to the plan have been made, or when significant turnover of key personnel has occurred. Industry best practices are more stringent and indicate that a new or revised contingency plan should be fully tested and implemented within 90 days of development.[17]

Although testing of contingency planning was not part of the FISCAM's application control testing that we performed,[18] we noted during our review that SENTRY's contingency plan was last updated in September of 2002 but was not tested. Prior to the issuance of this report, we confirmed with the BOP that testing of the BOP's SENTRY contingency plan was performed on March 27, 2003, and the plan was in the review process. We suggest that BOP continue to test its contingency plan and update the plan as circumstances warrant.

We also contacted the JMD regarding this matter. JMD informed us that the Department's standards (Department of Justice Order 2640.2D) are currently being modified to reflect the industry best practice of the 90-day requirement for testing contingency plans. We agree with JMD in implementing this more stringent requirement.

[17] Department of Justice Order 2640.2D, Chapter 1, "Security Program Management," Section 9(c) requires that contingency plans be tested annually or as soon as possible after a significant change to the environment that would alter the in-place assessed risk.

[18] Contingency planning is a FISCAM general control.

OBJECTIVES, SCOPE, AND METHODOLOGY

Our audit objectives were to review the application controls for the BOP's SENTRY database and determine whether inmate data entered in SENTRY are valid, properly authorized, and completely and accurately processed.[19] In order to meet these objectives, we tested SENTRY application controls using the GAO's FISCAM, which divides the testing of application controls into four major areas: authorization controls (input), completeness controls (processing), accuracy controls (output), and controls over integrity of processing and data files.

For testing of SENTRY's application controls, we judgmentally selected 3 of the 29 CCOs to conduct onsite reviews of their operational workflow — Annapolis Junction, Maryland; Philadelphia, Pennsylvania; and Chicago, Illinois. These CCOs were judgmentally selected because they process large volumes of inmate data into SENTRY.

Furthermore, we performed reviews of source documents at the three CCO offices to test input, process, output, and data integrity controls. In addition to the testing performed at the selected CCOs, we interviewed approximately 40 BOP officials. These interviews included the BOP managers and officials from the Computer Services Administration, Mainframe Systems Support, Systems Development Branch, Policy and Information Resource Management, Office of Information Systems, and Community Corrections. Additionally, we reviewed application, operation, and end-user manuals; the BOP's and Department information technology management policy and procedures; the BOP's project management guidance; the BOP's organizational structures and federal court cases; and prior GAO and OIG reports specific to SENTRY.

Findings identified at the time of fieldwork were communicated to the BOP to initiate corrective action. All audit work was performed in accordance with Government Auditing Standards and were based on the GAO's FISCAM, the BOP's Standard Operating Procedures, and federal laws and regulations governing inmate processing within the BOP facilities.

[19] Although we performed an application controls review of SENTRY, this audit report does not include an evaluation of SENTRY's general controls. As part of our testing of the BOP's Annual Financial Statement for fiscal year 2002, we conducted a general control review of SENTRY's operating environment. That general control review identified weaknesses in the area of system development/change control, which represents one of the six FISCAM general control areas.

FEDERAL INFORMATION SYSTEM CONTROL AUDIT MANUAL
APPLICATION CONTROL AREAS

Authorization Controls (Input)	VULNERABILITIES
Data are authorized	
1. Controlled and authorized source documents	
2. Supervisory reviews (Input process)	√
Restricted terminals	
3. Secured/restricted terminals (Audit logs)	√
4a. Limited transactions (Access controls)	√
4b. Limited transactions (Segregation of duties)	
Master files/Exception Reporting	
5. Unauthorized transactions	
6. Reported exceptions	
Completeness Controls (Processing)	
Computer processed transactions	
7. Record counts and control totals	
8. Computer sequence checking	
9. Computer matching of transaction data	√
10. Checking reports for transaction data	
Reconciliations	
11. Completeness of data processed in the processing cycle.	
12. Completeness of data processed for the total cycle.	
Accuracy Controls (Output)	
Data entry design	
13. Source documents	
14. Preformatted screens	
15. Key verification	
16. Automated entry devices	
Data validation	
17. Programmed validation	
18. Tests of critical calculations	
19. Restricted overriding data validation	
Erroneous data	
20. Controlled rejected transactions	
21. Reported erroneous data	
Output reports	
22. Control output	
23. Review of processing reports	
Controls over Integrity of Processing and Data Files	
24. Current versions of production programs and data files	
25. Routine to verify proper version	
26. Routine for checking internal file header labels	
27. Protection against concurrent file updates	

APPLICATION CONTROLS REVIEW GUIDELINES

GENERAL ACCOUNTING OFFICE
FEDERAL INFORMATION SYSTEM CONTROL AUDIT MANUAL

The application control guidelines used for this audit were obtained from the GAO's FISCAM. The information below details the sections from the FISCAM used during our review of SENTRY.

OVERVIEW

Application controls are the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, payroll, grants, or loans. An application system is typically a collection or group of individual computer programs that relate to a common function. In the federal government, some applications may be complex comprehensive systems, involving numerous computer programs and organizational units, such as those associated with benefit payment systems. For the purposes of this document, application controls encompass both the routines contained within the computer program code, and the policies and procedures associated with user activities, such as manual measures performed by the user to determine that data were processed accurately by the computer.

Application controls help make certain that transactions are valid, properly authorized, and completely and accurately processed by the computer. They are commonly categorized into three phases of a processing cycle:

- Input - data are authorized, converted to an automated form, and entered into the application in an accurate, complete, and timely manner;

- Processing - data are properly processed by the computer and files are updated correctly; and

- Output - files and reports generated by the application actually occur and accurately reflect the results of processing, and reports are controlled and distributed to the authorized users.

Some guides provide additional categories of application controls. For example, data origination is a breakout of input it controls to focus on source documents and their need for authorization and proper preparation and control. Also, data storage and retrieval focuses on access to and use of data files and protecting their integrity.

