



# **REVIEW OF THE UNITED STATES MARSHALS SERVICE'S PRISONER TRACKING SYSTEM**

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

Audit Report 04-29  
August 2004

# REVIEW OF THE UNITED STATES MARSHALS SERVICE'S PRISONER TRACKING SYSTEM

## EXECUTIVE SUMMARY

The United States Marshals Service (USMS) is responsible for housing federal prisoners awaiting trial in federal courts. On any given day, the USMS maintains custody of approximately 40,000 federal prisoners in local jails, contract facilities, and federal Bureau of Prisons (BOP) facilities throughout the country. Depending upon the length of a prisoner's court trial, time spent in USMS custody may run from several days to several years.

The USMS uses the Prisoner Tracking System (PTS) application to maintain tracking information for federal prisoners in USMS custody. The PTS contains information that is specific to each individual prisoner, including the prisoner's personal data, property, medical information, criminal information, and location. Additionally, the USMS uses the application as an informational and scheduling tool to assist USMS personnel in locating prisoners for court appearances. Prisoners' records are created using information obtained from key source documents, and this information is entered into the PTS. The PTS information is critical to processing and transporting prisoners because the USMS relies on the confidentiality, availability, and integrity of this information to ensure the safety of both the prisoners and the law enforcement officers charged with their care.

The objectives of this audit were to assess the effectiveness of select general controls for the PTS at the entity-wide level, review PTS's application controls, and perform data integrity testing. The Office of the Inspector General (OIG) performed this audit in accordance with the Government Auditing Standards. We used the Federal Information System Controls Audit Manual (FISCAM), Department of Justice (Department) policies and procedures, National Institute of Standards and Technology (NIST) Special Publications (SP), Office of Management and Budget (OMB) Guidelines, and the USMS's policies for prisoner processing and cellblock operations as criteria for this audit.<sup>1</sup> Specific details of our audit objectives, scope, and methodology appear in Appendix 1.

---

<sup>1</sup> The General Accounting Office's (GAO) FISCAM provides a methodology for guiding auditors in evaluating general and application controls used by information systems to protect the integrity, confidentiality, and availability of data. Descriptions of the FISCAM select general control and application control areas tested during this audit can be found in Appendix 3.

The USMS divides its operations into four regions with 94 district offices (DOs). To gain a nationwide representation of PTS operational activities, we elected to review DOs in each of the four USMS regions. We judgmentally selected the following sites: Alexandria, Virginia; Washington, D.C.; New York, New York; Houston, Texas; Philadelphia, Pennsylvania; Chicago, Illinois; Miami, Florida; and Phoenix, Arizona.

During our audit, we reviewed select general controls designed to protect the PTS application against unauthorized use, loss, or modification of its data.<sup>2</sup> Additionally, we reviewed application controls within the PTS that are used to ensure the validity, proper authorization, and completeness of transactions when entering prisoners' data into the PTS. We also tested output reports from the PTS application against source documents contained in prisoner file folders to assess the data integrity within the PTS.

## **SUMMARY RESULTS OF THE AUDIT**

### **Select General Controls**

Our review of the PTS identified weaknesses within each of the six general control categories designed to protect the PTS's system environment. Specifically, we found deficiencies within PTS's entity-wide security program planning and management, access controls, application software development and change control, system software, segregation of duties, and service continuity controls.

---

<sup>2</sup> General controls are entity-wide controls used to protect a system's environment. The PTS application can only be accessed via the USMS's Marshals Network (MNET); therefore, MNET serves as the PTS application's system environment. We reviewed the select general controls recommended by the FISCAM for evaluating and testing application controls because general controls for MNET were assessed during the OIG's January 2004 Federal Information Security Management Act (FISMA) review. The results of this assessment can be found in the OIG's Audit Report No. 04-11.

Following the chart below we summarize each vulnerability.

### GENERAL CONTROL AREAS

|                                                                                                     | VULNERABILITIES NOTED |
|-----------------------------------------------------------------------------------------------------|-----------------------|
| <b>Entity-wide Security Program Planning &amp; Management</b>                                       |                       |
| Assess risks periodically                                                                           |                       |
| Document an entity-wide security program plan                                                       |                       |
| Establish a security management structure and clearly assign security responsibilities              | Ö                     |
| Implement effective security-related personnel policies                                             | Ö                     |
| Monitor the security program's effectiveness and make changes as needed                             |                       |
| <b>Access Controls</b>                                                                              |                       |
| Classify information resources according to their criticality and sensitivity                       |                       |
| Maintain a current list of authorized users and ensure that their access is authorized              | Ö                     |
| Establish physical and logical controls to prevent and detect unauthorized access                   | Ö                     |
| Monitor access, investigate apparent security violations, and take appropriate remedial action      |                       |
| <b>Application Software Development &amp; Change Control</b>                                        |                       |
| Authorize processing features and modifications                                                     | Ö                     |
| Test and approve all new and revised software                                                       |                       |
| Control software libraries                                                                          |                       |
| <b>System Software</b>                                                                              |                       |
| Limit access to system software                                                                     |                       |
| Monitor access to and use of system software                                                        |                       |
| Control system software changes                                                                     | Ö                     |
| <b>Segregation of Duties</b>                                                                        |                       |
| Segregate incompatible duties and establish related policies                                        | Ö                     |
| Establish access controls to enforce segregation of duties                                          |                       |
| Control personnel activities through formal operating procedures and supervision and review         | Ö                     |
| <b>Service Continuity</b>                                                                           |                       |
| Assess the criticality and sensitivity of computerized operations and identify supporting resources | Ö                     |
| Take steps to prevent and minimize potential damage and interruption                                | Ö                     |
| Develop and document a comprehensive contingency plan                                               |                       |
| Test the contingency plan periodically and adjust it as appropriate                                 | Ö                     |

## ***Entity-wide Security Program Planning and Management***

Within the area of entity-wide security program planning and management, a security manager for the PTS application was not appointed and employees lacked adequate training and expertise. These deficiencies could negatively impact the USMS's ability to assess risks and provide protection for sensitive PTS data.

### ***Access Controls***

The USMS did not properly maintain the PTS authorized user list and allowed accounts to remain on the list for employees who no longer required access. Active but invalid accounts could enable an unauthorized user to gain access to sensitive information. Ineffective access controls diminish the reliability of data and subject the system to unauthorized use, loss, or modification.

Additionally, the USMS did not enforce physical access controls to protect data entry terminals from access by unauthorized users. Physical access to computer facilities that house data entry terminals could allow unauthorized individuals to obtain confidential printed reports, view sensitive data displayed on computer screens, and steal or damage equipment.

### ***Application Software Development and Change Control***

Interviews conducted during our site visits disclosed that program modifications were not properly authorized. Application users are generally responsible for requesting and authorizing system changes. However, we found that the PTS application end-users were either unfamiliar with or unaware of the process for requesting changes to the application. Inadequacies with controls that protect application software from unauthorized changes could result in the USMS allowing unauthorized modifications to be made to the PTS application.

### ***System Software***

The effectiveness of the PTS's system software controls were jeopardized because the USMS is using outdated programming and database management software to support the application. The use of such outdated software prevents the USMS from implementing new security enhancements that are designed to protect the application. This deficiency also increases the risk that without timely software updates that enhance functionality and

security, data could be improperly processed by the application or insufficiently protected.

### ***Segregation of Duties***

Policies and procedures are not in place to segregate incompatible duties for personnel performing critical functions, such as prisoner intake and record creation processes. Compounding this problem, the USMS has no formal procedures to guide personnel performing activities that directly affect the reliability of the PTS data. Without the segregation of duties, and in the absence of formal procedures, the USMS cannot ensure the confidentiality, integrity, and availability of PTS data during the prisoner processing cycle.

### ***Service Continuity***

Backup tapes were not being rotated off-site, and the contingency plan for the PTS had not been tested. We also found that key personnel responsible for emergency response activities lacked sufficient training and expertise. System administrators were not familiar with the current version of the software supporting the PTS application or the location of their local DOs database files. Consequently, the USMS may lose the capability to restore the PTS's application software and data because it is relying on insufficient preventative measures to mitigate service disruptions. Moreover, the USMS is depending on inadequately trained individuals to respond appropriately in the case of an emergency and to assist in restoring the application software and data files of this mission critical operation.

## Application Controls

In addition to the general controls findings previously mentioned, our review of the PTS identified deficiencies within each of the four application control areas we tested. Following the chart below is a summary of each vulnerability indicated in the chart.

### APPLICATION CONTROL AREAS

|                                                                                                             | VULNERABILITIES NOTED |
|-------------------------------------------------------------------------------------------------------------|-----------------------|
| <b>Authorization Controls</b>                                                                               |                       |
| All data are authorized before entering the application system                                              | 0                     |
| Restrict data entry terminals to authorized users for authorized purposes                                   | 0                     |
| Master files and exception reporting help ensure all data are processed and are authorized                  |                       |
| <b>Completeness Controls</b>                                                                                |                       |
| All authorized transactions are entered into and processed by the computer                                  | 0                     |
| Reconciliations are performed to verify data completeness                                                   |                       |
| <b>Accuracy Controls</b>                                                                                    |                       |
| 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                                          | 0                     |
| Output reports are reviewed to help maintain data accuracy and validity                                     | 0                     |
| <b>Controls Over Integrity of Processing and Data Files</b>                                                 |                       |
| Procedures ensure that the current version of production programs and data files are used during processing |                       |
| Programs include routines to verify that the proper version of the computer files is used during processing |                       |
| Programs include routines for checking internal file header labels before processing                        |                       |
| Mechanisms within the application protect against concurrent file updates                                   | 0                     |

### Authorization Controls

We found problems with authorization controls that ensure the validity of transactions. The USMS has not formally established baseline requirements for key source documents used to create prisoner records in the PTS or for the proper authorization of source documents. This lack of standards from the USMS headquarters for key source documents resulted in

inconsistent data collection, record creation, and file maintenance practices throughout the USMS sites audited. Formal standards would help to ensure, at a minimum, that each prisoner file folder contains photographs, medical information, and fingerprint cards. Also, such standards would help to ensure that critical identifying information is collected from a reliable source. These standards could also provide reasonable assurance against the misidentification or mishandling of a prisoner due to inaccurate, unauthorized, or unreliable data.

Additionally, supervisory or independent reviews to ensure the proper authorization of source documents and transactions were not being performed prior to the data being entered into the PTS. This occurred because the USMS has not implemented adequate authorization standards for source documents or required that supervisory reviews be performed on a consistent basis. This precautionary measure would help ensure that transactions are properly authorized and supported by a reliable source document that has been signed. It would also assist with the prevention of unauthorized, inappropriate, or incorrect transactions from being entered that could negatively impact the integrity of data within the PTS.

Controls for ensuring that data entry terminals are used for authorized purposes, such as audit logs, were weak. Audit logs that help to recreate events and track user activity were not being maintained for the PTS application. The USMS management does not require that audit logs be maintained for the PTS to track the occurrence of unauthorized activities. In our opinion, this condition increases the risk to the USMS that covert activity by a user, such as entering an unauthorized transaction resulting in the early release of a prisoner, may go undetected. The risks to the safety of the USMS personnel who process and transport prisoners and the general public are increased when coupled with weak authorization controls over source documents and the lack of supervisory reviews of transactions.

### ***Completeness Controls***

The PTS application does not effectively use a completeness control known as computer sequence checking to automatically perform global database searches. Computer sequence checking would identify or prevent the assignment of multiple USMS numbers to the same prisoner.<sup>3</sup> At present, each of the 94 DOs maintains a local PTS database

---

<sup>3</sup> Computer sequence checking helps identify missing or duplicate numbers in a series. USMS numbers are assigned sequentially to prisoners processed by a DO; however, database searches are conducted by prisoner name rather than USMS number.

and the application is only programmed to automatically perform searches for existing name and USMS number information within a user's own local database. The current configuration does not provide assurance that the prisoner does not have an existing USMS number in any one of the other 93 local USMS databases. Without the capability to perform global searches of all existing databases, the USMS cannot ensure that it complies with its own policies prohibiting the multiple assignment of USMS numbers to the same prisoner.

### ***Accuracy Controls***

Within the area of accuracy controls, we found that the USMS management does not have an effective means of determining the existence of erroneous data, such as uncorrected errors, or the severity of errors in data entered into or processed by the application. Information regarding erroneous data was not collected and reported back to the USMS management for investigation or correction. This occurred because the USMS did not require that information regarding such data be collected. This type of oversight could negatively impact the reliability of the PTS's data through the propagation of undetected errors throughout the application.

We also found that the PTS's accuracy controls were impacted because the USMS did not adequately control the production and distribution of sensitive PTS output reports. Specifically, authorized users of the PTS print sensitive output reports to shared network printers used by non-authorized employees. This practice exposes sensitive system data at a level above that which employees are required to perform their duties. Without adequate controls over the distribution of output reports, unauthorized individuals may inadvertently gain access to output reports and divulge sensitive and confidential information.

### ***Controls Over Integrity of Processing and Data Files***

Controls over integrity of processing and data files for the PTS application were deficient. This was due to the USMS not ensuring that each installation of the PTS application at the 94 DOs nationwide protects against simultaneous updates. We observed that the application allowed two users to update the same file concurrently, which raises doubt as to which user's information was accurately recorded and processed by the application. This type of system malfunction could negatively impact the reliability of data within the PTS application.

## Data Integrity

In addition to the deficiencies discovered within PTS's general and application controls, our audit disclosed weaknesses within PTS's data integrity. We tested the two factors that contribute to data integrity: completeness of prisoner records and accuracy of information. Our review discovered weaknesses within both areas tested. A summary of each vulnerability follows the chart.

### Data Integrity Assessment Factors

|                                                                                             | VULNERABILITIES NOTED |
|---------------------------------------------------------------------------------------------|-----------------------|
| <b>Completeness of Information</b>                                                          |                       |
| Records contain all of the data elements and documents used as support for the transactions | 0                     |
| <b>Accuracy of Information</b>                                                              |                       |
| Output reports reflect the data obtained from the source documents                          | 0                     |

#### *Completeness of Information*

Our findings revealed deficiencies in the completeness of prisoner records. Many of the prisoner file folders we reviewed were missing key source documents used to validate data entry transactions and to substantiate the actions taken by USMS personnel.<sup>4</sup> This occurred because the USMS did not establish and implement standards regarding data collection in order to comply with federal records retention requirements. Incomplete prisoner file folders pose a significant risk to the USMS's ability to validate the PTS transactions, verify information, and justify the actions of its employees. Additionally, maintaining adequate and proper documentation of program activities enables the USMS to protect the federal government's legal and financial interests.

#### *Accuracy of Information*

Reviews of output reports produced by the PTS application disclosed discrepancies in the accuracy of information. Output reports help to maintain the accuracy and validity of data within a system and determine the completeness of processing. We found that prisoner identifying information, such as a prisoner's date of birth, appearing on the PTS output reports did not match source documents contained in the prisoner's file folder.

---

<sup>4</sup> The GAO defines a source document as any form of information that serves as the basis for entry of data into a computer system.

Additionally, critical dates, such as a prisoner's custody date, did not correlate with dates on source documents in the prisoner's file folder. Inaccurate PTS information could result in the overpayment of jail bills, the untimely release of a prisoner, or the misidentification of a prisoner requiring special handling within the prisoner population.

## **CONCLUSION AND RECOMMENDATIONS**

We consider our findings in the areas of select general controls, application controls, and data integrity to be major weaknesses. We further conclude that the state of the PTS's existing controls poses a high risk to the protection of its data from unauthorized use, loss, or modification.<sup>5</sup>

We conclude that these weaknesses occurred because the USMS did not fully comply with current Department policies and procedures, NIST standards, OMB guidelines, or its own procedures for prisoner processing and cellblock operations. If not corrected, these security vulnerabilities could impair the USMS's ability to fully ensure the integrity, confidentiality, and availability of data within the PTS.

This report contains 20 recommendations for improving select general controls, application controls, and the integrity of data for the PTS. In general, we recommend that the USMS:

- Appoint a security manager responsible for the PTS application;
- Develop a training program to ensure that PTS users receive specialized training before being granted access to the application and ensure that system administrators are trained in their responsibilities;
- Review access authorizations for the PTS application and update the PTS authorized user list in a timely manner;
- Ensure that existing measures, such as door locks, are used to provide protection against unauthorized access to sensitive areas;

---

<sup>5</sup> NIST SP 800-18 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 requirements for protecting the confidentiality, integrity, and availability of system information into three basic categories – high, medium, and low – according to the system's sensitivity level. Specifically, a high risk is considered a critical concern of the system.

- Inform users regarding policies and procedures for requesting changes to the application and update the PTS's production environment by replacing outdated software with current software;
- Develop and enforce policies and procedures to segregate duties among staff performing critical PTS functions;
- Identify and train employees involved in emergency response procedures in their roles and responsibilities; maintain emergency contact lists on-site; rotate and store backup tapes off-site; and test the PTS contingency plan annually;
- Standardize the record creation process throughout the USMS for the PTS and establish key source document requirements for data collection;
- Implement a control, such as requiring the supervisory authorization of data, to ensure that before information is entered into the system, transactions are supported by properly authorized source documents;
- Maintain and review audit trails for the PTS application;
- Modify PTS to perform automatic global database searches to assist with the prevention of assigning multiple USMS numbers to the same prisoner, report erroneous data to the PTS users department for investigation and correction, and protect the PTS output reports containing sensitive privacy information from access by unauthorized persons;
- Ensure each installation of the PTS application protects against simultaneous updates of the same record by more than one end-user; and
- Maintain adequate source documents in prisoners' file folders to substantiate employee activities and implement quality control measures to ensure data integrity.

## TABLE OF CONTENTS

|                                                                                                                                          | <u>Page</u> |
|------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| I. BACKGROUND .....                                                                                                                      | 1           |
| PTS Application System Environment .....                                                                                                 | 2           |
| II. FINDINGS AND RECOMMENDATIONS.....                                                                                                    | 3           |
| 1. Select General Controls .....                                                                                                         | 3           |
| Entity-wide Security Program Planning and Management.....                                                                                | 3           |
| Access Controls.....                                                                                                                     | 7           |
| Application Software Development and Change Control.....                                                                                 | 11          |
| System Software.....                                                                                                                     | 13          |
| Segregation of Duties .....                                                                                                              | 15          |
| Service Continuity .....                                                                                                                 | 17          |
| 2. Application Controls.....                                                                                                             | 21          |
| Authorization Controls.....                                                                                                              | 22          |
| Completeness Controls.....                                                                                                               | 27          |
| Accuracy Controls.....                                                                                                                   | 29          |
| Controls Over Integrity of Processing and Data Files .....                                                                               | 33          |
| 3. Data Integrity Testing.....                                                                                                           | 34          |
| Completeness of Information.....                                                                                                         | 35          |
| Accuracy of Information .....                                                                                                            | 37          |
| III. CONCLUSION .....                                                                                                                    | 40          |
| APPENDIX 1 OBJECTIVES, SCOPE, AND METHODOLOGY .....                                                                                      | 43          |
| APPENDIX 2 FIELDWORK SITE VISIT MAP.....                                                                                                 | 45          |
| APPENDIX 3 FEDERAL INFORMATION SYSTEM CONTROLS AUDIT<br>MANUAL, SELECT GENERAL CONTROLS AND<br>APPLICATION CONTROLS.....                 | 46          |
| APPENDIX 4 GENERAL ACCOUNTING OFFICE, ASSESSING THE<br>RELIABILITY OF COMPUTER-PROCESSED DATA,<br>DATA INTEGRITY ASSESSMENT FACTORS..... | 48          |
| APPENDIX 5 GENERAL ACCOUNTING OFFICE, FEDERAL<br>INFORMATION SYSTEM CONTROLS AUDIT MANUAL,<br>GENERAL CONTROLS REVIEW GUIDELINES .....   | 49          |

|             |                                                                                                                             |    |
|-------------|-----------------------------------------------------------------------------------------------------------------------------|----|
| APPENDIX 6  | GENERAL ACCOUNTING OFFICE, FEDERAL INFORMATION SYSTEM CONTROLS AUDIT MANUAL, APPLICATION CONTROLS REVIEW GUIDELINES.....    | 67 |
| APPENDIX 7  | GENERAL ACCOUNTING OFFICE, ASSESSING THE RELIABILITY OF COMPUTER-PROCESSED DATA, DATA INTEGRITY ASSESSMENT GUIDELINES ..... | 76 |
| APPENDIX 8  | ACRONYMS AND ABBREVIATIONS.....                                                                                             | 77 |
| APPENDIX 9  | GENERAL CONTROLS CRITERIA .....                                                                                             | 78 |
| APPENDIX 10 | APPLICATION CONTROLS CRITERIA.....                                                                                          | 79 |
| APPENDIX 11 | DATA INTEGRITY ASSESSMENT CRITERIA .....                                                                                    | 81 |
| APPENDIX 12 | AUDITEE RESPONSE .....                                                                                                      | 82 |
| APPENDIX 13 | ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE REPORT.....                                                              | 92 |

# REVIEW OF THE UNITED STATES MARSHALS SERVICE'S PRISONER TRACKING SYSTEM

## I. BACKGROUND

The United States Marshals Service (USMS) is responsible for housing federal prisoners awaiting trial in federal courts. On any given day, the USMS maintains custody of approximately 40,000 federal prisoners in local jails, contract facilities, and federal Bureau of Prisons (BOP) facilities throughout the country. Depending upon the length of a prisoner's court trial, time spent in USMS custody may run from several days to several years.

The USMS Prisoner Tracking System (PTS) supports the USMS's responsibility to maintain custody of individual federal prisoners while criminal proceedings are pending. This period of custody extends from the time of their arrest or remand to the USMS by the court until the prisoner is sentenced, released from custody, or returned to the custody of the U.S. Parole Commission or the BOP.

The PTS was implemented by the USMS in March 1993 to maintain tracking information for federal prisoners and to monitor federal prisoners in state and local detention facilities under contract to the USMS. The PTS replaced the Prisoner Population Management System. The PTS captures information necessary to complete the administrative processing, housing, safekeeping, health care, and disposition of federal prisoners in USMS custody.<sup>6</sup> From fiscal year (FY) 2001 to FY 2004, the PTS's total operating costs were \$3,370,000, with annual operating costs averaging \$842,500. Another \$1,070,000 is projected for FY 2005 and a project to upgrade the PTS application's functionality, funded at \$5 million over a 5-year period, is currently underway.<sup>7</sup>

The PTS is also used as an informational and scheduling tool. As an informational tool, the PTS provides identifying data specific to each prisoner, including the prisoner's personal data, property, medical information, criminal information, location, and time spent at a facility. As a scheduling tool, PTS information assists USMS personnel in locating prisoners to be transported for court appearances.

---

<sup>6</sup> USMS System Security Plan for the Prisoner Tracking System (PTS)/USMS Automated Booking System (USMS-ABS), June 2003.

<sup>7</sup> Operating costs were obtained from budget requests submitted to the Office of Management and Budget by the Justice Management Division.

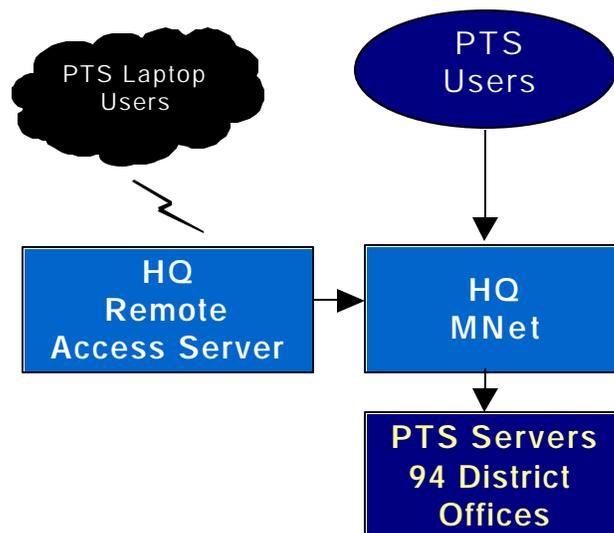
In addition, the PTS also contains records of court proceedings generated during the day-to-day processing and disposition of prisoners in the USMS's custody. Prisoners' records contained within the PTS are created using information obtained from key source documents, such as the individual custody and detention form, intake photos, Federal Bureau of Investigation (FBI) finger print cards, and the prisoners' medical form.

## **PTS Application System Environment**

The PTS application software runs on a local server in each of the 94 USMS district offices (DOs) located throughout the U.S. and its territories. In addition to the application, a database is maintained on the local server that contains information relative to prisoners processed by the DO. Thus, the USMS PTS environment consists of 94 copies of the PTS application along with 94 individual databases.

At each DO, PTS client workstations connect to their local PTS application server to gain access to database information. PTS users initially log into the Marshals' Network (MNET) located at the USMS headquarters in Arlington, Virginia, in order to log into the PTS application server at their location. Additionally, remote users can gain access to the PTS server in their district by dialing into the remote access server located at the USMS headquarters. The user is required to provide additional remote access user identification information in order to log into MNET. The following diagram depicts the PTS's access configuration.

### **PTS Access Configuration**



## II. FINDINGS AND RECOMMENDATIONS

Our review of select general controls designed to protect the PTS's system environment identified weaknesses with the PTS's entity-wide security program planning and management, access controls, application software development and change control, system software, segregation of duties, and service continuity controls. We also identified deficiencies with the PTS's application controls that are used to help ensure the validity of transactions and proper authorization of data. These deficiencies included inadequate authorization controls, completeness controls, accuracy controls, and controls over integrity of processing and data files. Our findings relative to data integrity included deficiencies with the completeness of prisoner records and the accuracy of information contained within the PTS. In our judgment, these findings are major weaknesses in the PTS. We consider the system overall to be at a high risk to the protection of its data from unauthorized use, loss, or modification. These weaknesses occurred because the USMS did not develop or fully enforce its own policies or comply with the Department policies, NIST standards, and OMB guidelines. If not corrected, these weaknesses could impair the USMS's ability to fully protect the integrity, confidentiality, and availability of data contained within the PTS database.

### 1. SELECT GENERAL CONTROLS

General controls are entity-wide access controls used to safeguard a system's environment. Our review of select general controls for the PTS application identified weaknesses in all six of the Federal Information System Controls Audit Manual (FISCAM) general controls areas – entity-wide security program planning and management, access controls, application software development and change control, system software, segregation of duties, and service continuity controls.

#### **Entity-wide Security Program Planning and Management**

Entity-wide security program planning and management allows an organization to establish a security control structure that enables senior

management to identify and address security risks. An effective plan requires that an organization:

- Assess risks periodically;
- Document an entity-wide security program plan;
- Establish a security management structure and clearly assign security responsibilities;
- Implement effective security-related personnel policies; and
- Monitor the security program’s effectiveness and make changes as needed.

We confirmed that the USMS adequately assessed risks, documented an entity-wide security program plan, and monitored the security program’s effectiveness. However, vulnerabilities were noted as indicated in the following chart:

**Entity-wide Security Program Planning & Management**

| CONTROL AREAS                                                                                 | VULNERABILITIES NOTED |
|-----------------------------------------------------------------------------------------------|-----------------------|
| Assess risks periodically                                                                     |                       |
| Document an entity-wide security program plan                                                 |                       |
| <b>Establish a security management structure and clearly assign security responsibilities</b> | 0                     |
| <b>Implement effective security-related personnel policies</b>                                | 0                     |
| Monitor the security program’s effectiveness and make changes as needed                       |                       |

***Establish a Security Management Structure and Clearly Assign Security Responsibilities***

Security managers are an essential component of an organization’s security control structure and are responsible for reporting compliance issues to senior management. Security managers perform specific functions to ensure the effectiveness of security plans established to protect systems that maintain sensitive data. These functions include assessing and managing risks to protect the confidentiality, availability, and integrity of system data. Security managers are also actively involved in addressing threats posed by authorized internal users and unauthorized outsiders attempting to gain access to system data, and implementing logical and physical access controls to prevent breaches in security.

Our review of the PTS’s entity-wide security program planning and management revealed that no security manager for the PTS application had

been formally appointed. This occurred because USMS did not establish a security management structure and clearly assign security responsibilities.

The PTS's system security plan, included in the application's certification and accreditation documentation, lists an individual as the "Computer Systems Security Officer (CSSO)." However, when we interviewed the individual designated as the CSSO, we found that he was not actively involved in providing security manager duties for the PTS application and did not know he had been officially appointed. Subsequent interviews with USMS management officials confirmed that the USMS had not officially appointed a security manager to address computer security practices specific to the PTS application.

OMB Circular A-130 requires that an entity "assign responsibility for security for each major application to a management official." Furthermore, the guidance recommends that the individual be "assigned the responsibility in writing to assure the application has adequate security."

Without the appointment of a security manager for the PTS application, the USMS cannot ensure that the application has adequate security or that security-related tasks are carried out. Such tasks include properly authorizing system access, communicating security policies to the user population, and monitoring risk management activities.

**Recommendation:**

We recommend that the USMS:

1. Appoint a security manager responsible for the PTS application and ensure the appointment is documented.

***Implement Effective Security-Related Personnel Policies***

The USMS did not implement effective security-related personnel policies to assure that employees possess adequate training and expertise. The USMS's Prisoner Services Division (PSD) offers specialized PTS training at a federal government facility in Glynco, Georgia. However, users of the PTS application who perform critical functions such as record creation and record updating were not required by management to attend the specialized training prior to being granted access to the system.

OMB Circular A-130 states that users of an application should receive specialized training prior to being granted access, and that the specialized training should focus on their responsibilities and rules of expected behavior

for the application. We found that no policy existed that required users to receive specialized training prior to or within a reasonable period after hire, and that the majority of PTS users had never received the specialized training offered by the USMS.

Additionally, we determined that USMS personnel functioning as system administrators for the application did not have adequate training and expertise. According to the system administrator position description provided by the USMS, system administrators are responsible for "operating, troubleshooting, repairing, and maintaining IT systems." Additionally, the document states that employees must possess the requisite technical knowledge to sustain the availability of the hardware and software environment. The system administrator must also be competent to maintain operating systems, applications, and data elements. However, we found that some system administrators were unfamiliar with their hardware and software environment and lacked specific knowledge, such as what version of the application was running on their server, what files supported the application, or where the PTS database they were responsible for protecting was located.

OMB Circular A-130 requires that an aspect of an entity's information management policy should require that employees, such as system administrators, are trained in skills appropriate to the management and protection of system information and that this training shall be an ongoing part of the information life cycle.<sup>8</sup>

These deficiencies could negatively impact the USMS's ability to assess risks and provide protection for sensitive PTS data.

### **Recommendations:**

We recommend that the USMS:

2. Develop a training program to ensure that users of the PTS application receive specialized training before being granted access to the application.
3. Ensure that individuals performing system administrator duties are properly trained in their responsibilities.

---

<sup>8</sup> OMB defines the term "information life cycle" as the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

## **Access Controls**

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. Access controls are both logical and physical. These controls are used to ensure that staff duties and responsibilities are implemented in a way that safeguards programs.

In order to successfully implement the critical elements of access controls, an organization must:

- Classify information resources according to their criticality and sensitivity;
- Maintain a current list of authorized users and ensure that their access is authorized;
- Establish physical and logical controls to prevent or detect unauthorized access; and
- Monitor access, investigate apparent security violations, and take appropriate remedial action.

We found that the USMS successfully classified information resources and investigated apparent security violations. However, vulnerabilities were identified as indicated in the chart below:

### **Access Controls**

| <b>CONTROL AREAS</b>                                                                           | <b>VULNERABILITIES NOTED</b> |
|------------------------------------------------------------------------------------------------|------------------------------|
| Classify information resources according to their criticality and sensitivity                  |                              |
| <b>Maintain a current list of authorized users and ensure that their access is authorized</b>  | 0                            |
| <b>Establish physical and logical controls to prevent and detect unauthorized access</b>       | 0                            |
| Monitor access, investigate apparent security violations, and take appropriate remedial action |                              |

### ***Maintain a Current List of Authorized Users and Ensure That Their Access is Authorized***

We found that the PTS's list of authorized users contained multiple errors and inaccurate information. This resulted because USMS headquarters did not properly maintain a current list of authorized users that was coordinated with information maintained by the DOs. Additionally, the USMS did not regularly review the PTS authorized user list, validate the levels of access authorized to users, or update the user list accordingly.

We obtained a consolidated user list for all authorized PTS users from USMS headquarters. Officials at USMS headquarters informed us that system administrators at each DO were responsible for maintaining their respective user list by adding and deleting names. Therefore, we sorted the headquarters list by DO location to produce a list for each of the following sites we visited: Eastern District of Virginia (E/VA) in Alexandria, Virginia; the District Court for the District of Columbia (DC/DC) in Washington, D.C.; the Southern District of New York (S/NY) in New York, New York; the Southern District of Texas (S/TX) in Houston, Texas; Eastern District of Pennsylvania (E/PA) in Philadelphia, Pennsylvania; the Northern District of Illinois (N/IL) in Chicago, Illinois; the Southern District of Florida (S/FL) in Miami, Florida; and the District of Arizona (D/AZ) in Phoenix, Arizona.

Our review of the eight DO lists disclosed that: a) the USMS allowed accounts to remain on the application’s authorized user list for employees who no longer required access to the PTS; and b) the authorized user list generated by USMS headquarters did not match the authorized user lists maintained at the DOs.

The following chart represents specific deficiencies noted during our review of the authorized user list at each site we visited. The “total number of user accounts” column represents the total number of names appearing on the PTS authorized user list obtained from the USMS headquarters for each site visited. The figures in the “number determined invalid or unknown” column represent accounts that could not be confirmed as “valid” by the responsible system administrator. User accounts in this category were determined to be “invalid” if the names had not been removed from the user list although the user had departed the site or was no longer authorized access to the PTS application. User accounts were determined to be “unknown” if the system administrator could not attest to the users’ identity or their authority to access the application.

### PTS Authorized User List

| Sites Visited  | Total Number of User Accounts According to HQ | Number Determined Invalid or Unknown by Comparing DO to HQ | Percentage of Invalid Accounts |
|----------------|-----------------------------------------------|------------------------------------------------------------|--------------------------------|
| E/VA           | 76                                            | 16                                                         | 21%                            |
| DC/DC          | 111                                           | 64                                                         | 58%                            |
| S/NY           | 144                                           | 33                                                         | 23%                            |
| E/PA           | 94                                            | 35                                                         | 37%                            |
| S/TX           | 346                                           | 113                                                        | 33%                            |
| N/IL           | 88                                            | 41                                                         | 47%                            |
| S/FL           | 143                                           | 45                                                         | 31%                            |
| D/AZ           | 138                                           | 45                                                         | 33%                            |
| <b>Totals:</b> | <b>1140</b>                                   | <b>392</b>                                                 | <b>34%</b>                     |

**Source:** The OIG’s analysis of user lists workpapers for eight sites visited.

A further review of the authorized user list for each site visited revealed that erroneous or invalid entries appeared on the user list obtained from USMS headquarters. However, the system administrators provided evidence that they were properly maintaining the user list at their site. We surmised that the discrepancies involving erroneous entries and unknown accounts occurred because the consolidated user list generated by USMS headquarters was not incorporating the additions, deletions, and changes made at the DO level.

The DO user lists extracted from the HQ consolidated user list contained various column headings such as userID, name, and date of the user's last login. In addition to the deficiencies previously noted, the following deficiencies contributed to rendering accounts "invalid:"

- Employees' official titles and their DO locations were improperly entered in the "name" field of the user list;
- Descriptions of the employees' positions appeared in the "name" field of the user list as opposed to the users' proper name;
- UserID information (e.g., last name, first initial) frequently did not match the actual user's name that appeared on the DO list; and
- Entries were "missing name information," because userIDs did not have an accompanying user name.

Prior to our departure from each site, the system administrators agreed to remove entries deemed "invalid or unknown users" from their PTS-authorized user list.

The above conditions do not comply with the Department's Order 2640.2E, "Information Technology Security," which requires that each user be identified as unique. The Department's Order further 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.

Allowing "invalid and unknown" user accounts to remain on the PTS authorized user list could jeopardize the effectiveness of security features designed to restrict the user's access to only that information which is necessary for operations and for which the user has a need to know. The existence of active but invalid accounts could enable an unauthorized user to gain access to sensitive information. For example, accounts represented by an employee's official title or position description, as opposed to a specific userID, are equivalent to generic or "guest" accounts. Guest accounts could allow various members of a DO to share the same userID and password

information to gain access to and make changes within a system. Any actions performed by these accounts, detrimental or otherwise, would be difficult to trace back to a specific user. OMB Circular A-130 sets forth personnel controls that strengthen access authorizations, provides for individual accountability, and emphasizes the need to hold users accountable for their actions. Ineffective access authorizations, such as allowing generic accounts to remain on an authorized user list, diminish the reliability of data and subject the system to unauthorized use, loss, or modification.

**Recommendation:**

We recommend the USMS:

4. Ensure that access authorizations for the PTS are reviewed and that USMS headquarters update its authorized PTS users list in a timely manner to incorporate changes from the DOs.

***Establish Physical and Logical Controls to Prevent and Detect Unauthorized Access***

Physical access controls consist of measures such as locking doors to facilities housing computers that process sensitive information and posting guards at entrance points to those facilities.

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. As discussed previously, we determined that the PTS's access authorizations or logical access controls were weak because USMS headquarters did not properly maintain a current list of authorized users.

Physical access controls were adequately enforced at seven of the eight sites visited. However, we encountered an instance where physical access controls were not enforced to prevent or detect unauthorized access. We observed that the locks on the door to a restricted area at one location were not engaged. Adequate physical access controls to the building were provided by armed guards; however, the door to the restricted area housing

data terminals and sensitive PTS information was left unlocked and potentially accessible by unauthorized visitors to the building.