Instead of using the phases of a processing cycle, this document uses control categories that better tie in with the Specific Control Evaluation Worksheets (SCE) found in the FISCAM. The SCE is used to document the controls evaluation and is prepared for each significant accounting application. Included on the SCE are columns for recording the control objectives and control techniques being evaluated and accuracy including whether the assertion and related transactions are authorized, complete, valid, and accurate. The control objectives and techniques addressed in this chapter are consistent with other guidance, but our categorization, tying to the SCE, are the following:

- Authorization controls - aligns with the financial statement accounting assertion of existence or occurrence. This assertion, in part, concerns the validity of transactions and that they represent economic events that actually occurred during a given period.

- Completeness controls - relates to the financial statement accounting assertion on completeness, which deals with whether all valid transactions are recorded and properly classified.

- Accuracy controls - relates with the financial statement assertion on valuation or allocation. This assertion deals with whether transactions are recorded at correct amounts. The control category, however, is not limited to financial information, but also addresses the accuracy of other data elements.

- Controls over integrity of processing and data files - if deficient, could nullify each of the above control types and allow the occurrence of unauthorized transactions, as well as contribute to incomplete and inaccurate data.

AUTHORIZATION CONTROLS

Only authorized transactions should be entered into the application system and processed by the computer. Assessing authorization controls involves evaluating the entity's success in performing each of the following critical elements:

Critical Elements:

- All data are authorized before entering the application system.
- Restrict data entry terminals to authorized users for authorized purposes.
- Master files and exception reporting help ensure all data processed are authorized.

Data should be authorized before it is entered into the application system. Federal financial management systems are often characterized as large complex 'legacy' systems and often involve a multitude of documents that flow through various work steps. Paper source documents still play a significant role for originating data that enter application systems in the federal government. These source documents should fall under control measures so that unauthorized transactions are not submitted to and processed by the application. Also, data whether from a source document or not should undergo an independent or supervisory review prior to entering the application.

Source documents are controlled and require authorizing signatures.

Control over source documents should begin even before data is recorded on the document. Access restrictions over blank source documents should prevent unauthorized personnel from obtaining a blank source document, recording unauthorized information, and inserting the document in the flow with authorized documents and possibly causing a fraudulent or malicious transaction to occur. Use of pre-numbered source documents could help identify unauthorized documents that fall outside the range of authorized numbers for documents being prepared for data entry.

Key source documents for an application should require an authorizing signature, and the document should provide space for the signature by an authorized official.

For batch application systems - i.e., source documents are processed in batches - the source documents should be collected together and a batch control sheet should be prepared for individual batches. The control sheet should have space for recording the date, a batch control number, the number of documents in the batch, a control total for a key field in the documents, and the identification of the user submitting the batch. Establishing control over batches helps detect unauthorized modifications to

a document and prevents unauthorized documents from being entered into the application system. The document counts and control totals also help to determine whether all transactions are completely entered and processed by the computer. The following sections are also important to ensuring all transactions are authorized, particularly when the application system is designed such that transactions are entered individually instead of in batches.

Supervisory or independent reviews of data occur before entering the application system.

Providing supervisory or independent review of data before entering the application system helps prevent the occurrence of unauthorized transactions. A data control unit is effective for this purpose and this function has evolved as technology has advanced. With earlier systems, source documents were batched in the user department and sent to a data control unit that was organizationally under the information systems department. This unit monitored data entry and processing of the documents, seeing that all batches were received, entered, and processed completely. In addition, personnel in this unit verified that each source document was properly prepared and authorized before the data on the document was entered into the system.

This function has migrated to the user department as it gained access to application systems through computer terminals. Several or more personnel in the user department may now enter source documents into a transaction file that is not released for processing until a supervisory or independent review occurs. A user department control unit may have the responsibility to see that entered transactions are supported by a source document that contains a valid authorizing signature. Also, supervisors in the user department may hold this responsibility. These application systems may have a separate authorization screen accessed by computer terminal by control unit or supervisory personnel. After verifying the input transactions, the control unit or supervisory personnel enter the required authorization and release the data for further processing.

Unauthorized personnel who have unrestricted access to data entry terminals (as well as by authorized users who are not restricted in what transactions they can enter) can compromise the integrity of application data. Without limits, unauthorized personnel and authorized users could enter fraudulent or malicious transactions. To counter this risk, both physical and logical controls are needed to restrict data entry terminals to authorized users for authorized purposes. This section provides an overview

of controls relevant to restricting data entry terminals and limiting users in what transactions they can enter. Any work done in this section should be done in conjunction with the other two sections.

Data entry terminals are secured and restricted to authorized users.

Data entry terminals should be located in physically secure rooms. When terminals are not in use, these rooms should be locked, or the terminals themselves should be capable of being secured to prevent unauthorized use. Supervisors should sign on to each terminal device, or authorize terminal usage from a program file server, before an operator can sign on to begin work for the day. Each operator should be required to use a unique password and identification code before being granted access to the system.

Data entry terminals should be connected to the system only during specified periods of the day, which corresponds with the business hours of the data entry personnel. Each terminal should automatically disconnect from the system when not used after a specified period of time.

Where dial-up access is used to connect terminals to the system, connection should not be completed until the system calls back to the terminal. These terminals should generate a unique identifier code for computer verification. Such procedures help limit access to known, authorized terminals.

On-line access logs should be maintained by the system, such as through the use of security software, and should be reviewed regularly for unauthorized access attempts. All transactions should be logged as they are entered, along with the terminal ID that was used, and the ID of the person entering the data. This builds an audit trail and helps hold personnel accountable for the data they enter.

Users are limited in what transactions they can enter.