NIST Special Publication (SP) 800-18, "Guide for Developing Security Plans for Information Technology Systems" explains that physical access controls protect computer resources and "restrict the entry and exit of personnel."

By not enforcing adequate physical access controls, the USMS exposed the PTS to the risk that unauthorized individuals could gain access to sensitive information. Additionally, the USMS's ability to protect sensitive printed data or equipment from theft or inadvertent disclosure would be compromised if an unauthorized person entered a restricted facility containing sensitive PTS equipment and data.

**Recommendation:**

We recommend that the USMS:

5. Ensure that existing measures, such as door locks, are used to provide protection against unauthorized access to sensitive areas.

**Application Software Development and Change Control**

Application software development and change control is an essential component of an application's system development life cycle (SDLC). These measures allow managers responsible for seeing that software supporting their operation meets the requirement of the organization and produces reliable data.

An entity should institute policies, procedures, and techniques to ensure responsible individuals:

- Authorize processing features and program modifications properly;
- Test and approve all new and revised software; and
- Control software libraries.

We determined that the USMS adequately tested new software and controlled its software libraries. However, our review disclosed a deficiency as indicated in the chart below:

**Application Software Development & Change Control**

| CONTROL AREAS                                          | VULNERABILITIES NOTED |
|--------------------------------------------------------|-----------------------|
| <b>Authorize processing features and modifications</b> | 0                     |
| Test and approve all new and revised software          |                       |
| Control software libraries                             |                       |

***Authorize Processing Features and Modifications***

An entity should ensure that its SDLC policies provide a structured approach that identifies who can authorize modifications to the system, and the policies should be distributed to all users. Ultimately, application end users have the primary responsibility for taking part in the design and implementation of processing features and approving subsequent changes made to the application.

Although the USMS had a documented SDLC for the PTS that included instructions for requesting changes to the application, many of the PTS users at the DOs we visited were not aware of the policy and were not aware of how to formally request changes to the application. This condition exists because the USMS has not adequately disseminated established change control policies throughout the organization.

The Department’s Order 2640.2E, Chapter 1, “Security Program Management,” directs components to develop a process to integrate security into various stages of a system’s life cycle and to ensure that changes to any system are controlled.

Ineffective management over modifications to application software could hamper an entity’s ability to prevent knowledgeable programmers from covertly changing program code to access sensitive data. Additionally, the entity could risk the likelihood of implementing incorrect or outdated versions of operating system and application software. Failure to establish such controls could allow the introduction of malicious code that could lead to the loss or destruction of sensitive data.

**Recommendation:**

We recommend that the USMS:

- 6. Ensure PTS users are informed of the policies and procedures for requesting changes to the application.

**System Software**

Often referred to as a “utility,” system software is used by programmers to configure a system and manage the input, processing, output, and data storage associated with all of the applications that run on a system. System software operates at a higher level than application software and can thus be used to read, modify, or delete critical or sensitive information and to bypass security controls built into application programs. Moreover, some system software can change data and program code without leaving an audit trail, such as programming software and database management systems (DBMS).<sup>9</sup>

Weakness in controls over system software could negatively impact the reliability of information produced by applications supported by the computer system. An organization can protect the integrity of system software in the following ways:

- Limiting access to system software;
- Monitoring access to and use of system software; and
- Controlling system software changes.

Although the USMS effectively limited access to system software and monitored its use, deficiencies were noted in the area indicated in the following chart:

**System Software**

| <b>CONTROL AREAS</b>                         | <b>VULNERABILITIES NOTED</b> |
|----------------------------------------------|------------------------------|
| Limit access to system software              |                              |
| Monitor access to and use of system software |                              |
| <b>Control system software changes</b>       | <b>0</b>                     |

---

<sup>9</sup> DBMSs organize data in a database and manage actions such as queries and updates.

## ***Control System Software Changes***

The PTS application consists of a database controlled by a DBMS and application programming software. The database is used to store data pertaining to the USMS's prisoner operations and prisoner identifying information. The application's user interface and functionality are modified using a commercial-off-the shelf programming language.

We determined that the controls for the PTS's system software changes were deficient. The USMS is using an outdated version of the database management software and programming language to support the PTS application in its production environment. According to the DBMS and application programming software vendor, the company no longer provides technical support for these products and has not done so for over five years. This condition exists because the USMS has not updated and patched these critical components although the vendor has produced three version updates since the release of the version currently used by the USMS.

OMB Circular A-130 recommends that entities periodically review security controls and seek ways to improve security such as utilizing technical tools to look for security problems and installing the latest software patches. NIST SP 800-40 specifically addresses procedures for handling security patches. NIST warns that not patching information systems in a timely manner can impact operations and degrade the confidentiality, availability, and integrity of a system's information.

The USMS's use of outdated programming and database management software could prevent the USMS from implementing security enhancements such as system security patches designed to protect the PTS application from malicious software. This deficiency also increases the risk that without timely updates, data entered into the PTS could be improperly processed by the application.

### **Recommendation:**

We recommend that the USMS:

7. Remove outdated versions of the PTS's application programming software and database management system from the production environment and replace with current versions that are supported by the vendor.

## **Segregation of Duties**

Segregation of duties is the practice of dividing the steps in a critical function among different individuals. In a computer processing environment, such a control assists in the prevention of one individual having complete control of the input, processing, and output stages of the information cycle and keeps a single individual from subverting a critical process.

Organizations should take steps to ensure that they:

- Segregate incompatible duties and establish related policies;
- Establish access controls to enforce segregation of duties; and
- Control personnel activities through formal operating procedures and supervision and review.

Controls that sustain the proper segregation of duties enable management to maintain control over personnel activities. Additionally, segregation of duties requires the establishment of formal operating procedures as well as active supervision and review of these activities.<sup>10</sup>

We found that the USMS had adequately established access controls to enforce segregation of duties. However, deficiencies were noted within other control areas affecting segregation of duties as indicated below:

### **Segregation of Duties**

| <b>CONTROL AREAS</b>                                                                               | <b>VULNERABILITIES NOTED</b> |
|----------------------------------------------------------------------------------------------------|------------------------------|
| <b>Segregate incompatible duties and establish related policies</b>                                | 0                            |
| Establish access controls to enforce segregation of duties                                         |                              |
| <b>Control personnel activities through formal operating procedures and supervision and review</b> | 0                            |

### ***Segregate Incompatible Duties and Establish Related Policies***

Our review of the PTS disclosed that the USMS had not properly segregated incompatible duties and established related policies to ensure personnel understand their roles and responsibilities. Duties and responsibilities associated with the USMS's PTS system life cycle were not

<sup>10</sup> OMB Circular A-130 defines procedures as detailed steps to be followed by users, system operations personnel, or others to accomplish a particular task (e.g., preparing new user accounts and assigning the appropriate privileges). It adds that procedures normally assist in complying with applicable security policies, standards, and guidelines.

properly segregated among staff. At the USMS's headquarters, only one individual is assigned to code, test, and implement changes to the PTS application. The same individual is authorized to move changes into the production environment and distribute those changes to the 94 DO servers. This condition allows a single individual to have complete control over application programming and change control processes that should be divided among two or more individuals.

The Department's Order 2640.2E, Chapter 2, specifies the requirement for segregation of duties. The Order states that system duties should be "defined and documented." OMB Circular A-130 discusses the requirement for personnel security and recommends that an application's security plan incorporate measures for the separation of duties. Furthermore, NIST SP 800-12, "Computer Security Handbook" describes separation of duties as "dividing roles and responsibilities so that a single individual cannot subvert a critical process."

### ***Control Personnel Activities Through Formal Operating Procedures and Supervision and Review***

We found that the USMS has not developed formal policies and procedures to guide PTS users in performing their duties. Although the USMS has published a user manual for the PTS application, the manual falls short of providing formal operating procedures to be followed during critical processes such as the record creation process and subsequent record updates. These processes directly affect the confidentiality, integrity, and availability of the PTS data. Due to the lack of policies and procedures, we found that the record creation process was not standardized at any of the DOs we visited and that this condition exists throughout the USMS.

Following our site visits, we conferred with program managers for the PTS application who informed us that USMS headquarters has not provided formal operating policies and procedures to standardize the record creation process nor has it established standards for the collection of source information used to create prisoner records in the PTS. In the absence of formal policies and procedures, USMS headquarters and DOs had not formally established compensating controls such as requiring adequate supervision or review of information once a record is created or updated in the system. We observed that all DOs we visited operated differently with respect to the record creation process. We also found that while some DOs performed minimal supervisory reviews, others did not perform any supervisory reviews because they were not required to do so. Supervisory reviews, performed on a consistent basis, would help to detect the types of completeness and accuracy errors we found during our review of PTS data.

Without proper segregation of duties, the USMS increases the risks that erroneous or fraudulent transactions could be processed by the PTS and that computer resources could be damaged or destroyed. Additionally, without the USMS providing adequate controls over personnel activities, mistakes within the PTS could occur and go undetected and expose the application and its data to unauthorized use, loss, or modification.

**Recommendation:**

We recommend that the USMS:

8. Ensure policies and procedures for segregating duties are developed and enforced to provide assurance that distinct functions are performed by different individuals and that no individual has complete control over the PTS's processing functions.

**Service Continuity**

Service continuity measures provide for the capability to protect information resources and minimize the risk of unplanned interruptions. Service continuity controls involve ensuring that when unexpected events occur, critical operations continue without interruption or are promptly resumed and the organization's sensitive data are protected. To review the adequacy of its service continuity control, an entity should:

- Assess the criticality and sensitivity of computerized operations and identify supporting resources;
- Take steps to prevent and minimize potential damage and interruption;
- Develop and document a comprehensive contingency plan; and
- Test the contingency plan periodically and adjust it as appropriate.

The USMS had developed a contingency plan for the PTS application. However, we found other deficiencies within service continuity controls for the PTS application as indicated below:

### **Service Continuity**

| <b>CONTROL AREAS</b>                                                                                       | <b>VULNERABILITIES NOTED</b> |
|------------------------------------------------------------------------------------------------------------|------------------------------|
| <b>Assess the criticality and sensitivity of computerized operations and identify supporting resources</b> | 0                            |
| <b>Take steps to prevent and minimize potential damage and interruption</b>                                | 0                            |
| Develop and document a comprehensive contingency plan                                                      |                              |
| <b>Test the contingency plan periodically and adjust it as appropriate</b>                                 | 0                            |

#### ***Assess the Criticality and Sensitivity of Computerized Operations and Identify Supporting Resources***

We determined that the USMS successfully assessed the criticality and sensitivity of the PTS. However, we found that the USMS was deficient in identifying supporting resources within the DOs, which according to FISCAM includes human resources. Specifically, the USMS had not implemented a means to identify employees with service continuity responsibilities to users within the DOs, such as making an emergency contact list available to users at each site. Although the USMS maintained emergency contact lists at its headquarters, this deficiency occurred because the USMS did not require the DOs to maintain emergency contact lists to identify supporting resources on-site. Consequently, we found that the majority of the DOs did not maintain lists or make this information available to users.

NIST SP 800-34, "Contingency Planning Guide for Information Technology Systems," identifies contact lists as an element of an effective contingency plan and recommends the frequent review of such lists.

We also found that the USMS did not distribute its contingency plan, which contains emergency contact information, to supporting resources at the DOs – although execution of the contingency plan requires support from the system administrators assigned to the DOs. NIST SP 800-34 states that copies of contingency plans are typically provided to persons with service continuity responsibilities, such as the system administrators at the DOs.

We found that the information regarding emergency notifications was contradictory. The USMS PTS contingency plan identifies the Help Desk as the point-of-contact for service disruptions. The plan also states that the system administrator is responsible for maintaining the PTS servers at each field location and for reporting failures.<sup>11</sup> However, the plan presents an emergency response scenario wherein the system administrator would notify the Help Desk if the PTS server in the DO were disabled or unavailable. This scenario implies that system administrators, who are assigned to the DOs, are logically the first responders to users within the DOs and would most likely be contacted in case of emergency.

The absence of an emergency contact list to identify individuals at the DOs with service continuity responsibilities could cause users to become confused as to who should be notified in the event of an emergency, especially during non-duty hours. Additionally, without a copy of the USMS contingency plan for the PTS, individuals identified as supporting resources could become confused as to their service continuity roles and responsibilities.

In addition to our findings regarding the clear identification of supporting resources, we also found problems with the competence of those individuals involved in emergency response procedures. This occurred because the USMS had not required or provided sufficient training for employees with service continuity responsibilities.

NIST SP 800-18 provides guidance for developing security plans for information technology (IT) systems. The guidance states that responsible individuals should be designated as points-of-contact for a system and that the individuals should be knowledgeable about the system. We reviewed the system administrator position description and verified that the system administrators are designated as the primary representative at the DOs for IT functions and are responsible for responding to emergency situations. The position description specifically states that the employee must possess knowledge of IT systems "recovery" methods and practices. However, we found that system administrators, who were expected to assist with service continuity functions, lacked sufficient training to support the restoration of the application and its data files. Many of the system administrators at the sites we visited did not know specific characteristics of the system that would enable them to respond appropriately in case of an emergency. Specifically, system administrators did not know the version of the application running on their server or the location of their PTS database.

---

<sup>11</sup> According to the USMS PTS Contingency Plan dated June 2003.

In the event of an emergency or system abnormality, system administrators who are not properly trained could impede restoration of the data files and software by failing to respond appropriately.

**Recommendation:**

We recommend that the USMS:

9. Ensure that:

- a) employees involved in emergency response procedures are identified and trained in their emergency roles and responsibilities; and
- b) emergency contact lists are maintained on-site.

***Take Steps to Prevent and Minimize Potential Damage and Interruption***

Two aspects of preventing and minimizing damage or interruption of service to users of the PTS application include ensuring that: a) data and program backup procedures have been implemented; and b) staff have been trained to respond to emergencies.

Our review disclosed that backup tapes created at three of the DOs we visited were not consistently rotated off-site. This occurred because the USMS did not take steps to prevent and minimize potential damage and interruption by securing backup data away from the processing facility. Additionally, the USMS did not enforce its own guidelines for backup operations. The PTS security plan addresses contingency planning and states that backups should be created nightly and transferred off-site once a month.

NIST SP 800-34, "Contingency Planning Guide for Information Technology Systems," addresses backup methods. The guidance requires that backup policies be established and backup data stored off-site.

Consequently, the USMS may lose the capability to restore the PTS's application software and data by relying on insufficient preventative measures to mitigate service disruptions if tapes are not properly secured at an off-site location.

We also found that the USMS did not effectively ensure that staff had been trained to respond to emergencies, another aspect of minimizing

service interruptions. As discussed in the previous section regarding identifying supporting resources, we found that system administrators lacked sufficient knowledge of their system environment to provide support of recovery functions and that copies of the contingency plan that specified emergency roles and responsibilities had not been distributed to the DOs. Therefore, we recommended the USMS provide training for employees involved in emergency response procedures in Recommendation 9.

**Recommendation:**

We recommend that the USMS:

10. Ensure the PTS's backup tapes are properly rotated and stored at an off-site location.

***Test the Contingency Plan Periodically and Adjust It As Appropriate***

Although the USMS has developed and documented a contingency plan for the PTS application, it has not tested the plan. The Department's Order 2640.2E, Chapter 1, sets standards for contingency planning. It directs components to develop a contingency plan and test the plan annually. Furthermore, OMB Circular A-130 advises that untested contingency plans "may create a false sense of ability to recover in a timely manner."

The USMS places the PTS application and its data at risk by having an untested contingency plan for PTS. This deficiency could prevent the USMS from achieving timely restoration of critical PTS system information and diminish the assurance for continuity of operations in the event of a disaster.

**Recommendation:**

We recommend that the USMS:

11. Perform annual testing of the PTS contingency plan as required by the Department.

**2. APPLICATION CONTROLS**

Application controls are the structures, policies, and procedures that apply to application systems. Application controls include both the routines built into the computer program code and the external safeguards provided by users. External safeguards include manual measures performed by the

user such as reviewing output reports to determine that the computer processes data accurately.

Application controls help make certain that transactions are valid, properly authorized, and completely and accurately processed by the computer during all three phases of a processing cycle – input, processing, and output. At the time of input, data should be authorized, converted to an automated form, and entered into the system. This transaction is expected to be accurate, complete, and occur in a timely manner. For the processing phase, the computer accepts the data entered and files are updated in the system's database. Lastly, in the output phase, files and reports are generated by the system and the results are expected to yield an accurate processing of the data entered into the system. Controls should be in place to ensure that system outputs are controlled and distributed only to authorized persons.

To assess the effectiveness of application controls for the PTS, we reviewed authorization, completeness, accuracy, and integrity of processing controls. We identified deficiencies within all of the application control areas.

### **Authorization Controls**

Authorization controls are designed to ensure the validity of system transactions, and that the transactions performed represent an event that actually occurred during a given period. These controls regulate access to network resources and ensure that data is properly converted to an automated form so it can be processed accurately, completely, and timely.

Effective authorization controls should protect the data input process and include the following critical elements:

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

The USMS effectively used master files to help ensure that all data are processed. However, the following deficiencies were noted as indicated below:

### Authorization Controls

| CONTROL AREAS                                                                              | VULNERABILITIES NOTED |
|--------------------------------------------------------------------------------------------|-----------------------|
| <b>All data are authorized before entering the application system</b>                      | 0                     |
| <b>Restrict data entry terminals to authorized users for authorized purposes</b>           | 0                     |
| Master files and exception reporting help ensure all data are processed and are authorized |                       |

#### ***All Data Are Authorized Before Entering the Application System***

In order to ensure that all data are authorized before entering the application system, the FISCAM recommends that entities should implement measures to: a) control source documents and require authorizing signatures; and b) ensure supervisory reviews of data occur before entering the application system. The guidance acknowledges that paper source documents continue to play an important role during the data collection process. It cautions, however, that source documents should be controlled at the earliest point in the process and the data should be approved for use prior to entering the system. FISCAM also outlines requirements for performing independent or supervisory reviews of data regardless of the source. Our review disclosed deficiencies within both areas designed to ensure the proper authorization of data.

#### *Control source documents and require authorizing signatures*

We found that the USMS had not established controls over source documents, nor provided for their proper authorization. The GAO defines a source document as information that serves as the basis for the entry of data into a computer system. At all sites visited, we experienced difficulty in verifying the validity of the transactions we reviewed on PTS output reports due to the absence of source documents or because of inconsistencies with the collection and authorization of source documents. Therefore, the USMS was not able to attest to the validity of many transactions entered into the PTS or support the actions taken by its employees.

This condition occurred because the USMS had not formally established baseline requirements for source documents to provide a

reasonable assurance that critical identifying information is collected from a reliable source and is properly authorized. Additionally, the USMS had not implemented effective controls to ensure the proper authorization of data obtained from source documents prior to that data being used in PTS transactions.

Because baseline requirements for source documents had not been established by the USMS, we consulted the USMS employees performing record creation duties at the sites visited to determine what documents were used as source documents during the record creation process for the PTS. According to these employees, "key" source documents used to support the record creation process included: the individual custody and detention form (USM-129); FBI fingerprints card (FD-129); intake photo; and medical form (USM-552).

However, we found that because the USMS did not require employees to collect these source documents on a consistent basis, some DOs were not creating records based on documentation, but rather on interviews with prisoners. This occurred because the USMS had not formally established baseline requirements for source documents, such as the ones identified by USMS personnel, to provide a reasonable assurance that critical identifying information is collected from a reliable source and is properly authorized.

The USMS Cellblock Operations Directive advises employees to interview the prisoner during the initial intake process and collect identifying, arrest, prosecution, and medical information from the prisoner. The directive instructs employees to then enter the information obtained from the prisoner into the PTS to create a prisoner record. Under these conditions, the USMS is basing the reliability of the information collected on the integrity of the prisoner. Furthermore, the directive does not require that information be approved by an authorizing official or verified from other presumably more reliable sources such as court documents or forms completed by arresting officers.

OMB Circular A-130 advises federal agencies of the requirement for records management and states that agencies should "create and keep adequate and proper documentation of their activities."<sup>12</sup> OMB also warns that the lack of sufficient record keeping weakens agencies' ability to

---

<sup>12</sup> According to OMB, the term "records management" involves those managerial activities that support records creation, records maintenance and use, and records disposition. Records management allows agencies to achieve adequate and proper documentation of the policies and transactions of the federal government and effective and economical management of agency operations. (44 U.S.C. 2901(2))

responsibly perform their missions. OMB emphasizes the importance of record-keeping activities in each stage of a system's life cycle and directs agencies to document their procedures for information collection.

By failing to establish standards and controls over source documents and provide for the proper authorization of data, the USMS is jeopardizing the reliability of information collected during the record creation process. The reliability of data that serves as the basis for creating records in the PTS has a direct impact on the confidentiality, availability, and integrity of the data within the PTS.

Throughout our review, we also found inconsistencies with the collection of source documents, the authorization of data, and the maintenance of source documents within each prisoner's file folder. We noted that each DO essentially performed data collection, record creation, and file maintenance functions differently. These inconsistent practices resulted in the deficiencies discovered during our assessment of the PTS's data integrity. Specifically, we discovered findings within the PTS's completeness of information and accuracy of information. This occurred because the USMS had not standardized the record creation process throughout the USMS to aid in establishing control over source documents.

The GAO's guidance for assessing data reliability emphasizes the need for organizations to establish and adhere to standardized rules for the collection and use of data in computer processing environments. Additionally, adherence to the consistent interpretation of data rules, or the use of standardized processes, contributes to data reliability. The guidance stresses that standardization and consistency are particularly important to systems where data is entered at multiple sites, such as the PTS. The guidance asserts "inconsistent interpretation of data rules can lead to data that, taken as a whole, are unreliable." Failure to establish and enforce standardized procedures during critical processes, such as the record creation process for the PTS, could negatively affect the reliability of data within the PTS and impact the mission of the USMS.

We determined that the USMS's cellblock directive and user manual do not provide adequate data rules for employees or set standards for consistency during the record creation process. In the case of the PTS, formal standards would ensure, at a minimum, that each prisoner file folder contains photographs, medical information, and fingerprint cards; and that critical identifying information is collected from a reliable source such as a court document or agent arrest form. These standards could also provide reasonable assurance against the misidentification or mishandling of a prisoner due to inaccurate, unauthorized, or unreliable data.

**Recommendation:**

We recommend that the USMS:

12. Develop policies and procedures to:

- a) establish key source document requirements; and
- b) standardize the record creation process throughout the USMS for the PTS.

*Ensure supervisory reviews of data occur before entering the application system*

We also found that supervisory or independent reviews of source document information were not being performed on a consistent basis prior to the information being entered into the PTS. This was evidenced by the fact that handwritten "Individual Custody and Detention" (USM-129) forms, when used, did not always contain an authorizing signature. We observed that some DOs provided supervisory reviews during the record creation process while others did not. In addition, our review of prisoner file folders for accuracy of information disclosed discrepancies between information on source documents and information on the PTS output reports. We determined that these inaccuracies could have been prevented through the use of compensating controls such as supervisory reviews. This condition existed because the USMS did not require DOs to perform supervisory reviews of source documents and transactions.

In the absence of policies and procedures, supervisory reviews serve as a compensating control to ensure the proper authorization of source documents and transactions. OMB Circular A-130 prescribes the use of controls that monitor individual accountability and prevent and detect harm caused by "authorized individuals engaged in improper activities, whether intentional or accidental."

**Recommendation:**

We recommend that the USMS:

- 13. Implement a control, such as requiring the supervisory authorization of data, to ensure that before information is entered into the system, transactions are supported by properly authorized source documents.

### ***Restrict Data Entry Terminals to Authorized Users for Authorized Purposes***

The USMS has not implemented automated controls to trace actions on the system or ensure that data entry terminals are restricted to authorized users for authorized purposes. In our judgment, this weakness exists because the USMS does not maintain sufficient audit trails for the PTS application or require exception reports generated from audit logs. These reports could help identify unauthorized activities such as excessive errors made by an employee, record deletions, or attempts to gain access to resources to which the user is not authorized.

The Department's Order 2640.2E, 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. Audit logs provide a measure of assurance to enforce individual user accountability.

The USMS has not implemented automated controls to trace the occurrence of unauthorized activities or look for patterns of behavior by users of the PTS application. Therefore, USMS management has reduced its ability to monitor unauthorized attempts by users who have access to sensitive data above their access levels, unauthorized changes or deletions to prisoner records, or activities of users with privileged accounts. These vulnerabilities could impact the integrity of data within the PTS application.

#### **Recommendation:**

We recommend that the USMS:

14. Maintain and review audit trails for the PTS application as required by the Department.

#### **Completeness Controls**

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.

Completeness controls in an application provide safeguards for ensuring that:

- All authorized transactions are entered into and processed by the computer; and
- Reconciliations are performed to verify data completeness.

Our review of the USMS’s completeness controls for the PTS disclosed a deficiency as indicated in the following chart:

### Completeness Controls

| CONTROL AREAS                                                                     | VULNERABILITIES NOTED |
|-----------------------------------------------------------------------------------|-----------------------|
| <b>All authorized transactions are entered into and processed by the computer</b> | 0                     |
| Reconciliations are performed to verify data completeness                         |                       |

#### ***All Authorized Transactions Are Entered Into and Processed by the Computer***

In our review of completeness controls, we found that mechanisms built into the PTS application to perform computer sequence checking were inadequate for the PTS environment. This condition exists because the current configuration of the PTS application is restrictive in that the default system configuration confines sequence checking to the information contained in the local database and does not automatically extend the search to other DO databases.

The USMS Cellblock Operations Directive dictates that a prisoner will be assigned only one USMS number throughout their history with the agency. This would require that all 94 DO databases be searched to determine if the prisoner being processed has an existing USMS number assigned by another district before a district issued a USMS number.

The PTS application’s current software configuration is not conducive to automatically facilitate global database searches for prisoners’ USMS tracking numbers and name information because the USMS maintains a separate PTS database at each of its 94 DOs. Under the current configuration, PTS users can (by default) search only their local database to determine if a prisoner has been previously assigned a USMS number in their district. The PTS application is not programmed to automatically extend the search to other DO databases.

In order to determine if a prisoner has an existing USMS number that was assigned in another district, the PTS user must manually connect to the PTS database where the original USMS number and prisoner information is maintained. In the absence of knowing where the USMS number originated, the PTS user would have to manually perform 93 additional database searches to determine if a USMS number exists for the prisoner in another DO.

In its own directive regarding cellblock operations, the USMS advises PTS users to exit the application and go to the Federal Bureau of Prisons's (BOP) SENTRY application to search for the existence of a previously assigned USMS number.<sup>13</sup> This workaround solution is impractical because it forces PTS users to seek USMS information outside their own component that should be readily available on USMS systems. Additionally, not all users of the PTS application have access to BOP SENTRY; therefore, those users are restricted from performing the search within SENTRY to check for a pre-existing USMS number before assigning a new USMS number.

The current configuration of the PTS application constrains a name search to the local database. This constraint threatens compliance with the USMS's own directives regarding multiple USMS numbers. Additionally, it does not provide adequate assurance to the USMS that multiple USMS numbers will not be assigned to the same individual.

**Recommendation:**

We recommend the USMS:

15. Ensure that the PTS application is modified to perform automatic global database searches of all its DO databases to prevent the assignment of more than one USMS number to the same prisoner.

**Accuracy Controls**

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 well-designed data entry processes, easy-to-follow data entry screens, limit and reasonableness checks, and validation of

---

<sup>13</sup> The OIG conducted a Review of Select Application Controls for the BOP SENTRY application in its Audit Report No. 03-25, July 2003. SENTRY is BOP's primary mission support database. The system collects, maintains, and tracks critical inmate information, including inmate location, medical history, behavior history, and release data.

override actions for appropriateness and correctness. Without accuracy controls, invalid data may enter the system and produce unreliable results.

Entities can take steps to strengthen the effectiveness of accuracy controls by making sure that:

- 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
- Output reports are reviewed to help maintain data accuracy and validity.

We determined that the PTS’s data entry design and data validation and editing features were adequate. However, our review identified weaknesses with accuracy controls within the PTS application as indicated below:

### **Accuracy Controls**

| CONTROL AREAS                                                                  | VULNERABILITIES NOTED |
|--------------------------------------------------------------------------------|-----------------------|
| Data entry design features contribute to data accuracy                         |                       |
| Data validation and editing are performed to identify erroneous data           |                       |
| <b>Erroneous data are captured, reported, investigated, and corrected</b>      | 0                     |
| <b>Output reports are reviewed to help maintain data accuracy and validity</b> | 0                     |

#### ***Erroneous Data Are Captured, Reported, Investigated, and Corrected***

Our review of accuracy controls for the PTS application disclosed that erroneous data within the system was not identified, reported, investigated, nor corrected. Information on erroneous data is useful in forming a basis from which management can review and analyze the levels and types of transaction errors and formulate plans for corrective action. However, we found that information on rejected transactions and erroneous data was not analyzed because the USMS management did not require erroneous data to be collected and reported back for investigation and correction.

NIST SP 800-12, Chapter 4, “Common Threats,” warns that errors and omissions can threaten data and system integrity. It classifies some errors

as threats, because users frequently make errors that result in security problems. The guidance recommends that because application programs cannot detect all types of input errors or omissions, erroneous data should be reviewed to determine if errors cause threats to a system or result in vulnerabilities.

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 in PTS data 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 application.

Without the USMS effectively implementing measures to strengthen accuracy controls, invalid data may be entered in the system, be processed by the system, and cause production results that are unreliable to the system users. Our review of the PTS output reports for accuracy of the information reflects the existence of errors and omissions that accuracy controls are designed to detect.

**Recommendation:**

We recommend that the USMS:

16. Ensure erroneous data are collected and reported back to USMS management for investigation and correction.

***Output Reports Are Reviewed to Help Maintain Data Accuracy and Validity***

A critical element of accuracy controls includes the review of output reports to help maintain data accuracy and validity. An aspect of enforcing the review of output reports consists of maintaining control over system output production and distribution. We determined that the controls over system output production and distribution for the PTS application were weak because the USMS did not enforce strict controls to prevent the exposure of sensitive PTS output to non-authorized employees.

The USMS allows authorized PTS users and non-authorized USMS employees to share the same network printers. This poses a problem with the district office's ability to adequately protect sensitive output production and distribution from non-authorized employees who have physical access to network printers. We also observed that cover pages are not used to

safeguard sensitive PTS data from viewing by unauthorized individuals when the output is printed on network printers. Cover pages could serve as a mitigating control to identify the owner of the printed output on shared printers.

NIST SP 800-53, "Recommended Security Controls" provides guidance for protecting sensitive information to prevent the unauthorized receipt of paper media. It cautions that entities should provide adequate supervision of personnel and develop detailed procedures to ensure that unauthorized individuals cannot read, copy, alter, or destroy information generated by the information system in printed form. Additionally, the guidance stresses assurances that "Output from the information system is given only to authorized users."

The Department's Order 2640.2E, "Access Control," requires that users only have access to information necessary to perform their duties and no more. Moreover, it requires that controls be in place to ensure that users can only access resources critical to the accomplishment of their duties.

OMB Circular A-130 also provides requirements for information safeguards. It states that information protected by the Privacy Act of 1974 should be collected, maintained, and protected to prevent disclosure of personal information and intrusion into the privacy of individuals. The Circular holds agencies responsible to see that appropriate information safeguards are instituted and that employees are trained in the protection of privacy.

By allowing authorized PTS users to print sensitive PTS output on network printers shared by non-authorized USMS employees, the USMS is neglecting critical physical security measures that protect against unauthorized access. This vulnerability poses a threat to the USMS's ability to comply with federal regulations that require protection of privacy information from unauthorized disclosure. It also undermines the USMS's efforts to effectively enforce appropriate access control and segregation of duties.

**Recommendation:**

We recommend the USMS:

17. Ensure that PTS output reports containing sensitive privacy information are protected from unauthorized persons.

**Controls Over Integrity of Processing and Data Files**

Controls over integrity of processing and data files are used to ensure that the current versions of production programs and data files are made available to users during system processing. These controls prevent users from accessing outdated versions of software that may be present in the production environment. Controls over integrity of processing and data files include:

- Procedures that ensure that the current version of production programs and data files are used during processing;
- Programs with routines that verify that the proper version of the computer file is used during processing;
- Programs with routines that check for internal file header labels before processing; and
- Mechanisms within the application that protect against concurrent file updates.

We found that procedures existed to ensure that the current versions of production programs, data files, and computer files are used during processing and that programs check internal file header labels before processing. However, we discovered the following deficiency in the control area indicated below:

**Controls Over Integrity of Processing and Data Files**

| CONTROL AREAS                                                                                               | VULNERABILITIES NOTED |
|-------------------------------------------------------------------------------------------------------------|-----------------------|
| Procedures ensure that the current version of production programs and data files are used during processing |                       |
| Programs include routines to verify that the proper version of the computer files is used during processing |                       |
| Programs include routines for checking internal file header labels before processing                        |                       |
| <b>Mechanisms within the application protect against concurrent file updates</b>                            | 0                     |

***Mechanisms Within the Application Protect Against Concurrent File Updates***

Our review of the PTS application disclosed deficiencies within the controls that prevent concurrent updates of files. According to USMS headquarters, the PTS application is distributed to each of the 94 DOs. USMS headquarters also asserted that system administrators at each site cannot modify the PTS’s functionality and that the application should

function uniformly. However, we discovered malfunctions with the controls built into the application to prevent concurrent file updates. We performed testing at all DO locations visited, and at four locations we observed that the controls against concurrent updates did not work consistently. PTS users were able to access the same prisoner record and make changes to the database simultaneously.

OMB Circular A-130 recommends that entities periodically review security controls and seek ways to improve security such as utilizing technical tools to look for security problems and installing the latest software patches. NIST SP 800-40 specifically addresses procedures for handling security patches and confirms that many organizations fail to keep software updated and patched. It warns that not patching information systems in a timely manner can impact operations and degrade the confidentiality, availability, and integrity of a system's information.

Weaknesses with controls that protect against the concurrent update of records within an application threaten the integrity of its data. When multiple users of the application can access the same prisoner record and make changes to the database simultaneously, there is no assurance that the information in the record is correct or that the application has processed the information properly.

It appears that this weakness occurred because the USMS did not ensure that all of its DOs received identical versions of the PTS application or that the existing versions were not patched in a timely manner. Specifically, USMS should confirm that the version of the PTS application in production at each site contains the full security controls, including those designed to prevent simultaneous updates to protect the integrity of data.

**Recommendation:**

We recommend the USMS:

18. Ensure that each installation of the application protects against simultaneous updates of the same record by more than one end-user.

**3. DATA INTEGRITY TESTING**

The goal of maintaining data integrity is the assurance that information processed by the computer is reasonably complete and accurate and meets the needs of the organization. Completeness and accuracy of information reflect how well data integrity is maintained.

- **Completeness of information.** This requires that the PTS records contain all necessary data elements and transactions are supported by source documents; and
- **Accuracy of information.** Information on the PTS output reports reflect the data entered into the PTS from source documents.

Our review of the factors that contribute to data integrity disclosed deficiencies within the areas indicated below:

### Data Integrity Assessment Factors

|                                                                                                    | VULNERABILITIES NOTED |
|----------------------------------------------------------------------------------------------------|-----------------------|
| <b>Completeness of Information</b>                                                                 |                       |
| <b>Records contain all of the data elements and documents used as support for the transactions</b> | 0                     |
| <b>Accuracy of Information</b>                                                                     |                       |
| <b>Output reports reflect the data obtained from the source documents</b>                          | 0                     |

#### **Completeness of Information**

Completeness is achieved when data elements are processed as intended and source documents are maintained to support the results of processing. We evaluated the completeness of prisoner file folders to determine if PTS data were properly authorized and supported by adequate and proper documentation. Our review for completeness of information focused on the existence of key source documents in prisoner records as discussed earlier in the authorization controls section of this report.

#### ***Records contain all of the data elements and documents used as support for the transactions***

We found that many of the prisoner file folders reviewed were missing information used to validate data entry transactions and to substantiate the actions taken by USMS personnel. This occurred because the USMS did not establish and implement standards regarding data collection and comply with federal records retention requirements.

The chart below details the number of occurrences for source document discrepancies found during the review of 25 records at each site, and the percentages were calculated against the total number of records (200) reviewed at all sites.

### PTS's Prisoner File Folder Completeness Analysis

| Sites Visited      | Missing Original USM-129 & 312 | Missing Photos | Missing Fingerprint Cards (FD-129) | Missing USM-552/553 (medical form) |
|--------------------|--------------------------------|----------------|------------------------------------|------------------------------------|
| E/VA               | 7                              | 3              | 1                                  | 2                                  |
| DC/DC              | 2                              | 5              | 2                                  | 22                                 |
| S/NY               | 2                              | 1              | 2                                  | 4                                  |
| E/PA               | 5                              | 10             | 1                                  | 24                                 |
| S/TX               | 7                              | 3              | 3                                  | 11                                 |
| N/IL               | 5                              | 0              | 0                                  | 24                                 |
| S/FL               | 1                              | 0              | 0                                  | 3                                  |
| D/AZ               | 9                              | 3              | 6                                  | 2                                  |
| <b>Totals:</b>     | <b>38</b>                      | <b>25</b>      | <b>15</b>                          | <b>92</b>                          |
| <b>Percentage:</b> | <b>19%</b>                     | <b>13%</b>     | <b>8%</b>                          | <b>46%</b>                         |

Source: The OIG's analysis of record completeness.