It is not enough to restrict access to data entry terminals to authorized users, as these users may still enter unauthorized transactions, if they are not limited on what transactions they can enter. Limits can be accomplished through authorization profiles. One authorization profile level can be placed over the terminal so that only specified transactions can be entered from a given terminal. For example, a terminal in a payroll office may be granted authorization so that payroll information, such as employee time and attendance and pay withholdings, could be entered from that terminal.

However, to effect a separation of duties, this terminal could be denied authorization to enter personnel actions, such as hirings that would create a new employee pay record, or promotions. These latter transactions are normally restricted to a personnel or human resources office.

Authorization profiles can also be established for user personnel. These personnel can be denied authorization for initiating transactions that would add or change a record on the authorized vendor master file. If one employee had the capability to initiate both types of transactions, the employee could potentially cause a fraudulent transaction by creating a vendor master record and initiating a payment that would be sent to the specified address or bank account controlled by the employee.

Before the auditor can rely on authorization profiles to reduce the audit risk, the auditor must determine the adequacy of the general controls over the profiles. That is, if the general controls are not effective in preventing unauthorized changes to the data matrix or table that constitutes the profile, the auditor should not rely upon this control.

An effectively controlled application system will also have authorization type controls to monitor data as it is processed. Two such controls include the use of master files and exception reporting that help determine the validity of transactions. These controls require computer programs to perform the validity checks and involve a process commonly referred to as data validation and editing. Many of the programmed checks in this process also concern the validity and accuracy of data fields in a transaction record, including whether a data field has a valid code, such as a pay withholding code used in a payroll application system. This section focuses on checks to determine the validity of a transaction. Data validation and editing is a more detailed discussion of data validation and editing, focusing on checks to determine the validity and accuracy of data fields.

Master files help identify unauthorized transactions.

A master file is a computer file that contains account and/or reference information that are integral to application systems, such as a payroll master file containing authorized employees and pay data. Master files and their approved records can help identify unauthorized transactions. For example, an accounts payable system should have a master file of approved vendors. As payment transactions are processed, they would be compared with this file and any payment for a vendor not on the file would be rejected and investigated by supervisor personnel, or by personnel specifically assigned this responsibility that do not also have responsibility for initiating vendor

payments. Using this process, there is greater assurance that all transactions not rejected are authorized and valid payments.

Exceptions are reported to management for their review and approval.

An exception report lists items requiring review and approval. These items may be valid, but exceed parameters established by management. Implementation of this control may vary, such that one system may print checks and have them routed to management to be released after their approval, and another system may hold the transaction in a suspense account until management enters an authorizing indicator, thus triggering the disbursement.

Before the auditor can rely on these controls to reduce the audit risk, the auditor must, as in the previous section, determine the adequacy of the general controls over these controls. That is, these controls would be rendered ineffective if the general controls would not prevent unauthorized changes to the master files and exception criteria, and to the program code responsible for performing the file and criteria comparisons with transaction data.

COMPLETENESS CONTROLS

All authorized transactions should be entered into and completely processed by the computer. Assessing the controls over completeness involves evaluating the entity's success in performing each of the critical elements listed below.

Critical Elements:

- All authorized transactions are entered into and processed by the computer, and
- Reconciliation is performed to verify data completeness.

A control for completeness is one of the most basic application controls, but is essential to ensure that all transactions are processed, and missing or duplicate transactions are identified. The most commonly encountered controls for completeness include the use of record counts and control totals, computer sequence checking, computer matching of transaction data with data in a master or suspense file, and checking of reports for transaction data.

Record counts and control totals.

In general, user-prepared totals established over source documents and data to be entered can be carried into and through processing. The computer can generate similar totals and track the data from one processing stage to the next and verify that the data was entered and processed, as it should have been. For example, a file of valid transactions (i.e.; transactions that pass data validation and editing) can contain a control record showing the record count and control totals for the file. As the file is processed through a job (or job step) the computer can calculate a record count and control totals for the transactions processed. The computer calculated amounts are compared with the amounts in the control record. Agreements in the amounts provide evidence that the processing was done accurately and completely. Disagreements indicate that a problem has occurred and needs to be investigated and rectified. On-line or real-time systems, where transactions are not entered as a batch, can still utilize this technique by establishing record counts and control totals over transactions entered during a specific time period, such as daily.

Computer sequence checking.

This control begins by providing each transaction with a unique sequential number. Some transactions originate on source documents with preassigned serial numbers. This number should be entered into the computer along with the other data on the transaction. The computer can identify numbers missing from the sequence and provide a report of missing numbers. The missing numbers should be investigated to determine whether they are numbers for voided source documents, or are valid documents that may have been lost or misplaced.

For transactions not on source documents with preassigned serial numbers, the computer can assign a unique sequential number as the data is entered. At a later point in processing, such as when transaction data updates a master file, the computer can verify that all numbers are accounted for. Again, missing numbers are reported for investigation.

Sequence checking is also valuable in identifying duplicate transactions. For example, two transactions with the same preassigned serial number for a source document would indicate that the transaction had been erroneously entered a second time. As another example, a file of sequential numbers for purchase orders could help prevent paying for the purchase more than once. After the purchased goods and vendor's bill are

received, a payment transaction with the purchase order number would be matched with the file containing all purchase order numbers, and an indicator for the payment would be recorded on the file for that purchase. The payment indicator would cause following payment transactions for the same purchase order to be rejected and reported for investigation.

Computer matching of transaction data.

This control involves matching transaction data with data in a master or suspense file. Unmatched items from both the transaction data and master or suspense file are reported for investigation. For example, a payroll system may be designed so that each employee's time and attendance sheet is matched to the employee's master pay record. Each time sheet that does not match with a master pay record is reported to determine whether it represents a valid employee and the master pay file needs to be updated. Each master pay record that does not receive a match is reported to determine whether a valid employee exists and a time sheet must be found or created so that the employee will receive pay on time. Also, master pay records with more than one time sheet are reported, which indicates a duplicate time sheet exists for one employee.