OMB Circular A-130 outlines an information management policy that includes records retention requirements and advises agencies to record sufficient information to ensure the management and accountability of its programs. Additionally, the guidance directs agencies to incorporate records management functions into a system's SDLC that include maintaining adequate and proper documentation of agency activities. Furthermore, OMB directs agencies to provide training and guidance to all employees regarding their records management responsibilities, especially with respect to maintaining adequate and proper documentation of program activities to protect the federal government's legal and financial interests.

Incomplete prisoner file folders pose a significant risk to the USMS's ability to validate PTS transactions, verify information, and justify the actions of its employees.

#### Recommendation:

We recommend the USMS:

19. Ensure that adequate and proper source documents are maintained in prisoner file folders to substantiate employee activities.

## **Accuracy of Information**

Information is considered accurate if the results of computer processing reflect the contents of source documents. Accuracy of information can be verified by the periodic spot-checking of system output reports to validate and confirm that the application has processed the data entered into it correctly.

### ***Output reports reflect the data obtained from the source documents***

System output is evidence of the results of the input and processing functions of an application and reflects the effectiveness of such operations. If reviewed, output reports help to maintain the accuracy and validity of data within a system and determine the completeness of processing. The USMS' form 129 (USM-129) is the PTS application's output report resulting from prisoner record creation and subsequent record updates.

After performing the analysis for the existence of key source documents used to create and update prisoner records, we reviewed the same prisoner file folders for accuracy of information. This review included the manual inspection of source documents contained in prisoner file folders. The source documents were then compared against the information appearing on the prisoner's USM-129 form (PTS's output report) to determine data accuracy.

Our review of output reports produced by the PTS application disclosed discrepancies in the accuracy of information. We found that prisoner identifying information, such as a prisoner's date of birth (DOB) and social security number (SSN), appearing on the PTS output reports did not always match the source documents contained in the prisoner's file folder. Additionally, critical dates, such as a prisoner's custody date, did not always correlate with dates on source documents in the prisoner file folders. Such dates are used by the USMS to calculate expenditures for reimbursements to contract jail facilities.

We noted common deficiencies in eight areas. These areas included:

- Incorrect DOB;
- Incorrect SSN;
- Misfiled documents;
- Concurrent jail days;
- Misnumbered file jackets (prisoner's file folder);
- Missing transactions;
- Wrong dates (such as custody and sentence dates); and
- No supporting documentation.

The chart below illustrates the results of our review of the PTS’s output reports. The numbers in each column represent the number of inaccuracies found during the review of 25 records at each site. The percentages were calculated against the total number of records (200) reviewed.

### Accuracy of PTS’s Output Reports

|                    | Incorrect DOB | Incorrect SSN | Misfiled Documents | Concurrent Jail Days | Misnumbered File Jackets | Missing Transactions | Wrong Dates | No Supporting Documentation |
|--------------------|---------------|---------------|--------------------|----------------------|--------------------------|----------------------|-------------|-----------------------------|
| E/VA               | 2             | 1             | 1                  | 1                    | 0                        | 7                    | 8           | 18                          |
| DC/DC              | 1             | 2             | 0                  | 1                    | 1                        | 7                    | 10          | 23                          |
| S/NY               | 0             | 0             | 0                  | 0                    | 0                        | 1                    | 8           | 5                           |
| E/PA               | 0             | 1             | 2                  | 0                    | 3                        | 0                    | 2           | 21                          |
| S/TX               | 4             | 0             | 0                  | 0                    | 3                        | 0                    | 12          | 20                          |
| N/IL               | 1             | 1             | 0                  | 0                    | 0                        | 0                    | 7           | 25                          |
| S/FL               | 0             | 1             | 0                  | 0                    | 5                        | 2                    | 7           | 24                          |
| D/AZ               | 1             | 0             | 1                  | 0                    | 0                        | 1                    | 1           | 15                          |
| <b>Total:</b>      | <b>9</b>      | <b>6</b>      | <b>4</b>           | <b>2</b>             | <b>12</b>                | <b>18</b>            | <b>55</b>   | <b>151</b>                  |
| <b>Percentage:</b> | <b>5%</b>     | <b>3%</b>     | <b>2%</b>          | <b>1%</b>            | <b>6%</b>                | <b>9%</b>            | <b>28%</b>  | <b>76%</b>                  |

Source: The OIG’s analysis of data accuracy.

**DOB and SSN information.** This information is used to distinguish between prisoners with identical names. We found instances where documents in the prisoners’ file folders did not match the DOB or SSN information appearing on the PTS’s USM-129 report.

**Misfiled documents.** We discovered documentation pertaining to one USMS prisoner erroneously filed inside another prisoner’s file folder. Prisoner file folders contain records of court proceedings such as writs,<sup>14</sup> judgment and commitment orders, and warrants that are used to initiate and substantiate updates to prisoner records. A document filed in the wrong prisoner’s file folder could delay or prevent the processing of a time-sensitive prisoner action such as a release, movement, or designation to a BOP facility.

**Concurrent jail days.** These represent instances where entries in the chronological prisoner history section of the USM-129 indicated that a prisoner was housed at two different jail facilities on the same dates. USMS uses the number of jail days to calculate monthly obligations to state and local contract jail facilities. Therefore, jail day discrepancies could negatively

<sup>14</sup> Writs are formal legal documents that order or prohibit some action. For example, a “Writ Ad Testificandum” is a legal document ordering a witness to testify in a court proceeding.

impact the accurate payment of bills causing the USMS to pay for contract jail services it did not receive.

**Misnumbered file jackets.** At one site visited, we experienced difficulty locating a prisoner's file folder because the USMS number on the file folder did not match the prisoner's USMS number. We also observed what appeared to be a re-constructed file folder because the prisoner's USM-129 showed substantial confinement history, but the file folder had little or no contents and was missing the minimal source documents such as photographs and fingerprint cards. An error of this nature could prevent USMS personnel from locating records in a timely manner or result in the need to "reconstruct" a prisoner file folder for the prisoner in custody.

**Missing transactions.** We identified occurrences where documentation existed in the prisoner's file folder that changed the prisoner's status, but the transaction was not entered into the PTS. Specifically, the prisoner's file folder contained documentation that would trigger an update action such as the receipt of a judgment and commitment order, but the appropriate transaction to update the record was not entered into the PTS (WT-J/C).<sup>15</sup> Again, this type of discrepancy could prevent or delay a time-sensitive transaction from being entered into the PTS.

**Wrong dates.** These were identified when comparing the PTS's system output (USM-129 report) with the agent's arrest form source document. Incorrect entries were identified for critical dates – the prisoner's arrest date and USMS custody date. Discrepancies with the prisoner's arrest date and USMS custody date directly affect the credit a prisoner receives for time served and also factor in the calculation for jail days used to reconcile jail bills and other expenditures.

**No supporting documentation.** At all sites visited, we found that prisoners' file folders were missing documents that were needed to substantiate record update actions taken by the USMS personnel. In these instances, we determined that documentation did not exist for many of the status code transactions and the majority of the facility history transactions that chronicled prisoner movements. Specifically, key documents, such as prisoner manifest forms, were not consistently maintained in the prisoner's

---

<sup>15</sup> The code "WT-J/C" is the status code for a sentenced prisoner for whom the district has not yet received the Judgment/Commitment (J&C) papers to confirm the sentence information. Upon receipt of the J&C, the district may send a request to BOP in order to determine which BOP facility the prisoner will serve the period of confinement.

file folder or filed in the DOs for longer than one year.<sup>16</sup> Other supporting documents, such as “requests for designation” or correspondence from the BOP that justified prisoner movements, were also not maintained in the prisoner file folders we reviewed.

We found a significant number of errors with respect to the accuracy of information on system output and with the completeness of prisoner file folders records. We attributed the existence of these conditions to the lack of policies and procedures to standardize the intake process, as well as the lack of supervisory review of data before it is entered into the PTS application.

### **Recommendation:**

We recommend that the USMS:

20. Ensure that data integrity assurances and quality control measures are developed and implemented to:
  - a) require the periodic spot-checking and validation of output from the PTS; and
  - b) confirm that the processing of information is correct.

## **III. CONCLUSION**

The weaknesses identified in our review of select general controls included problems with entity-wide security planning and management. We found that the USMS has not appointed a security manager for PTS and the organization did not ensure that employees receive specialized PTS training either before accessing the system or within a reasonable period thereafter. Weaknesses with segregation of duties occurred because the USMS has not developed and implemented formal operating policies and procedures to guide users in the performance of their duties. Furthermore, the organization has not developed policies to segregate incompatible duties.

We also found that PTS users were not familiar with the USMS’s application software development and change control procedures and that the USMS is using outdated programming and database management

---

<sup>16</sup> According to USMS Policy Directive No. 99-47, Cellblock Operations, prisoner manifest forms such as the USMS’ Form 40/41, “Prisoner Remand or Order to Deliver & Receipt for U.S. Prisoners,” are executed to reflect the transfer of custody during the release of prisoners to the temporary custody of law enforcement officers.

software to support the PTS, a mission-critical application. We determined that access controls were inadequate because the PTS authorized user list was not properly maintained and physical access controls designed to protect data terminals that process sensitive PTS information were not enforced.

Our review of the PTS's application controls disclosed that controls to properly authorize data and validate transactions were deficient. Specifically, we found that the USMS had not established proper authorization controls or standards for key source documents used to create prisoner records in the PTS. Additionally, supervisory reviews of source documents and transactions were not being performed on a consistent basis to mitigate this condition. We also discovered that audit logs used to recreate events and track user activity were not being kept. Problems with accuracy controls included weaknesses with erroneous data not being collected or reported back to management for investigation or correction. Furthermore, the USMS failed to control system output reports by allowing authorized PTS users to share printers with non-authorized USMS employees.

Deficiencies with completeness controls involved the USMS's failure to enforce its own policy that dictates that a prisoner may not have more than one USMS prisoner number. To complicate matters, the current PTS configuration does not provide for universal computer sequence checking to prevent the assignment of multiple USMS numbers to the same prisoner. In addition, we found that the application did not consistently enforce controls over integrity of processing and data files. We observed that the system allowed concurrent file updates when two users were able to update the same prisoner record at the same time.

Problems were identified with data integrity for the PTS application during our review of prisoner records for completeness and in our checks for accuracy of information contained in system output. We found that prisoner file folders were missing key source documents critical to the record creation process and that the proper documentation needed to substantiate actions taken by USMS personnel was not maintained in the folders.

We consider our findings in the areas of select general controls, application controls, and data integrity to be major weaknesses that pose a high risk to the protection of its data from unauthorized use, loss, or modification. We conclude that the weaknesses with select general controls and application controls occurred because the USMS did not enforce its own policies and did not comply with the Department's policies and procedures, NIST standards, and OMB guidelines. We further conclude that the

deficiencies with data integrity occurred because the USMS did not develop and implement formal policies and procedures to guide users in the performance of critical duties, such as creating and updating prisoner records in the PTS. As a result, we found errors and omissions on system output reports that we attributed to the lack of sufficient training and inconsistent practices.

The USMS's reliance on the data within the PTS with inaccurate information could result in over expenditures for reimbursable contracts with private jail facilities. Additionally, the untimely release of a prisoner or the misidentification of a prisoner requiring segregation or protection within the prisoner population also could occur. If not corrected, these weaknesses could impair the USMS's ability to ensure the integrity, confidentiality, and availability of data contained within the PTS.

## OBJECTIVES, SCOPE, AND METHODOLOGY

Our audit objectives were to review application controls, select general controls, and assess the reliability of the Prisoner Tracking System (PTS) data. The audit work, which occurred between June and December 2003, was performed in accordance with the Government Auditing Standards. We conducted fieldwork at the United States Marshals Service (USMS) headquarters in Arlington, Virginia, and 8 of the 94 USMS district offices (DOs). The eight DOs were: Alexandria, Virginia; Washington, D.C.; New York, New York; Houston, Texas; Philadelphia, Pennsylvania; Chicago, Illinois; Miami, Florida; and Phoenix, Arizona. The DOs were selected because their location, detainee processing volume, or USMS headquarters identified them as "model sites."

Although our primary objectives were to review application controls and perform data integrity testing, our audit criteria for evaluating application controls included certain select general control areas. Those steps involved obtaining an overview of the application's user population (access controls), developing an understanding of the operational workflow process (entity-wide security program planning and management and segregation of duties), and developing an understanding of the hardware and software environment (system software, application software development, and service continuity). Therefore, this report contains findings from select general control areas required to assess the effectiveness of PTS's application controls.

The Marshals Network (MNET) serves as the PTS's system environment because PTS users must login to MNET to gain access to PTS servers. The OIG performed an audit of MNET's general controls during its fiscal year 2003 Federal Information Security Management Act (FISMA) review. We therefore relied on audit findings disclosed during the FISMA review as an assessment of the PTS application's system environment and reported on those select general controls we reviewed as required by the application controls audit criteria.

To accomplish our audit objectives, we conducted over 50 interviews and visited the 8 DOs represented on the map in Appendix 2. We interviewed USMS headquarters officials from the Prisoner Services Division, Planning and Analysis Branch, and Information Technology Services Division to assess select general controls, such as entity-wide security program planning and management of the PTS and service continuity. From these interviews, we were able to gain an understanding of the application's user population, operational workflow process, and hardware and software

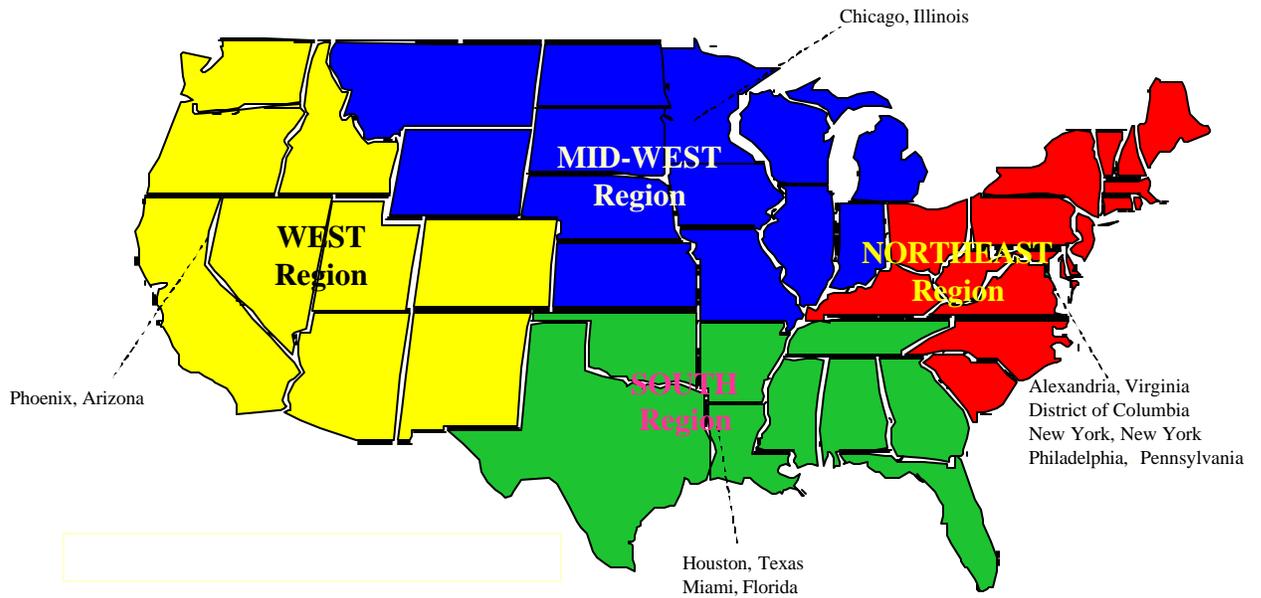
environment. Additionally, we obtained information from deputy marshals, administrative officers, criminal clerks, detention enforcement officers, and system administrators at each DO visited to evaluate the overall effectiveness of application controls for protecting the PTS's data. We specifically reviewed authorization, completeness, accuracy, and integrity of processing controls.

Our visits to the selected DOs included observing operational activities and performing data integrity testing. Our observation of operational activities allowed us to assess the USMS's compliance with the Federal Information System Controls Audit Manual (FISCAM), USMS's PTS User Manual, and USMS's Policy Directive No. 99-47 (Cellblock Operations). To perform data integrity testing, we judgmentally selected a total of 200 prisoners' file folders (25 file folders at each of the 8 sites visited). We reviewed these prisoners' records for completeness of information and manually compared source documents to the PTS output to determine accuracy of information as recommended in the General Accounting Office's (GAO) guidance for Assessing the Reliability of Computer-Processed Data.

Additionally, we reviewed the certification and accreditation documentation for the PTS, the Department's information technology management policies and procedures, the USMS's organizational structures, and information contained within individual prisoner file folders.

FIELDWORK SITE VISIT MAP

District Offices Visited Representing  
United States Marshals Service Regions



## FEDERAL INFORMATION SYSTEM CONTROLS AUDIT MANUAL

## SELECT GENERAL CONTROLS

| CONTROL AREAS                                                                                       | VULNERABILITIES NOTED |
|-----------------------------------------------------------------------------------------------------|-----------------------|
| <b>Entity-wide Security Program Planning &amp; Management</b>                                       |                       |
| Assess risks periodically                                                                           |                       |
| Document an entity-wide security program plan                                                       |                       |
| Establish a security management structure and clearly assign security responsibilities              | Ö                     |
| Implement effective security-related personnel policies                                             | Ö                     |
| Monitor the security program's effectiveness and make changes as needed                             |                       |
| <b>Access Controls</b>                                                                              |                       |
| Classify information resources according to their criticality and sensitivity                       |                       |
| Maintain a current list of authorized users and ensure that their access is authorized              | Ö                     |
| Establish physical and logical controls to prevent and detect unauthorized access                   | Ö                     |
| Monitor access, investigate apparent security violations, and take appropriate remedial action      |                       |
| <b>Application Software Development &amp; Change Control</b>                                        |                       |
| Authorize processing features and modifications                                                     | Ö                     |
| Test and approve all new and revised software                                                       |                       |
| Control software libraries                                                                          |                       |
| <b>System Software</b>                                                                              |                       |
| Limit access to system software                                                                     |                       |
| Monitor access to and use of system software                                                        |                       |
| Control system software changes                                                                     | Ö                     |
| <b>Segregation of Duties</b>                                                                        |                       |
| Segregate incompatible duties and establish related policies                                        | Ö                     |
| Establish access controls to enforce segregation of duties                                          |                       |
| Control personnel activities through formal operating procedures and supervision and review         | Ö                     |
| <b>Service Continuity</b>                                                                           |                       |
| Assess the criticality and sensitivity of computerized operations and identify supporting resources | Ö                     |
| Take steps to prevent and minimize potential damage and interruption                                | Ö                     |
| Develop and document a comprehensive contingency plan                                               |                       |
| Test the contingency plan periodically and adjust it as appropriate                                 | Ö                     |

# FEDERAL INFORMATION SYSTEM CONTROLS AUDIT MANUAL

## APPLICATION CONTROLS

| CONTROL AREAS                                                                                               | VULNERABILITIES NOTED |
|-------------------------------------------------------------------------------------------------------------|-----------------------|
| <b>Authorization Controls</b>                                                                               |                       |
| All data are authorized before entering the application system                                              | 0                     |
| Restrict data entry terminals to authorized users for authorized purposes                                   | 0                     |
| Master files and exception reporting help ensure all data are processed and are authorized                  |                       |
| <b>Completeness Controls</b>                                                                                |                       |
| All authorized transactions are entered into and processed by the computer                                  | 0                     |
| Reconciliations are performed to verify data completeness                                                   |                       |
| <b>Accuracy Controls</b>                                                                                    |                       |
| 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                                          | 0                     |
| Output reports are reviewed to help maintain data accuracy and validity                                     | 0                     |
| <b>Controls Over Integrity of Processing and Data Files</b>                                                 |                       |
| Procedures ensure that the current version of production programs and data files are used during processing |                       |
| Programs include routines to verify that the proper version of the computer files is used during processing |                       |
| Programs include routines for checking internal file header labels before processing                        |                       |
| Mechanisms within the application protect against concurrent file updates                                   | 0                     |

**GENERAL ACCOUNTING OFFICE  
ASSESSING THE RELIABILITY OF COMPUTER-PROCESSED DATA**

**DATA INTEGRITY ASSESSMENT FACTORS**

|                                                                                   | <b>VULNERABILITIES NOTED</b> |
|-----------------------------------------------------------------------------------|------------------------------|
| <b>Completeness of Information</b>                                                |                              |
| Contain all of the data elements and records used as support for the transactions | 0                            |
| <b>Accuracy of Information</b>                                                    |                              |
| Reflect the data obtained from the source documents                               | 0                            |

**GENERAL ACCOUNTING OFFICE  
FEDERAL INFORMATION SYSTEM CONTROLS AUDIT MANUAL**

**GENERAL CONTROLS REVIEW GUIDELINES**

The general controls guidelines used for this audit were obtained from Chapter 3, "Evaluating and Testing General Controls," of the GAO's FISCAM. The information below represents only those sections from the FISCAM that serve as the basis for the vulnerabilities identified during our review of the Prisoner Tracking System.<sup>17</sup>

### **3.0 OVERVIEW**

General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. They create the environment in which application systems and controls operate. During a financial statement audit, the auditor will focus on general controls that normally pertain to an entity's major computer facilities and systems supporting a number of different applications, such as major data processing installations or local area networks. If general controls are weak, they severely diminish the reliability of controls associated with individual applications. For this reason, general controls are usually evaluated separately from and prior to evaluating application controls.

There are six major categories of general controls that the auditor should consider. These are:

- **entity-wide security program planning and management** that provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls;
- **access controls** that limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure;
- **application software development and change controls** that prevent unauthorized programs or modifications to an existing program from being implemented;

---

<sup>17</sup> The areas from the FISCAM selected for inclusion in this report have been paraphrased.

- **system software** controls that limit and monitor access to the powerful programs and sensitive files that (1) control the computer hardware, and (2) secure applications supported by the system;
- **segregation of duties** that are policies, procedures, and an organizational structure established so that one individual cannot control key aspects of computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to assets or records; and
- **service continuity** controls to ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed, and critical and sensitive data are protected.

For each of these six categories, the manual identifies several critical elements that represent tasks that are essential for establishing adequate controls. For each critical element, there is a discussion of the associated objectives, risks, and critical activities, as well as related control techniques and audit concerns. The auditor can use this information to evaluate entity practices.

### **3.1 ENTITY-WIDE SECURITY PROGRAM PLANNING AND MANAGEMENT (SP)**

An entity-wide program for security planning and management is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

## **CRITICAL ELEMENTS**

- SP-1 Assess risks periodically
- SP-2 Document an entity-wide security program plan
- SP-3 Establish a security management structure and clearly assign security responsibilities
- SP-4 Implement effective security-related personnel policies
- SP-5 Monitor the security program's effectiveness and make changes as needed

### **Critical Element SP-3: Establish a security management structure and clearly assign security responsibilities**

Senior management should establish a structure to implement the security program throughout the entity. The structure generally consists of a core of personnel who are designated as security managers. These personnel play a key role in developing, communicating, and monitoring compliance with security policies and reporting on these activities to senior management. The security management function also serves as a focal point for others who plan a role in evaluating the appropriateness and effectiveness of computer-related controls on a day-to-day basis. These include program managers who rely on the entity's computer systems, system administrators, and system users.

#### **SP-3.1: A security management structure has been established**

The effectiveness of the security program is affected by the way in which responsibility for overseeing its implementation is assigned. Generally, such responsibility is assigned to a central security program office.

Responsibilities of the central security program office may include:

- facilitating risk assessments,
- coordinating the development of and distributing security policies and procedures,
- routinely monitoring compliance with these policies,
- promoting security awareness among system users,
- providing reports to senior management on policy and control evaluation results and giving advice to senior management on security policy-related issues; and
- representing the entity in the security community.

### **SP-3.2: Information security responsibilities are clearly assigned**

OMB Circular A-130, Appendix III, requires that the rules of the system and application “shall clearly delineate responsibilities and expected behavior of all individuals with access . . . and shall be clear about the consequences of behavior not consistent with the rules.” Security-related responsibilities of offices and individuals throughout the entity that should be clearly defined include those of (1) information resource owners and users, (2) information resources management and data processing personnel, (3) senior management, and (4) security administrators. Further, responsibilities for individual employee accountability regarding the use and disclosure of information resources should be established.”

|                                                                                       |
|---------------------------------------------------------------------------------------|
| <b>Critical Element SP-4: Implement effective security-related personnel policies</b> |
|---------------------------------------------------------------------------------------|

Policies related to personnel actions, such as hiring and termination, and employee expertise are important factors for information security. If personnel policies are not adequate, an entity runs the risk of (1) hiring unqualified or untrustworthy individuals, (2) providing terminated employees opportunities to sabotage or otherwise impair entity operations or assets, (3) failing to detect continuing unauthorized employee actions, (4) lowering employee morale, which may in turn diminish employee compliance with controls, and (5) allowing staff expertise to decline.

### **SP-4.2: Employees have adequate training and expertise**

Management should ensure that employees – including data owners, system users, data processing personnel, and security management personnel – have the expertise to carry out their information security responsibilities. To accomplish this, the security program should include:

- job descriptions that include the education, experience, and expertise needed;
- periodic reassessment of the adequacy of employees’ skills;
- annual training requirements and professional development programs to help make certain employees’ skills, especially technical skills, are adequate and current; and
- monitoring employee training and professional development accomplishments.

### 3.2 ACCESS CONTROLS (AC)

Access controls should provide reasonable assurance that computer resources (data files, application programs, and computer-related facilities and equipment) are protected against unauthorized modification, disclosure, loss, or impairment. Such controls include physical controls, such as keeping computers in locked rooms to limit physical access, and logical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files.

Inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data. The following examples illustrate the potential consequences of such vulnerabilities.

- By obtaining direct access to data files, an individual could make unauthorized changes for personal gain or obtain sensitive information. For example, a person could (1) alter the address of a payee and thereby direct a disbursement to himself or herself, (2) alter inventory quantities to conceal a theft of assets, (3) inadvertently or purposefully change a receivable balance, or (4) obtain confidential information about business transactions or individuals.
- By obtaining access to application programs used to process transactions, an individual could make unauthorized changes to these programs or introduce malicious programs, which in turn could be used to access data files, resulting in situations similar to those described above, or to process unauthorized transactions. For example, a person could alter a payroll or payables program to inappropriately generate a check for himself or herself.
- By obtaining access to computer facilities and equipment, an individual could (1) obtain access to terminals or telecommunications equipment that provide input into the computer, (2) obtain access to confidential or sensitive information on magnetic or printed media, (3) substitute unauthorized data or programs, or (4) steal or inflict malicious damage on computer equipment and software.

## **CRITICAL ELEMENTS**

- AC-1 Classify information resources according to their criticality and sensitivity
- AC-2 Maintain a current list of authorized users and ensure that their access is authorized
- AC-3 Establish physical and logical controls to prevent and detect unauthorized access
- AC-4 Monitor access, investigate apparent security violations, and take appropriate remedial action

### **Critical Element AC-2: Maintain a current list of authorized users and ensure that their access is authorized**

An entity should institute policies and procedures for authorizing access to information resources and documenting such authorizations. These policies and procedures should cover user access needed for routine operations, emergency access, and the sharing and disposition of data with individuals or groups outside the entity.

#### **AC-2.1: Resource owners have identified authorized users and their access authorized**

The computer resource owner should identify the specific user or class of users that are authorized to obtain direct access to each resource for which he or she is responsible. This process can be simplified by developing standard profiles, which describe access needs for groups of users with similar duties, such as accounts payable clerks.

Access may be permitted at a file, record, or field level. Files are composed of records, typically one for each item or transaction. Individual records are composed of fields that contain specific data elements relating to each record. Access authorizations should be documented on standard forms, maintained on file, approved by senior managers, and securely transferred to security managers. Owners should periodically review access authorization listings and determine whether they remain appropriate.

Listings of authorized users and their specific access needs and any modifications should be approved by an appropriate senior manager and

directly communicated in writing by the resource owner to the security management function.

It is equally important to notify the security management function immediately when an employee is terminated or, for some other reason, is no longer authorized access to information resources.

**Critical Element AC-3: Establish physical and logical controls to prevent and detect unauthorized access**

The entity should have a cost-effective process for protecting data files, application programs, and hardware through a combination of physical and logical security controls. Physical security involves restricting physical access to computer resources, usually by limiting access to the buildings and rooms where they are housed, or by installing locks on computer terminals. However, physical controls alone cannot ensure that programs and data are protected. For this reason, it is important to establish logical security controls that protect the integrity and confidentiality of sensitive files. The security function should be responsible for implementing and maintaining both physical and logical controls based upon authorizations provided by the owners of the resources.

**AC-3.1: Adequate physical security controls have been implemented**

Physical security controls restrict physical access to computer resources and protect them from intentional or unintentional loss or impairment.

In evaluating the effectiveness of physical security controls, the auditor should consider the effectiveness of the entity's policies and practices for:

- granting and discontinuing access authorizations,
- controlling passkeys,
- controlling entry during and after normal business hours,
- controlling the deposit and withdrawal of tapes and other storage media to and from the library,
- handling emergencies,
- controlling reentry after emergencies; and
- establishing compensatory controls when restricting physical access is not feasible, as is often the case with telecommunications lines.

### 3.3 APPLICATION SOFTWARE DEVELOPMENT AND CHANGE CONTROL (CC)

Application software is designed to support a specific operation, such as payroll or loan accounting. Typically several applications may operate under one set of operating system software. Controls over operating system software are discussed in Section 3.4.

Establishing controls over the modifications of application software programs helps to ensure that only authorized programs and authorized modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure all programs and program modifications are properly authorized, tested, and approved; and that access to and distribution of programs is carefully controlled. Without proper controls, there is a risk that security features could be inadvertently or deliberately omitted or "turned off" or that processing irregularities or malicious code could be introduced. For example,

- a knowledgeable programmer could surreptitiously modify program code to provide a means of bypassing controls to gain access to sensitive data;
- the wrong version of a program could be implemented, thereby perpetuating outdated or erroneous processing that is assumed to have been updated; or
- a virus could be introduced, inadvertently or on purpose, that disrupts processing.

#### **CRITICAL ELEMENTS**

CC-1 Authorize processing features and modifications  
CC-2 Test and approve all new and revised software  
CC-3 Control software libraries

#### **Critical Element CC-1: Authorize processing features and modifications**

The processing features built into application software should be authorized by the managers responsible for the agency program or operations that the application supports. This is because these are the managers responsible for seeing that software supporting their operations meets their needs and

produces reliable data and that the operations are carried out in accordance with applicable laws, regulations, and management policies. For example, the processing features associated with loan accounting software should be authorized by the loan program managers. Such user or owner authorization is needed when new systems are being developed, as well as when operational systems are being modified.

Authorization is the first step in implementing the features or the changes that have been decided on by the users, and the entity should have a process for obtaining, documenting, and communicating such authorizations as part of its system development life cycle (SDLC) methodology. If authorization procedures have not been developed or are not followed, an individual might be able to initiate program changes that result in erroneous processing or weakened access controls or edits built into the software.

### **CC-1.2: Authorizations for software modifications are documented and maintained**

Policies and procedures should be in place that detail who can authorize a modification and how these authorizations are to be documented. Generally the application users have the primary responsibility for authorizing systems changes. However, users should be required to discuss their proposed changes with systems developers to confirm that the change is feasible and cost effective. For this reason, an entity may require a senior systems developer to co-authorize a change.

The use of standardized change request forms helps ensure that requests are clearly communicated and that approvals are documented. Authorization documentation should be maintained for at least as long as a system is in operation in case questions arise regarding why or when system modifications were made. Authorization documents may be maintained in either paper or electronic form as long as their integrity is protected.

## **3.4 SYSTEM SOFTWARE (SS)**

System software is a set of programs designed to operate and control the processing activities of computer equipment. Generally, one set of system software is used to support and control a variety of applications that may run on the same computer hardware. System software helps control and coordinate the input, processing, output, and data storage associated with all of the applications that run on a system. Some system software can

change data and program code on files without leaving an audit trail. The following are examples of system software:

- operating system,
- system utilities,
- program library,
- file maintenance,
- security,
- data communications systems; and
- database management systems.

Controls over access to and modification of system software are essential in providing reasonable assurance that operating system-based security controls are not compromised and that the system will not be impaired. Inadequate controls in this area could lead to unauthorized individuals using system software to circumvent security controls to read, modify, or delete critical or sensitive information and programs; authorized users of the system gaining unauthorized privileges to conduct unauthorized actions; and/or systems software being used to circumvent edits and other controls built into application programs. Such weaknesses seriously diminish the reliability of information produced by all of the applications supported by the computer system and increase the risk of fraud and sabotage. System software programmers are often more technically qualified than other data processing personnel and, thus, have a greater ability to perform unauthorized actions if controls in this area are weak.

### **CRITICAL ELEMENTS**

- SS-1 Limit access to system software
- SS-2 Monitor access to and use of system software
- SS-3 Control system software changes

### **Critical Element SS-3: Control system software changes**

Modifications to system software should be controlled so that only authorized and properly tested changes are implemented. If system software is not adequately controlled and tested, system parameters may be inadequate to prevent unauthorized changes to application programs or data. Furthermore, software malfunctions during processing runs could result in inaccurate or incomplete financial data. Controls should provide that all

changes are tested and approved and that only approved system software is implemented.

### **SS-3.2: Installation of system software is documented and reviewed**

When possible, the installation of system software changes and new versions or products should be scheduled to minimize the impact on data processing operations, and an advance notice should be provided to system software users. The actual installation should be logged to establish an audit trail and reviewed by data center management. The migration of system software from the testing environment to the production environment should be done, after approval, by an independent library control group. Outdated versions of system software should be removed from the production environment to preclude their future use. Some changes may be made specifically to correct security or integrity vulnerabilities, while using outdated versions allows the entity's data and systems to remain exposed to these vulnerabilities.

All vendor-supplied system software should be supported by the vendor. Vendors often release new versions of system software products and may discontinue support of earlier versions. Enhancements and corrections made to subsequent versions of system software will not be available to entities that forgo acquiring the latest version. All system software should have current and complete documentation. Inadequate documentation will hinder maintenance activities, particularly during emergency situations when in-house systems programmers are attempting to restart a failed system and vendor assistance is not readily available.

### **3.5 SEGREGATION OF DUTIES (SD)**

Work responsibilities should be segregated so that one individual does not control all critical stages of a process. For example, while users may authorize program changes, programmers should not be allowed to do so because they are not the owners of the system and do not have the responsibility to see that the system meets user needs. Similarly, one computer programmer should not be allowed to independently write, test, and approve program changes. Often, segregation of duties is achieved by splitting responsibilities between two or more organizational groups. Dividing duties among two or more individuals or groups diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one group or individual will serve as a check on the activities of the other.

## **CRITICAL ELEMENTS**

- SD-1 Segregate incompatible duties and establish related policies
- SD-2 Establish access controls to enforce segregation of duties
- SD-3 Control personnel activities through formal operating procedures and supervision and review

### **Critical Element SD-1: Segregate incompatible duties and establish related policies**

The first steps in determining if duties are appropriately segregated are to analyze the entity's operations, identify incompatible duties, and assign these duties to different organizational units or individuals. Federal internal control standards specify that key duties and responsibilities for authorizing, processing, recording, and reviewing transactions should be separated. This concept can also be applied to the authorization, testing, and review of computer program changes.

Segregating duties begins by establishing independent organizational groups with defined functions, such as a payroll unit responsible for preparing payroll transaction input and a data processing unit responsible for processing input prepared by other units. Functions and related tasks performed by each unit should be documented for the unit and in staff job descriptions and should be clearly communicated to personnel assigned the responsibilities.

#### **SD-1.1: Incompatible duties have been identified and policies implemented to segregate these duties**

Management should have analyzed operations and identified incompatible duties that are then segregated through policies and organizational divisions. Although incompatible duties may vary from one entity to another, the following functions are generally performed by different individuals: Information Systems (IS) management, systems design, application programming, systems programming, quality assurance/testing, library management/change management, computer operations, production control and scheduling, data security, data administration, and network administration.

The following include examples of restrictions that are generally addressed in policies about segregating duties and are achieved through organizational divisions and access controls.

- Application users should not have access to operating system or application software.
- Programmers should not be responsible for moving programs into production or have access to production libraries or data.
- Access to operating system documentation should be restricted to authorized systems programming personnel.
- Access to application system documentation should be restricted to authorized applications programming personnel.
- Access to production software libraries should be restricted to library management personnel.
- Persons other than computer operators should not set up or operate the production computer.
- Only users, not computer staff, should be responsible for transaction origination or correction and for initiating changes to application files.
- Computer operators should not have access to program libraries or data files.

Some steps involved in processing a transaction also need to be separated among different individuals. For example, the following combinations of functions should not be performed by a single individual.

- Data entry and verification of data,
- Data entry and its reconciliation to output,
- Input of transactions for incompatible processing functions (e.g., input of vendor invoices and purchasing and receiving information); and
- Data entry and supervisory authorization functions (e.g., authorizing a rejected transaction to continue processing that exceeds some limit requiring a supervisor's review and approval).

Organizations with limited resources to segregate duties should have compensating controls, such as supervisory review of transactions performed.

|                                                                                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Critical Element SD-3: Control personnel activities through formal operating procedures and supervision and review</b></p> |
|----------------------------------------------------------------------------------------------------------------------------------|

Control over personnel activities requires formal operating procedures and active supervision and review of these activities. This is especially relevant

for computer operators. Inadequacies in this area could allow mistakes to occur and go undetected, and facilitate unauthorized use of the computer.