As another example, before initiating a payment, a vendor's invoice could be matched with a file containing records detailing goods received. Invoices not matched could be reported to show goods not received, and no invoices would be paid until a match occurred.

Checking reports for transaction data.

This activity involves checking each individual transaction with a detailed listing of items processed by the computer to verify that the transaction submitted was indeed processed. While an effective method, it is time-consuming and costly. Therefore, it is normally used with low-volume but high-value transactions, such as updating master files.

Reconciliations show the completeness of data processed at points in the processing cycle.

An application system is a collection or group of individual computer programs that relate to a common function. As data is entered into and processed through these programs, reconciliations of record counts and control totals at various points helps make certain that all the data was processed completely for the programs relative to the reconciliation. For example, control over a batch (a collection) of source documents may entail

a user to establish a record count and control total over the batch and record the amounts on a batch control sheet. The control information on the batch control sheet would be entered into the computer along with the information on each source document. The computer would compute a similar record count and control total for the batch as the data is entered. For the reconciliation, the computer would compare the computed amounts with the entered amounts from the batch control sheet. Agreement in the amounts indicates all data was completely entered. A disagreement may indicate some data is missing, an amount was entered incorrectly, or the batch control information was calculated or entered incorrectly. Batches with disagreements are commonly referred to as a "batch-out-of-balance." These should not undergo further processing until the disagreements are investigated and resolved. The record counts and control totals for batches in agreement are usable for reconciliations during later processing, as discussed below.

For applications where transactions are entered individually as they occur, this concept is still of use, as a record count and control total could be established over transactions entered during a specific time period, such as daily. Files should contain record count and control total information so that the computer can verify processing completeness as it progresses. Computer tape files would contain this information in a "trailer label" record that exists at the end of all data records on the tape. A disk file would contain this information in a control record. A program creating the file calculates and records the control information on the file. As a subsequent program processes the file, the computer calculates similar information and reconciles what it calculated with what was recorded on the file. Agreement in the amounts indicates all data was completely processed. This control information is commonly referred to as "run-to-run control totals."

As systems have become more integrated over the years, a file produced by one application may be used in another application. It is important to reconcile control information between the sending and receiving applications.

Performing the comparison of control numbers is commonly referred to as balancing, and should be done automatically by the computer, although some older systems may rely on manual balancing procedures. The control numbers for the balancing at key points should be documented, such as being printed on a control totals balance report, and should be reviewed by the data processing control group that monitors the completeness and accuracy of processing.

Reconciliations show the completeness of data processed for the total cycle.

Reconciliations should occur periodically that verify the completeness of data processed for a given cycle, such as daily, weekly, or relative to the processing cycle - for example, monthly for an accounts payable system. A control register is an effective tool to use in this process. Such reconciliations monitor the completeness of transactions processed, master files updated, and outputs generated, such as cash disbursements.

To illustrate with updating a master file, control information for this file should be recorded in the control register at the start of the cycle. Control information for the transactions entered that will update the master file should be reconciled with the control information over both accepted and rejected transactions. Control information for the accepted transactions that update the master file should be entered in the control register and added to the control information for the beginning master file. Control information for the updated master file should then be reconciled to the control register, should equal the sum of the beginning master file and accepted transactions. Another example illustrates reconciliation over disbursements for an accounts payable system. A vendor master file may contain a data field to record month-to-date payments. A total of all the vendors' month-to-date payments in the master file should be reconciled with and equal the total for all the checks written during the month to those vendors.

ACCURACY CONTROLS

The recording of valid and accurate data into an application system is essential to provide for an effective system that produces reliable results. Assessing the controls for valid and accurate data involves determining the entity's success in achieving each of the critical elements listed below.

Critical Elements.

- Data entry design features contribute to data accuracy,
- Data validation and editing are performed to identify erroneous data,
- Erroneous data are captured, reported, investigated, and corrected, and
- Review of output reports helps maintain data accuracy and validity.

Well-designed data entry processes can contribute to the entry of accurate and valid data. On the other hand, inadequacies in this area can contribute to data entry errors. The focus here includes source document design, preformatted computer terminal data entry screens, key verification, and the use of automated entry devices.

Source documents are designed to minimize errors.

Special purpose forms should be used that help the preparer to initially record data correctly and in a uniform format. This also facilitates the entry of data at a later stage. For example, rather than just providing a blank ("_____") for a social security number, a well-designed form would include the following to record the number: " - - ." For each type of transaction, the source document should provide a unique code or identifier, which should be preprinted on the document for data entry if it supports only one transaction type. The application computer programs use the transaction type for selecting the processing to be performed on the transaction. When several or more codes are options for identifying a data field's purpose, such as a payroll withholding, the options should be preprinted on the source document. A short list of options could appear under or near the data field, and a longer list could appear on the back of the document.

Preformatted computer terminal screens guide data entry.

Using preformatted computer terminal screens for data entry helps increase data accuracy at the point of entry. The computer screen (and the associated program code) prompts the terminal operator for data by field. Programmed routines allow the data to be checked or edited as it is keyed. After the data has been entered and passes the programmed edits, the computer screen prompt moves to the next data field indicating to the terminal operator the next data to be entered.

Key verification increases the accuracy of significant data fields.

For paper intensive source document environments found in large government transaction operations, key verification is a common technique still used to increase the accuracy of significant data fields. For this technique, after initial entry of transaction data, a separate individual reads the same source document and keys data into a machine that checks the results of keystrokes with what was originally keyed. Data that is keyed differently is reviewed to determine the correct data. As an example, the

Internal Revenue Service (IRS) uses key verification to ensure that certain data from tax returns have been entered correctly. This technique's effectiveness is reduced if the original data entry person is also the one performing the key verification, or if the key verifier is located next to or in the proximity of the original data entry person, thereby negating a separation of duties in performing this function.

Automated entry devices increase data accuracy.