### **SD-3.1: Formal procedures guide personnel in performing their duties**

Detailed, written instructions should exist and be followed to guide personnel in performing their duties. These instructions are especially important for computer operators. For example, computer operator instruction manuals should provide guidance on system startup and shut down procedures, emergency procedures, system and job status reporting, and operator prohibited activities. Application-specific manuals (commonly called "run" manuals) should provide additional instructions for operators specific to each application, such as instructions on job setup, console and error messages, job checkpoints, and restart and recovery steps after system failures. Operators should be prevented from overriding file label or equipment error messages.

### **SD-3.2: Active supervision and review are provided for all personnel**

Supervision and review of personnel activities help make certain that these activities are performed in accordance with prescribed procedures, that mistakes are corrected, and that the computer is used only for authorized purposes. To aid in this oversight, all computer operator activities on the computer system should be recorded on an automated history log, which serves as an audit trail. Supervisors should routinely review this history log and investigate any abnormalities.

## **3.6 SERVICE CONTINUITY (SC)**

Losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an agency's ability to accomplish its mission. For this reason, an agency should have (1) procedures in place to protect information resources and minimize the risk of unplanned interruptions and (2) a plan to recover critical operations should interruptions occur. These plans should consider the activities performed at general support facilities, such as data processing centers and telecommunications facilities, as well as the activities performed by users of specific applications. To determine whether recovery plans will work as intended, they should be tested periodically in disaster simulation exercises.

To mitigate service interruptions, it is essential that the related controls be understood and supported by management and staff throughout the organization. Senior management commitment is especially important to

ensure that adequate resources are devoted to emergency planning, training, and related testing. In addition, all staff with service continuity responsibilities, such as staff responsible for backing up files, should be fully aware of the risks of not fulfilling these duties.

### **CRITICAL ELEMENTS**

- SC-1 Assess the criticality and sensitivity of computerized operations and identify supporting resources
- SC-2 Take steps to prevent and minimize potential damage and interruption
- SC-3 Develop and document a comprehensive contingency plan
- SC-4 Test the contingency plan periodically and adjust it as appropriate

### **Critical Element SC-1: Assess the criticality and sensitivity of computerized operations and identify supporting resources**

At most entities, the continuity of certain automated operations is more important than others, and it is not cost-effective to provide the same level of continuity for all operations. For this reason, it is important that management analyze data and operations to determine which are the most critical and what resources are needed to recover and support them. This is the first step in determining which resources merit the greatest protection and what contingency plans need to be made.

#### **SC-1.2: Resources supporting critical operations are identified**

Once critical data and operations have been determined, the minimum resources needed to support them should be identified and their role analyzed. The resources considered include computer resources, such as computer hardware, software, and data files; computer supplies, including paper stock and preprinted forms; telecommunications services; and any other resources that are necessary to the operation, such as people, office facilities and supplies, and noncomputerized records. For example, an analysis should be performed to identify the maximum number of disk drives needed at one time and the specific requirements for telecommunications lines and devices.

Because essential resources are likely to be held or managed by a variety of groups within an organization, it is important that program and information

security (IS) support staff work together to identify the resources for critical operations.

**Critical Element SC-2: Take steps to prevent and minimize potential damage and interruption**

There are a number of steps that an organization should take to prevent or minimize the damage to automated operations that can occur from unexpected events. These can be categorized as follows:

- routinely duplicating or backing up data files, computer programs, and critical documents with off-site storage;
- installing environmental controls, such as fire suppression systems or backup power supplies;
- arranging for remote backup facilities that can be used if the entity's usual facilities are damaged beyond use; and
- ensuring that staff and other users of the system understand their responsibilities in case of emergencies.

Taking such steps, especially implementing thorough backup procedures and installing environmental controls, are generally inexpensive ways to prevent relatively minor problems from becoming costly disasters. In particular, an entity should maintain an ability to restore data files, which may be impossible to recreate if lost. In addition, effective maintenance, problem management, and change management for hardware equipment will help prevent unexpected interruptions.

**SC-2.1: Data and program backup procedures have been implemented**

Routinely copying data files and software and securely storing these files at a remote location are usually the most cost-effective actions that an entity can take to mitigate service interruptions. Although equipment can often be readily replaced, the cost could be significant, and reconstructing computerized data files and replacing software can be extremely costly and time-consuming. Sometimes, reconstruction of data files may be virtually impossible. In addition to the direct costs of reconstructing files and obtaining software, the related service interruptions could lead to significant financial losses.

A program should be in place for regularly backing up computer files, including master files, transaction files, application programs, systems software, and database software, and storing these backup copies securely

at an off-site location. Although choosing a backup storage location is a matter of judgment, the backup location should be far enough away from the primary location that it will not be impaired by the same events, such as fires, storms, and electrical power outages. In addition, it should be protected from unauthorized access and from environmental hazards, such as fires and power outages.

### **SC-2.3: Staff have been trained to respond to emergencies**

Staff should be trained in and aware of their responsibilities in preventing, mitigating, and responding to emergency situations. For example, data center staff should receive periodic training in emergency fire, water, and alarm incident procedures as well as their responsibilities in starting up and running an alternate data processing site. Also, if outside users are critical to the entity's operations, they should be informed of the steps they may have to take as a result of an emergency.

Generally, information on emergency procedures and responsibilities can be provided through training sessions and by distributing written policies and procedures. Training sessions should be held at least once a year and whenever changes to emergency plans are made.

Also, if staff could be required to relocate or significantly alter their commuting routine in order to operate an alternate site in an emergency, it is advisable for an entity to incorporate into the contingency plan steps for arranging lodging and meals or any other facilities or services that may be needed to accommodate the essential human resources.

|                                                                                                   |
|---------------------------------------------------------------------------------------------------|
| <b>Critical Element SC-4: Periodically test the contingency plan and adjust it as appropriate</b> |
|---------------------------------------------------------------------------------------------------|

Testing contingency plans is essential to determine whether they will function as intended in an emergency situation. According to OMB, federal managers have reported that testing revealed important weaknesses in their plans, such as backup facilities that could not adequately replicate critical operations as anticipated. Through the testing process, these plans were substantially improved.

The most useful tests involve simulating a disaster situation to test overall service continuity. Such a test would include testing whether the alternative data processing site will function as intended and whether critical computer data and programs recovered from off-site storage are accessible and current. In executing the plan, managers will be able to identify weaknesses

and make changes accordingly. Moreover, tests will assess how well employees have been trained to carry out their roles and responsibilities in a disaster situation.

#### **SC-4.1: The plan is periodically tested**

The frequency of contingency plan testing will vary depending on the criticality of the entity's operations. Generally, contingency plans for very critical functions 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 people has occurred. It is important for top management to assess the risk of contingency plan problems and develop and document a policy on the frequency and extent of such testing.

**GENERAL ACCOUNTING OFFICE  
FEDERAL INFORMATION SYSTEM CONTROLS AUDIT MANUAL**

**APPLICATION CONTROLS REVIEW GUIDELINES**

The general controls guidelines used for this audit were obtained from Chapter 4, "Evaluating and Testing Application Controls," of the GAO's FISCAM. The information below represents only those sections from the FISCAM that serve as the basis for the vulnerabilities identified during our review of the Prisoner Tracking System.<sup>18</sup>

**4.0 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.

---

<sup>18</sup> The areas from the FISCAM selected for inclusion in this report have been paraphrased.

Some guides provide additional categories of application controls. For example, data origination is a breakout of input 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 Financial Audit Manual. 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** – This is most closely aligned with the financial statement accounting assertion of existence or occurrence. This assertion, in part, concerns the validity of transactions and ensures that they represent economic events that actually occurred during a given period.
- **Completeness controls** – This directly relates to the financial statement accounting assertion on completeness, which deals with whether all valid transactions are recorded and properly classified.
- **Accuracy controls** – This most directly 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** – These controls, 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.

## 4.1 AUTHORIZATION CONTROLS (AN)

Only authorized transactions should be entered into the application system and processed by the computer.

### **Critical Elements**

- AN-1 All data are authorized before entering the application system
- AN-2 Restrict data entry terminals to authorized users for authorized purposes
- AN-3 Master files and exception reporting help ensure all data are processed and are authorized

### **Critical Element AN-1: All data are authorized before entering the application system**

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.

#### **AN-1.1 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.

**AN-1.2 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 by supervisory personnel. After verifying the input transactions, the control unit or supervisory personnel enter the required authorization and release the data for further processing.

**Critical Element AN-2: Restrict data entry terminals to authorized users for authorized purposes**

The integrity of application data can be compromised by 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. 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.

## **AN-2.1 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, for example, 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.

## **4.2 COMPLETENESS CONTROLS (CP)**

All authorized transactions should be entered into and completely processed by the computer.

### **Critical Elements**

- CP-1 All authorized transactions are entered into and processed by the computer
- CP-2 Reconciliations are performed to verify data completeness

**Critical Element CP-1: All authorized transactions are entered into and processed by the computer**

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.

**CP-1.2 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 those 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.

### 4.3 ACCURACY CONTROLS (AY)

The recording of valid and accurate data into an application system is essential to provide for an effective system that produces reliable results.

#### **CRITICAL ELEMENTS**

- AY-1 Data entry design features contribute to data accuracy
- AY-2 Data validation and editing are performed to identify erroneous data
- AY-3 Erroneous data are captured, reported, investigated, and corrected
- AY-4 Output reports are reviewed to help maintain data accuracy and validity

#### **Critical Element AY-3: Erroneous data are captured, reported, investigated, and corrected**

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.

#### **AY-3.2 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 the systems allow 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.

**Critical Element AY-4: Output reports are reviewed to help maintain data accuracy and validity**

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 user department personnel.

**AY-4.1 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.

#### **4.4 CONTROLS OVER INTEGRITY OF PROCESSING AND DATA FILES**

##### **Examples 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.

**GENERAL ACCOUNTING OFFICE  
ASSESSING THE RELIABILITY OF COMPUTER-PROCESSED DATA  
DATA INTEGRITY ASSESSMENT GUIDELINES**

Data reliability refers to the accuracy and completeness of computer-processed data, given the intended purposes for use. Computer-processed data include data (1) entered into a computer system and (2) resulting from computer processing. Computer-processed data can vary in form – from electronic files to tables in published reports. The definition of computer-processed data is therefore broad. In this guidance, the term data always refers to computer-processed data.

The “Yellow Book” requires that a data reliability assessment be performed for all data used as support for engagement findings, conclusions, or recommendations.<sup>19</sup> This guidance will help you to design a data reliability assessment appropriate for the purposes of the engagement and then to evaluate the results of the assessment.

Data are reliable when they are (1) complete (they contain all of the data elements and records needed for the engagement) and (2) accurate (they reflect the data entered at the source or, if available, in the source documents).<sup>20, 21</sup> A subcategory of accuracy is consistency. Consistency refers to the need to obtain and use data that are clear and well-defined enough to yield similar results in similar analyses. For example, if data are entered at multiple sites, inconsistent interpretation of data rules can lead to data that, taken as a whole, are unreliable. Reliability also means that for any computer processing of the data elements used, the results are reasonably complete and accurate, meet your intended purposes, and are not subject to inappropriate alteration.

---

<sup>19</sup> The GAO’s “Government Auditing Standards,” 2003 Revision, commonly referred to as the “Yellow Book” sets forth generally accepted government auditing standards for use by government auditors.

<sup>20</sup> A data element is a unit of information with definable parameters (for example, a social security number), sometimes referred to as a *data variable* or *data field*.

<sup>21</sup> Source document. Information that is the basis for entry of data into a computer.

## ACRONYMS AND ABBREVIATIONS

|                    |                                                          |
|--------------------|----------------------------------------------------------|
| <b>ABS</b>         | Automated Booking Station                                |
| <b>BOP</b>         | Federal Bureau of Prisons                                |
| <b>CSSO</b>        | Computer Systems Security Officer                        |
| <b>D/AZ</b>        | District of Arizona                                      |
| <b>DBMS</b>        | Database Management System                               |
| <b>DC/DC</b>       | District Court for the District of Columbia              |
| <b>Department</b>  | Department of Justice                                    |
| <b>DO</b>          | District Office                                          |
| <b>DOB</b>         | Date of Birth                                            |
| <b>E/PA</b>        | Eastern District of Pennsylvania                         |
| <b>E/VA</b>        | Eastern District of Virginia                             |
| <b>FBI</b>         | Federal Bureau of Investigation                          |
| <b>FD-129</b>      | FBI Fingerprint Cards                                    |
| <b>FISCAM</b>      | Federal Information System Controls Audit Manual         |
| <b>FISMA</b>       | Federal Information Security Management Act              |
| <b>GAO</b>         | General Accounting Office                                |
| <b>J&amp;C</b>     | Judgment and Commitment Order                            |
| <b>MNet</b>        | Marshals Network                                         |
| <b>N/IL</b>        | Northern District of Illinois                            |
| <b>NIST</b>        | National Institute of Standards and Technology           |
| <b>OIG</b>         | Office of the Inspector General                          |
| <b>OMB</b>         | Office of Management and Budget                          |
| <b>PTS</b>         | Prisoner Tracking System                                 |
| <b>PSD</b>         | Prisoner Services Division                               |
| <b>SDLC</b>        | Software Development Life Cycle                          |
| <b>S/FL</b>        | Southern District of Florida                             |
| <b>S/NY</b>        | Southern District of New York                            |
| <b>SP</b>          | Special Publication                                      |
| <b>S/TX</b>        | Southern District of Texas                               |
| <b>SSN</b>         | Social Security Number                                   |
| <b>U.S.C.</b>      | United States Code                                       |
| <b>USERID</b>      | User identification                                      |
| <b>USM</b>         | United States Marshals                                   |
| <b>USM-552/553</b> | Medical Summary of Federal Prisoner/Alien in Transit     |
| <b>USMS</b>        | United States Marshals Service                           |
| <b>USM-129</b>     | United States Marshals Service-129 Prisoner Intake Form  |
| <b>USM-312</b>     | United States Marshals Service-312 Personal History Form |
| <b>WT-J/C</b>      | Waiting Judgment and Commitment Order                    |

**GENERAL CONTROLS CRITERIA**

1. Privacy Act of 1974, Public Law 93-579
2. Computer Fraud & Abuse Act of 1986, as amended, Public Law 99-474
3. Computer Security Act of 1987, Public Law 100-235
4. Paperwork Reduction Act of 1978, as amended in 1995, U.S. Code 44 Chapter 35
5. OMB Circular A-130, "Management of Federal Information Resources," Section 6, "Definitions" and Section 8, "Policy"
6. OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," Section A, "Requirements" and B, "Descriptive Information"
7. The GAO's Federal Information System Controls Audit Manual, Chapter 3, "Evaluating and Testing General Controls"
8. Department of Justice Order 2640.2E, Information Technology Security, Chapter 1, "Security Program Management" and Chapter 2, "Security Requirements"
9. National Institute of Standards and Technology, Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook"
10. National Institute of Standards and Technology, Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems"
11. National Institute of Standards and Technology, Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems"
12. National Institute of Standards and Technology, Special Publication 800-40
13. National Institute of Standards and Technology, Federal Information Processing Standards Publication 73, Section 3.1.1

**APPLICATION CONTROLS CRITERIA**

1. The GAO's Federal Information System Controls Audit Manual, Chapter 4, "Evaluating and Testing Application Controls"
2. Department of Justice Order 2640.2E, Information Technology Security, Chapter 2, "Security Requirements," Section 16, "Access Control;" 18.h., "Accountability and Audit Trails;" 23, "Assignment and Segregation of Duties"
3. OMB Circular A-130, "Management of Federal Information Resources," Section 6, "Definitions" and Section 8, "Policy"
4. OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," Section A.3.b.2., "Application Security Plan" and B.b.2.g., "Public Access Controls"
5. OMB Circular A-130, Appendix IV, "Analysis of Key Sections," Analysis, Section 8a(4), "Records Management" and "Training"
6. National Institute of Standards and Technology, Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook," Chapter 4, "Common Threats," 1. "Errors and Omissions"
7. National Institute of Standards and Technology, Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems"
8. National Institute of Standards and Technology, Special Publication 800-53, "Recommended Security Controls," SI-2.b "Personnel Supervision;" SI-5.e.MP-1e, "Media Access;" and SI-5.e, "Validation of Mission Processing, Output"
9. National Institute of Standards and Technology, Special Publication 800-64, "Security Considerations in the Information System Development Life Cycle," B.10.3, "Auditing"
10. National Institute of Standards and Technology, Federal Information Processing Standards Publication 73, Section 3.1, "Data Validation"
11. The USMS's Prisoner Tracking System Contingency Plan, Version 1.08, dated June 2003

12. The USMS's "Cellblock Operations" Directive 99-47, "Prisoner Tracking System (PTS) and Appendix B – "Records to be Maintained in the USM-123 File"
13. The USMS's "Prisoner Tracking System User Manual," dated June 2003
14. The USMS's "PTS System Security Guide," dated June 2003
15. The "USMS System Security Plan for the Prisoner Tracking System (PTS)/USMS Automated Booking Station (USMS-ABS)," Version 1.05, dated June 2003
16. The USMS's Security Evaluation Report dated June 2003

**DATA INTEGRITY ASSESSMENT CRITERIA**

1. "Assessing the Reliability of Computer-Processed Data,"  
GAO-03-273G, October 2002
2. National Institute of Standards and Technology, Special Publication  
800-12, "An Introduction to Computer Security: The NIST  
Handbook," 1.4, "Important Terminology"



U.S. Department of Justice

United States Marshals Service

Office of the Director

Washington, DC 20530-1000

June 8, 2004

MEMORANDUM TO: Guy K. Zimmerman  
Assistant Inspector General  
for Audit

FROM: Benigno G. Reyna   
Director

SUBJECT: Response to Draft Audit Report - Review of the United States  
Marshals Service's Prisoner Tracking System

Thank you for the opportunity to comment on the draft audit report on your Review of the United States Marshals Service's Prisoner Tracking System (PTS). We have reviewed the recommendations contained in the report, and our comments are attached.

For purposes of accuracy, please note that Page 1 of the report includes dollar figures ascribed to PTS, with Footnote 7 reporting these figures to be derived from budget requests submitted to OMB and JMD. These figures are not consistent with what USMS has submitted through the budget process. We are at OIG's disposal to discuss the figures reported and provide the information we believe to be accurate.

Should you have any questions or concerns regarding this response, please contact Isabel Howell, Audit Liaison, at 202-307-9744.

Attachment

cc: Stacie Hynton  
Assistant Director  
Prisoner Services Division, USMS

Diane Litman  
Acting Chief Information Officer

Michael Pearson  
Assistant Director  
Executive Services Division, USMS

Vickie L. Sloan  
DOJ Audit Liaison

**USMS Response to Draft Audit Report on the  
Review of United States Marshals Service's  
Prisoner Tracking System**

**Recommendation 1:**

Appoint a security manager responsible for the PTS application and ensure the appointment is documented.