The use of automated entry devices (e.g., optical or magnetic ink character readers) can reduce data error rates, as well as speed the entry process. The IRS's use of preprinted labels, showing the taxpayer's name, address, and social security number is such an example. This information can be entered without keying the data, which ensures a more accurate and faster process.

A crucial control activity involves identifying erroneous data at the point it enters the application system, or at some later point during the processing cycle. This is accomplished in a process that is commonly called data validation and editing. Programmed validation and edit checks are key to this process, and are generally performed on transaction data entering the system, as well as data prior to updating master files, and data resulting from processing.

Programmed validation and edit checks identify erroneous data.

Programmed validation and edit checks are, for the most part, the most critical and comprehensive set of controls in assuring that the initial recording of data into the system is accurate. These controls are built as early as possible in the input process, and provide extensive coverage over as many data fields that a user feels a need to control. This approach is used extensively in both batch and on-line environments.

Programmed validation and edit checks can effectively start as the data are being keyed in at a computer terminal using preformatted computer screens. For example, an alphabetic character entered for a numeric field can be rejected as it is keyed. Also, data involving quantities or values can be checked to ensure they fall within reasonable predetermined limits, or within the range of a set of numbers. Further, key fields, such as a loan account number, or parts number in an inventory system, could employ a check digit to help validate that the number is being entered correctly. The check digit is an additional number contained in the key field, which is determined by a formula from the other numbers of the key field. The

computer recalculates the check digit using the formula with the numbers entered and compares the calculation with the check digit entered. Agreement between the check digit entered and the recalculated check digit provides support that all the numbers were entered correctly with no transposition errors.

Programmed validation and edit checks may also occur after data has entered the application. For example, transaction data may enter the processing cycle from another application and should be subjected to these checks. This should occur before updating master files, and should be performed early in the data flow to reduce the processing associated with incorrect data. Some of these later checks may focus on determining the validity of a transaction data field. For example, a benefit payment system may compare the transaction's disability type code to a table of valid codes. Other checks may focus on determining the validity of the transaction itself, such as comparing vendor invoices with an approved vendor file, and with a file on purchase orders and goods received.

These checks also help provide that data recorded in key fields on master files are accurate and valid. One check, known as relationship editing, compares data in a transaction record with data in a master record for appropriateness and correctness before updating the master record. As an example, a personnel action to effect a promotion for an employee on a master pay file will first establish a match between the transaction record and pay record based on the employee's social security number. However, before posting the new grade level and salary to the pay record, the computer may ensure that the names in the transaction record and pay records agree, and that the old grade level in the personnel action is the same grade level as the existing grade level in the pay record. Only after agreement with both items will the pay record be updated.

The total transaction should undergo data validation and editing, and all fields in error should be identified before the transaction is rejected from further processing.

Tests are made of critical calculations.

Data resulting from processing routines, such as critical calculations, should also be tested to ensure the results are valid. For example, limits and reasonableness checks would help identify erroneous results before they cause some negative impact. Unusual items could be held and reported for management review and approval. Through such means, disbursements

exceeding a certain amount could be routed for a manager's review and approval prior to release of the disbursement.

Before the auditor can rely on the entity's data validation and editing checks, discussed in this and the previous sections, to reduce the audit risk, the auditor must determine the adequacy of the general controls over these checks. To be effective, the general controls should protect the program code and any related tables associated with the validation and edit routines from unauthorized changes.

Overriding or bypassing data validation and editing is restricted.

Many systems allow data validation and edit routines to be bypassed, which could allow the system to accept and process erroneous data. Using the bypass capability (sometimes referred to as an override) should be very limited and closely controlled and monitored by supervisory personnel. For example, each override should be automatically logged and reviewed by supervisors for appropriateness and correctness.

Transactions detected with errors need to be controlled to ensure that they are corrected and reentered in a timely manner. During data entry, particularly with more modern systems, an error can be identified and corrected at the data entry terminal. With errors identified during the data processing cycle, however, a break generally has been made from the data entry terminal. Therefore, errors identified cannot be communicated in a real-time mode back to personnel entering the data for immediate correction. An automated error suspense file is an essential element to controlling these data errors, and the errors need to be effectively reported back to the user department for investigation and correction.

Rejected transactions are controlled with an automated error suspense file.

Using an automated error suspense file should control rejected transactions. Transactions entered into this file should be annotated with:

- codes indicating the type of data error,
- date and time the transaction was processed as well as the error identified, and
- the identity of the user who originated the transaction.

Record counts and control totals should be developed automatically during processing of erroneous transactions to the suspense file and used in reconciling the transactions successfully processed. A control group should be responsible for controlling and monitoring the rejected transactions.

The suspense file should be purged of the related erroneous transaction as the correction is made. Record counts and control totals for the suspense file should be adjusted accordingly. Periodically, the suspense file should be analyzed to determine the extent and type of transaction errors being made, and the age of uncorrected transactions. This analysis may indicate a need for a system change or some specific training to reduce future data errors.

General controls should protect the suspense file from unauthorized access and modification, in order for the auditor to be able to rely on this control technique to reduce audit risk.

Erroneous data are reported back to the user department for investigation and correction.

Systems that allow user groups to enter data at a computer terminal often allow data to be edited as it is entered, and generally allows immediate correction of errors as they are identified. Error messages should clearly indicate what the error is and what corrective action is necessary. Errors identified at a later point in processing should be reported to the user originating the transaction for correction.

Some systems may use error reports to communicate to the user department the rejected transactions in need of correction. More modern systems will provide user departments' access to a file containing erroneous transactions. Using a computer terminal, users can initiate corrective actions. Again, error messages should clearly indicate what the error is and what corrective action is necessary. The user responsible for originating the transaction should be responsible for correcting the error. All corrections should be reviewed and approved by supervisors before being reentered into the system, or released for processing if corrected from a computer terminal.

Output can be in several forms, including printed reports, data accessible on-line by users, and computer files that will be used in a later processing cycle, or by other programs in the application. Output should be reviewed and control information should be reconciled to determine whether errors occurred during processing. Various reports are typically produced by

application systems that, if reviewed, help maintain the data's accuracy and validity. Production and distribution of these reports need to be controlled, and to be effective, they need to be reviewed by the user.

Control output production and distribution.

Someone should be assigned responsibilities for seeing that all outputs are produced and distributed in accordance with the requirements and design of the application system. In larger organizations with mainframe computer environments, this responsibility is typically assigned as part of the responsibilities of a data control group, which falls within the information systems department. This group, or some alternative, should maintain a schedule by application that shows the output products produced, when they should be completed, whom the recipients are, the copies needed, and when they are to be distributed. The group should review output products for general acceptability and reconcile control information to determine the completeness of processing.

Printed reports should contain proper identification, including a title page with the report name, time and date of production, and the processing period covered by the report. Reports should also have an "end-of-report" message to positively indicate the end of a report. A report may have pages missing at the end of the report, which may go undetected without this type of message. Controls and procedures are needed to ensure the proper distribution of output to authorized users. Without control over distribution, users may not receive needed output in a timely manner, and unauthorized persons may gain access to output containing privacy or sensitive information. Each output should be logged, manually if not done automatically, along with the recipients of the output, including outputs that are transmitted to a user's terminal device. For these transmissions, the computer system should automatically check the output message before displaying, writing, or printing to make sure the output has not reached the wrong terminal device. In the user department, outputs transmitted should be summarized daily and printed for each terminal device, and reviewed by supervisors.

Occasionally, errors may be identified in output products requiring corrective action, including possibly rerunning application programs to produce the correct product. A control log of output product errors should be maintained, including the corrective actions taken. Output from reruns should be subjected to the same quality review as the original output.

Reports showing the results of processing are reviewed by users.

The user department has ultimate responsibility for maintaining data quality, and should review output reports for data accuracy, validity, and completeness. Some typical reports that are commonly produced for review by users include the following:

- An error report that shows rejected transactions, the cause(s) of the rejections, and corrections needed.
- A transaction report that lists important data fields of every valid transaction in the processing cycle. Transactions that are internally generated by the application (e.g., inventory orders as stocks reach the reorder quantity) are included and listed separately.
- A master record change report (also known as a "was-is" report) that shows the contents of every master record before and after every master record change.
- An exception report that lists items requiring review and approval. These items may be valid, but exceed parameters established by management, such as disbursements exceeding a dollar amount.

A control totals balance report lists the control fields and the totals calculated by the computer to show the results of processing. If similar figures were predetermined and entered with the data submitted for processing, the report will also identify agreements and variances.

CONTROLS OVER INTEGRITY OF PROCESSING AND DATA FILES

Example of items to cover:

- Procedures ensure that the current versions of production programs and data files are used during processing.
- Programs include routines to verify that the proper version of the computer file is used during processing.
- Programs include routines for checking internal file header labels before processing.
- The application protects against concurrent file updates.

SENTRY'S AUTHORIZED USERS LIST

(As indicated within the BOP's SENTRY Risk Assessment, December 2000)

Criminal Division

Department of Justice

Drug Enforcement Administration (DEA) - El Paso Intelligence

Drug Enforcement Administration (DEA) - National Drug Intelligence

Federal Bureau of Investigation

Immigration and Naturalization

Interpol Headquarters

Justice Management Division

Office of Pardon Attorney

Office of the Corrections Trustee

Office of the Inspector General

Parole Commission

United States Army

United States Attorneys

United States Marshals Service

United States Marshals Service Transportation

United States Navy

United States Probation Office

United States Sentencing Commission

ABBREVIATIONS

BOP	The Federal Bureau of Prisons
CA	Computer Associates
CCO	Community Corrections Office
DBMS	Database Management System
Department	The Department of Justice
FISCAM	Federal Information System Controls Audit Manual
GAO	Government Accounting Office
GUM	General Use Manual
IDMS	Integrated Data Management System
IFRP	Inmate Financial Responsibility Program Module
IRS	Internal Revenue Service
J&C	Judgment and Commitment Order
JCN	Justice Consolidated Network
JDC-D	Justice Data Center in Dallas, Texas
JMD	Justice Management Division
MAN	Metropolitan Area Network
NCC	Network Control Center
OIG	The Office of the Inspector General
PSI	Pre-Sentence Investigation Report
PLRA	The Prisoner Litigation Reform Act
USMS	United States Marshals Service
VCCLEA	Violent Crime Control and Law Enforcement Act of 1994

DESCRIPTION OF SENTRY DATABASE MODULES

***The Inmate Population Monitoring module* -** tracks inmate movement in every BOP facility, or while an inmate is in transit, regardless of location or time of day. It also provides immediate access to the current population of any institution, region, or community facility. The module encompasses admission processing; admission or release status; custody, quarters, unit, caseworker, and work assignments; inmate count monitoring; special inmate monitoring; education, court, and hospital callouts; inmate facility designations; release and transfer processing; program treatment monitoring; and social and education data reporting. A number of preformatted reports are available to assist institutions in managing day-to-day operations.

***Sentence Monitoring module* -** calculates and tracks all aspects of an inmate's sentence. It ensures that inmates' release dates are accurate and that sentence calculations comply with statutory requirements and the BOP regulations. As federal statutes regarding inmates' sentences have become increasingly complex, the module must now track inmates' education and disciplinary records, as well as participation in drug or boot camp programs, and include factors based on these records into the sentence. As lawsuits by inmates routinely challenge sentence calculations, the consistency and accuracy offered by the Sentence Monitoring module enables the BOP to successfully defend itself.

***Designations module* -** is the means by which all inmates are assigned to specific facilities. Using criteria identified in the BOP's inmate classification system — severity of offense, history of violence, type of detainer, etc. — and public safety factors where appropriate, the module calculates a total security score and inmate security level, factors in specific inmate requirements (e.g., drug abuse program, medical condition, judicial recommendation), and displays a list of appropriate facilities for the Inmate Designator to choose from, in order of distance from the inmate' s residence. If any of these facilities houses other inmates that the inmate needs to be separated from, SENTRY displays a warning. It records the Designator's choice of facility, creates a log entry to advise the facility that the inmate was designated there, and updates the running total of inmates on their way to that facility. This module also helps the BOP's Office of Capacity Planning determine security level requirements for future institutions.

***Central Inmate Monitoring module (CIM)* -** identifies inmates who the court has determined need special evaluation (e.g. review of mental status). The need to separate inmates who have threatened each other was the initial reason for developing this module. It tracks inmates' "separatees" and allows the BOP staff to designate them to institutions where they will be safe. If an inmate is admitted to a facility where separation from others is warranted, the institution is notified and may take appropriate action. According to the BOP, it has not had an injured inmate as a result of the BOP's failure to separate as considered necessary.

In addition, the system records inmates' participation in disruptive groups and street gangs such as the Aryan Brotherhood (AB),[20] the Black Guerrilla Family (BGF),[21] and the Latin Kings.[22] Managing the distribution of these gangs throughout the BOP's facilities lessens the likelihood of gang-on-gang violence.

The final function of CIM is the protection of Government witnesses. These inmates' identities and locations are shrouded from all SENTRY resources other than those in protective custody units and a limited number of management users in Regional and Central offices. If an unauthorized user attempts to retrieve information about these inmates, no indication is given that they even exist.

***Administrative Remedy System module* -** reports and tracks the responses of the BOP's inmates' complaints and the procedure for doing so. This module replaced the labor-intensive process of disseminating a variety of documents to the inmates. Each Administrative Remedy is logged electronically. An automated tracking capability helps track cases in process and monitor critical due dates.

---

[20] The letters "AB" represent Aryan Brotherhood, a prison gang that originated in 1967 in the California Department of Corrections at San Quentin. Many members display white supremacist ideology, but they are first and foremost a criminal gang involved in the methamphetamine trade. AB has also spawned other white gangs in the prison system. Several common nicknames for AB members are Alice, Alice Baker, Tip & Brand, and the Brand.

[21] The initials "BGF" (Black Guerilla Family) combined with cross sabers, shotguns, and black dragons taking over prison towers provide the backdrop for this tattoo. Former Black Panther George L. Jackson started this gang at San Quentin State Prison in California in 1966. The gang has a strong political ideology that promotes Black revolution and the overthrow of the government.

[22] The largest Latino gang in Chicago, and perhaps in the United States, is the Latin King and Queen Nation. The Latin Kings have their roots in the Puerto Rican experience in Chicago. Gentrification has pushed Chicago's Puerto Rican community and their gangs from Harrison Street on the near west side to Lincoln Park and then to Humboldt Park — which is now undergoing substantial gentrification. The Latin Kings are also a major force in the barrios of New York. Black & Gold is a documentary film of the politicalization and repression of the Latin Kings in New York City in the 1990s. Latin Kings have chapters all across the United States.

Inmate Discipline module - tracks every report of a breach of institution rule filed against an inmate from beginning of the process to the end to ensure compliance with policy. For example, the module ensures the appropriate regulations are imposed according to the seriousness of the act committed. This module is integrated into the inmate population monitoring module's generalized retrieval program to allow the addition of discipline information when searching for groups of inmates. It also interacts with modules used by the Office of Research to provide statistics on inmate assaults against staff members and other inmates.

Inmate Financial Responsibility Program module (IFRP) - records, manages, and monitors court-ordered financial obligations imposed on inmates. IFRP payments are deducted from institution earnings and applied to an inmate's financial obligations. These funds are automatically transmitted to the appropriate organization for disbursement to the Crime Victims Fund and other recipients.

State Billing module - tracks and reports amounts owed to different states for an inmate serving a state sentence in a BOP facility. Per diem rates are entered into SENTRY in accordance to the length of time served in a BOP facility. SENTRY accounts for the various rate computations and reports, to each jurisdiction, the inmate's name, length of time spent, per diem rate, and total dollar amount involved. Summary and management reports are distributed indicating the time an inmate spends in any BOP facility in any given year.

Property Management System module - keeps track of the BOP's accountable property and automatically computes the depreciation of capitalized property.

APPLICATION CONTROL CRITERIA

1. The GAO's Federal Information System Controls Audit Manual.

2. Department of Justice Order 2640.2D, Information Technology Security, Chapter 2, "Security Requirements."

3. OMB Circular A-130, Appendix III, Section A 3.b.2.

4. National Institute of Standards and Technology, Special Publication 800-18.

5. National Institute of Standards and Technology, Federal Information Processing Standards Publication 73, Section 3.1.1.

6. Office of the Inspector General Audit report number 03-13 "Independent Evaluation Pursuant to the Government Information Security Reform Act," fiscal year 2002, The Justice Consolidated Network.

7. The BOP's Standard Operating Procedures.

8. The BOP's SENTRY Contingency Plan.

9. The BOP's Information Technology Investment Report.

10. The BOP's Community Corrections Management Operations Procedures (PS 5100.07).

11. The BOP's SENTRY "General Use Manual."

12. The BOP's "SENTRY System Security Guide," dated June 23, 2000.

13. The BOP's "SENTRY System Security Plan," dated February 25, 2000.

14. The BOP's Security Evaluation Report.

15. The BOP's Policy Standard 1237.12.

U.S. Department of Justice

Federal Bureau of Prisons

Office of the Director *Washington, DC 20534*

June 24, 2003

MEMORANDUM FOR [redacted]
ASSISTANT INSPECTOR GENERAL
FOR AUDIT

FROM: [redacted] Director
Federal Bureau of Prisons

SUBJECT: Response to the Office of the Inspector General's (OIG) Draft Audit Report: Select Application Control Review of the Federal Bureau of Prisons' SENTRY Database System

The Bureau of Prisons (BOP) appreciates the opportunity to respond to the recommendations from the OIG's draft report entitled Select Application Control Review of the Federal Bureau of Prisons' SENTRY Database System.

Our comments to Recommendations 1, 4, 5, 6, and 7 are provided below.

Recommendation #1 - OIG recommends the BOP Director ensure that BOP management: Enforce the BOP (PS) 5100.07, which states that all CCO's are to use the BP-337 for inputting initial inmate data as the sole source document.

Response: The Bureau agrees with the recommendation. By July 1, 2003, all community corrections officers will be notified of the requirement, as outlined in PS 5100.07, that the BP-S337.051 form is the mandatory and sole data input form used during the designation process.

Recommendation #4 - OIG recommends the BOP Director ensure that BOP management: Update the BOP's "SENTRY System Security Guide," dated June 23, 2000, to require the routine generation and review of exception reports.

Response: The Bureau agrees with the recommendation. The Bureau will update the SENTRY System Security Guide by December 12, 2003, to require the routine generation and review of exception reports.

Recommendation #5 - OIG recommends the BOP Director ensure that BOP management: Provide the Information Security Officer with the exception reports generated from the audit logs in the time period specified by the BOP's "SENTRY System Security Guide."

Response: The Bureau agrees with the recommendation. Once the SENTRY System Security Guide is revised, the Bureau will begin creating and forwarding the exception reports to the Information Security Officer on at least a weekly basis. These exception reports will include attempts by users to execute transactions from unauthorized terminals as well as attempts to view or update information that they are not authorized to access. Target date for completion is October 1, 2003.

Recommendation #6 - OIG recommends the BOP Director ensure that BOP management: Enforce the BOP's existing access control policy by properly configuring SENTRY's workstation controls to ensure that users with system authorization are restricted to areas of the system that they have been authorized to access, and no more.

Response: The Bureau agrees with the recommendation. The Bureau's SENTRY system cannot currently restrict access to transactions based upon a person's UserID. We are in the initial stages of porting SENTRY to a Web architecture. As part of this port, we will be augmenting our current terminal id based security to include security based upon UserID. This will mean that an authorized user must also be at an authorized workstation in order to perform any restricted transactions. This is a level of security beyond what the OIG is requesting. This port of SENTRY is projected to be completed by FY 2005.

Recommendation #7 - OIG recommends the BOP Director ensure that BOP management: Update SENTRY's General Use Manual to reflect proper procedures for entering initial inmate records into SENTRY.

Response: The Bureau agrees with the recommendation. The Bureau is currently preparing a complete revision of the SENTRY General Use Manual. This revision will include converting the document to HTML, adding extensive search capabilities, links to additional information as well as updates to reflect the current working state of the SENTRY system. This revision will be

completed by December 5, 2003, and will include the instructions for the correct loading of initial inmate data.

We have not provided a response to Recommendations 2 and 3, as we have some disagreements with their implementation. We did not address these disagreements at the exit conference as the "owners" of this program were not represented. [redacted] has discussed this matter with [redacted], and we respectfully request an informal meeting with OIG to address these issues prior to providing an official response. Mr. [redacted] has relayed to Mr. [redacted] that this approach is acceptable.

If you have any questions regarding this response, please contact [redacted], Senior Deputy Assistant Director, Program Review Division, at [redacted]

OFFICE OF THE INSPECTOR GENERAL, AUDIT DIVISION ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT

The BOP's response to the audit (Appendix VIII) describes the actions taken or plans for implementing our recommendations. This appendix summarizes our response and the actions necessary to close the report.

Recommendation Number:

1. **Resolved.** The BOP agreed to enforce the BOP Policy Standards (PS) 5100.07, which states that all Community Corrections Offices (CCOs) are to use the BP-337 for inputting initial inmate data as the sole source document by July 1, 2003. To close this recommendation, the BOP needs to provide the OIG with evidence that the CCOs have received notification of the requirement.

2. **Unresolved**. The BOP did not respond to the OIG recommendation to redesign the BP-337 so that mandatory information needed for tracking BOP inmates can be documented. The BOP stated the appropriate BOP personnel were not present at the exit conference to address this issue. Therefore, the BOP requested an informal meeting with the OIG to address this issue prior to providing an official response. Please contact the OIG to schedule this meeting.

3. **Unresolved**. The BOP did not respond to the OIG recommendation to modify the BP-337 to indicate which source document should be used to complete each field within this form. The BOP stated the appropriate BOP personnel were not present at the exit conference to address this issue. Therefore, the BOP requested an informal meeting with the OIG to address this issue prior to providing an official response. Please contact the OIG to schedule this meeting.

4. **Resolved.** The BOP agreed to update the BOP's "SENTRY System Security Guide," dated June 23, 2000, to require the routine generation and review of exception reports by December 12, 2003. To close this recommendation, the BOP needs to provide the OIG with a copy of the updated and approved "SENTRY System Security Guide."

5. **Resolved**. The BOP agreed to provide the Information Security Officer with the exception reports generated from the audit logs in the time period specified by the BOP's "SENTRY System Security Guide" (SSG) by October 1, 2003. To close this recommendation, the BOP needs to provide the OIG with evidence of this occurring.

6. **Resolved.** The BOP agreed to enforce the BOP's existing access control policy by properly configuring SENTRY's workstation controls. Currently, the BOP is in the process of porting SENTRY to a Web architecture. This process is projected to be completed by FY 2005. To close this recommendation, the BOP needs to provide the OIG with a copy of the documented procedures and evidence of its full implementation.

7. **Resolved**. The BOP agreed to update SENTRY's General Use Manual (GUM) to reflect proper procedures for entering initial inmate records into SENTRY by December 5, 2003. To close this recommendation, the BOP needs to provide the OIG with a copy of the SENTRY's revised GUM and documented procedures.