**Response:** *(Agree.)* An Information Systems Security Officer (ISSO) for PTS was designated by memorandum dated April 30, 2004. (See Attachment A.)

**Recommendation 2:**

Develop a training program to ensure that PTS users receive specialized training before being granted access to the application.

**Response:** *(Agree.)* The future Justice Detainee Information System (JDIS), a merging of PTS with other USMS systems, will include a training module designed to teach a new user the application before he/she begins actually utilizing the application.

**Recommendation 3:**

Ensure that individuals performing system administrator duties are properly trained in their responsibilities.

**Response:** *(Additional Information Requested.)* The report states that "some system administrators were unfamiliar with their hardware and software environment and lacked specific knowledge...". Accordingly, we will work with the OIG to identify which system administrators lacked the adequate knowledge and expertise. During the exit interview, the OIG stated their finding was based on the auditors speaking to Administrative Officers and/or personnel with collateral IT duties in the Eastern District of Virginia, not to ITS system administrators, who do have adequate training and expertise. If this was the only instance then we will ask that the finding be deleted from the audit report or at a minimum correct the report to reflect the above.

**Recommendation 4:**

Ensure that access authorizations for the PTS are reviewed and that USMS Headquarters update its authorized PTS users list in a timely manner to incorporate changes from the District Offices.

**Response: (*Agree in Part.*)** There is no known DOJ or federal security requirement that states that both local offices and Headquarters must maintain user lists. However, the USMS recognizes the need for establishing internal controls to ensure the integrity of authorized access for PTS. Therefore, the USMS will ensure that our internal audits conducted by USMS Program Review include a review of the districts' lists for accuracy.

**Recommendation 5:**

Ensure that existing measures, such as door locks, are used to provide protection against unauthorized access to sensitive areas.

**Response: (*Additional Information Requested.*)** The audit report states, "physical access controls were adequately enforced at seven of the eight sites visited." It would appear this situation is an aberration versus a systemic problem that justifies categorization as a vulnerability in the report. During the exit interview the USMS requested the site where the locks were not engaged, but to date this information has not been received from the OIG. The USMS would require the location be provided in order to take corrective measures.

**Recommendation 6:**

Ensure PTS users are informed of the policies and procedures for requesting changes to the application.

**Response: (*Disagree.*)** The OIG states that, "PTS application end-users were either unfamiliar with or unaware of the process for requesting changes to the application." As acknowledged in the report, the USMS does have a Systems Development Life Cycle (SDLC) process in place that contains system change request instructions. The SDLC policy is published on the USMS Intranet (making it available to all USMS information technology users). USMS personnel were informed of the new procedures by e-mail at the time of its issuance and provided specialized training. Cumulatively, these measures seem reasonable and adequate to ensure end-users are aware of the necessary process. Moreover, because there is nothing in the audit report text to substantiate that the potential vulnerability noted in the last paragraph of page 12 exists at USMS, we ask that consideration be given to excluding this item as a noted vulnerability.

**Recommendation 7:**

Remove outdated version of the PTS's application programming software and database management system from the production environment and replace with current versions that are supported by the vendor.

**Response: (*Agree.*)** The USMS concurs with the OIG finding on pages iv and 13-14 of the report. The USMS has already taken steps through the development of JDIS to address this problem.

**Recommendation 8:**

Ensure policies and procedures for segregating duties are developed and enforced to provide assurance that district functions are performed by different individuals and that no individual has complete control over the PTS's processing functions.

**Response:** *(Agree in Part, Additional Information Requested.)* To the extent feasible with existing IT staffing resources, the USMS has segregated duties to minimize functional incompatibility. On April 30, 2004, the USMS Chief of IT Security issued memoranda designating specified individuals as Information Systems Security Officers (including for PTS) and delineated their duties. The memorandum is consistent with DOJ policy requirements and should resolve the noted vulnerability.

With regard to the lack of formal policies and procedures for the record creation process, as noted in the last two paragraphs on page 16 of the audit report, we have asked for clarification from the auditors. The formal policy and procedures are outlined in the PTS Users Manual and the Web Based Policy Directive 9.2 (Attachment B).

**Recommendation 9:**

Ensure that:

- a) Employees involved in emergency response procedures are identified and trained in their emergency roles and responsibilities; and
- b) Emergency contact lists are maintained on-site.

**Response:**

- a) *(Disagree, Additional Information Required.)* ITS Regional System Administrators have been briefed by USMS IT Headquarters management, are fully aware of required actions and responsibilities in the event of an emergency situation, and will work with local System Administrators to take appropriate actions.

It would be difficult for the USMS to comment further or address if any further corrective actions are necessary without the OIG identifying what locations or system administrators lack sufficient training to support the restoration of the application and its data files. Our concern has been previously identified in our response to recommendation 3, that the OIG's findings may have been based on the auditors speaking to Administrative Officers and/or personnel with collateral IT duties, not to ITS system administrators who do have adequate training and expertise. However, the USMS will continue to periodically test the IT emergency response procedures, as it is currently doing as part of an incident response exercise being undertaken in collaboration with DOJ.

- b) With regard to the findings and recommendations on pages v and 17-21, the USMS has published its contingency plans (including PTS) on the USMS Intranet site, so districts do have ready access to lists with emergency points of contact and to the emergency procedures to be followed. The PTS contingency plan, which will be tested annually in accordance with DOJ IT security policy, may be found at:  
“[http://156.9.232.31/it/security/resources/CP/FMS%20Contingency%20Plan\\_2003.pdf](http://156.9.232.31/it/security/resources/CP/FMS%20Contingency%20Plan_2003.pdf).”

**Recommendation 10:**

Ensure the PTS’s backup tapes are properly rotated and stored at an off-site location.

**Response: (*Additional Information Requested.*)** As stated in the audit report, there is established USMS IT policy that requires rotation and off-site storage of backup tapes. The USMS would request that the OIG provides details as to the specific sites where backup tapes are not being periodically rotated in order to take corrective action. In addition, ITS will require this be reinforced by USMS Program Review team when they are conducting on site audits of the district offices.

**Recommendation 11:**

Perform annual testing of the PTS contingency plan as required by the Department.

**Response: (*Agree.*)**

The PTS contingency plan will be tested annually in accordance with DOJ IT security policy

**Recommendation 12:**

Develop policies and procedures to:

- a) establish key source document requirements; and
- b) standardize the record creation process throughout the USMS for the PTS.

**Response: (*Agree in Part.*)**

- a) The USMS believes that the policy and procedures for establishing key source document requirements are already in place. The USMS agrees that an internal review should be formalized to ensure that current policies are being adhered to. Therefore, the USMS agrees to direct district management to review and check that source documents are being used correctly in the creation of a prisoner’s record in PTS. The USMS agrees to establish a requirement that, as part of Program Review’s internal audit, key source documents are used accurately when creating or updating a prisoner’s PTS record. The audit will include such things as a review of the prisoner’s file as compared to the reports of the USM-129/312 generated by PTS.

- b) ***(Disagree.)*** The record creation process is standardized throughout the USMS in the policies and procedures promulgated in the PTS User's Manual and associated policy directives.

**Recommendation 13:**

Implement a control, such as requiring the supervisory authorization of data, to ensure that before information is entered into the system, transactions are supported by properly authorized source documents.

**Response: *(Agree in Part.)*** The recommendation calls for a supervisor to sign off on a handwritten USM-129/312. In addition, the OIG also suggests that supervisors oversee data entry by checking each entry against the printed version of the USM-129/312 and checking each transaction against a source document. In our view, unless a prisoner is re-interviewed by the supervisor, there would be little that could be achieved on verification of information, the district can ensure data fields are completed when applicable. Therefore, without creating layers of redundant work, the USMS will notify district managers to perform a periodic spot check of PTS transactions to ensure integrity of information, limited resources will preclude implementation of supervisory verification to the extent OIG suggests.

**Recommendation 14:**

Maintain and review audit trails for the PTS application as required by the Department.

**Response: *(Agree in Part.)*** The Authorization Controls vulnerability (2<sup>nd</sup> checked item vulnerability) noted on page vi is inconsistent with the text supporting it on pages vii and 27 of the audit report. It would appear that the text supports the noted Completeness Controls vulnerability, but should be eliminated as a vulnerability under Authorization Controls. It should also be noted that while the USMS does agree that adequate audit logs do not currently exist on the PTS system, this is due to the age of the system software (as addressed previously in our response to Recommendation 7), not because "USMS management does not require that audit logs be maintained" (as stated on page vii of the audit report). The JDIS initiative underway will rectify the audit log problem.

**Recommendation 15:**

Ensure that the PTS application is modified to perform automatic global database searches of all its district offices' databases to prevent the assignment of more than one USMS number to the same prisoner.

**Response: *(Agree.)*** Through JDIS, global searches will be possible, and enhanced reporting capability will be provided to assist districts/PSD in the identification of erroneous data.

**Recommendation 16:**

Ensure erroneous data is collected and reported back to USMS management for investigation and correction.

**Response: (Agree.)** PSD already performs periodic spot checks of records via reports that are written for jail utilization and population projections. PSD is currently in the process of performing a “records clean-up” in anticipation of the release of a new version of PTS.

**Recommendation 17:**

Ensure that PTS output reports containing sensitive privacy information are protected from unauthorized persons.

**Response: (Disagree.)** The USMS position on this recommendation is that there is no “unauthorized” employee. All USMS employees a background investigation before beginning employment, and receive the appropriate clearance level for this type of information. In addition, all USMS employees will undergo computer security training. Unfortunately, networked printers are a requirement due to limited resources.

**Recommendation 18:**

Ensure that each installation of the application protects against simultaneous updates of the same record by more than one end-user.

**Response: (Additional Information Requested.)** USMS/ITS was unable to replicate the OIG-described situation of concurrent updates of the same PTS record. We ask that OIG provide backup details, so that we can respond to this finding/recommendation.

**Recommendation 19:**

Ensure that adequate and proper source documents are maintained in prisoner file folders to substantiate employee activities.

**Response: (Agree.)** Through policy revisions and memoranda, districts will be specifically instructed as to what information should be contained in the prisoner folder. (Also see our response to Recommendation 12 a).

**Recommendation 20:**

Ensure that data integrity assurances and quality control measures are developed and implemented to:

- a) require the periodic spot-checking and validation of output from the PTS; and

b) confirm that the processing of information is correct.

**Response. (*Agree.*)** Please refer to our responses to Recommendations 13, 16, and 19, as this recommendation is closely related. We will remind the district offices to keep clean and accurate prisoner folders.

**OIG Note:** Additional attachments to the consolidated response were too voluminous to incorporate into this report. The attachments may be obtained by contacting the United States Marshals Service.

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

The USMS's response to the audit (Appendix 12) describes the actions taken or plans for implementing our recommendations. In some cases, we made revisions to our final report where appropriate. This appendix summarizes our response and the actions necessary to close the report. In addition to responding to the recommendations the USMS stated in the second paragraph of the cover memorandum "For purposes of accuracy, please note that Page 1 of the report includes dollar figures ascribed to PTS, with Footnote 7 reporting these figures to be derived from budget requests submitted to OMB and JMD. These figures are not consistent with what USMS has submitted through the budget process. We are at OIG's disposal to discuss the figures reported and provide the information we believe to be accurate."

We requested operating cost information for the PTS on two occasions from USMS representatives prior to the issuance of the PTS draft report. On the first occasion, February 24, 2004, we sent a written request to the USMS Planning and Analysis Branch requesting budget information. During our second attempt on February 25, 2004, we sent a request to a USMS IT Services representative who replied that he had "passed the request on to the USMS budget people." We informed the USMS that this information would be used in the draft report and that the request was time sensitive since we were in the final stages of writing the draft report. Because we were not provided with information from either of the USMS contacts, we contacted the Justice Management Division to determine if any historical budget information existed in their files. On March 8, 2004, the Justice Management Division provided the information used in the report. According to JMD's representative, "The official source of the information are exhibit 300 or 53 reports prepared by the component that are on file in our office." Therefore, the OIG did not dispute the accuracy of the information since we were informed that it originated from the USMS.

Because the USMS expressed concern that the costs provided by the JMD were not accurate, we again contacted the USMS on July 12, 2004, to obtain the operating costs the USMS believed to be accurate for PTS. On July 21, 2004, the USMS provided an email containing

cost information for which we subsequently requested the supporting documentation such as an exhibit 300 or 53 report. However, the USMS could not provide any supporting budget documentation to substantiate the figures it provided. Therefore, the operating cost information previously provided by JMD will remain in the report as the official and best available data for the PTS.

With respect to our recommendations, the USMS frequently disagreed or the corrective action proposed by the USMS was not sufficient to address our recommendations. For these reasons, recommendations 3, 4, 5, 6, 8, 9, 10, 12, 13, 14, 17, and 18 are unresolved. The status of each recommendation follows:

**Recommendation Number:**

1. **Closed.** The USMS provided a copy of a signed memorandum dated April 30, 2004, designating an Information Systems Security Officer (ISSO) for the PTS. As a result of the USMS actions, we consider this recommendation closed.
2. **Resolved.** The USMS states that the future Justice Detainee Information System (JDIS) will include a training module for the PTS application. To close this recommendation, the USMS should provide milestones for its implementation to us with evidence that the training module for PTS is or has been developed.
3. **Unresolved.** The USMS requested additional information pertaining to which system administrators lacked adequate training and expertise regarding their knowledge of the PTS's hardware and software environment. The USMS believed that this finding was noted because the OIG may have interviewed the wrong personnel.

As we stated at our exit conference with the USMS, in planning our site visits, we first contacted each affected district office and requested the following individuals be made available for meetings or interviews: the U.S. Marshal (or designee), system administrator, and criminal clerk. At the Eastern District of Virginia, we were directed to an individual whom we were told was performing system administrator duties. As the interview progressed, however, we learned that the individual was performing some system administrator duties, but that the system administrator responsible for the site was physically located at the District Court for the District of Columbia. While at the Eastern District of Virginia, we gathered the information this individual

could provide and subsequently interviewed the responsible system administrator. We did not, however, interview the administrative officer in lieu of the system administrator. Rather, we were initially misdirected and subsequently spoke to the system administrator responsible for the office. When we spoke to the system administrator who represented the site in question, we still found deficiencies with the system administrator's knowledge.

As stated in the final report, the system administrator position description provided by the USMS states that system administrators are responsible for "operating, troubleshooting, repairing, and maintaining IT systems." Additionally, the position description states that employees must possess the requisite technical knowledge to sustain the availability of the hardware and software environment and be competent to maintain operating systems, applications, and data elements. According to the USMS headquarters, system administrators within the district offices are responsible for adding and deleting user names from the PTS authorized user list. However, we found specific problems at the sites indicated below:

### Deficiencies Found Pertaining to System Administrator Training and Expertise

| Specific Deficiencies                                                                                | E/VA | DC/DC | E/PA | S/NY | S/TX | N/IL | S/FL | D/AZ |
|------------------------------------------------------------------------------------------------------|------|-------|------|------|------|------|------|------|
| System Administrators lacked knowledge of the PTS change control process                             | X    | X     | X    | X    |      | X    | X    |      |
| System Administrators were unfamiliar with the PTS application's timeout period                      | X    | X     | X    |      | X    | X    | X    |      |
| System Administrators were unfamiliar with the PTS application's master files                        | X    | X     | X    | X    | X    | X    | X    |      |
| System Administrators did not know the version number of PTS running on the District Office's server | X    | X     |      | X    | X    | X    | X    | X    |
| System Administrators did not know how to delete user names from the PTS authorized user list        | X    | X     |      |      |      |      |      |      |

**Source:** OIG working papers

When we requested to speak to the system administrator at the Eastern District of Virginia, we were directed to the administrative officer. The administrative officer was performing cursory system administrator duties and he did not know where the PTS database

for the district office was located. We subsequently interviewed the system administrator, whom we located at the District Court for the District of Columbia, and found that she did not know how to delete names from the user list, among other things.

The areas identified in the previous chart represent facets of requisite technical knowledge that enable system administrators to effectively sustain the availability of the hardware and software environment and demonstrate competence in maintaining operating systems, applications, and data elements.

In order to resolve and close this recommendation, the USMS should provide documented evidence to us that individuals performing system administrator duties are properly trained in their responsibilities.

4. **Unresolved.** The USMS's response asserts that there is no Department or federal security requirement to maintain user lists at both the USMS district offices and at USMS headquarters. The USMS response does not address our recommendation. Our recommendation speaks to the condition that the PTS authorized user list provided by the USMS headquarters contained information that, once verified at the site, possessed multiple inaccuracies. Appendices 5 and 6 of this report contain excerpts from Chapters 3 and 4 of the GAO's FISCAM, which we used as guidance for the development of the audit program followed during the audit. Pages 54 through 55 of the final report provide the specific FISCAM requirement that the computer resource owner should maintain a current list of authorized users and ensure that their access is authorized. We did not recommend that separate lists be maintained. Separate lists exist because the USMS headquarters has delegated the user management responsibility to the district offices (DOs). This does not absolve the USMS headquarters from its responsibility as data owners to maintain a current list of authorized users and ensure that their access is authorized.

Additionally, the Department's Order 2640.2E requires that each authorized user of a system have a unique identifier. In the case of the authorized user list provided by USMS headquarters, entries were found to be outdated and did not reflect a replication of changes, additions, and deletions made at the district offices we visited. Our report details the nature and frequency of errors found during our user list review at each site. In order to resolve and close this recommendation, the USMS should provide evidence

to us that the access authorizations for the PTS are reviewed and that USMS headquarters updates its authorized PTS user list in a timely manner to incorporate changes from the DOs.

5. **Unresolved.** As we stated at our exit conference, we found that the lock on the door to the office suite containing data terminals, prisoner file folders, printed output reports, and other sensitive information was not engaged at the District Court for the District of Columbia location. During our visit, we were able to gain access to this area from the hallway in a building accessed by the public, and at the time, no one assigned to the district office was present in the area. Although physical security is provided at the entrance to the building, private citizens are unescorted once they enter the building, which presents a serious threat to the protection of sensitive information. We agree that this condition occurred at only one of the eight sites reviewed. However, we found that the means for providing adequate physical security was present and a lock was on the door. Unfortunately, the office failed to exercise due diligence to ensure its use. Additionally, this condition was in sharp contrast to the high levels of security observed at the other seven sites visited. In order to resolve and close this recommendation, the USMS should provide us with documented evidence that existing measures, such as door locks, are used to provide protection against unauthorized access to sensitive areas.
  
6. **Unresolved.** The USMS response states that system change request instructions for the PTS application have been sufficiently disseminated to users of the application. The USMS headquarters informed us prior to our site visits of the systems development life cycle (SDLC) process in place that contains system change request instructions. Although the USMS feels that users have been sufficiently notified of existing policies, our observations proved different. As stated previously, we followed an audit program in which identical questions were asked of individuals representing specific positions within the district office. Specifically, we asked those most familiar with the application, the criminal clerk and the system administrator, how changes were requested to the PTS application. We found at all eight of the locations visited, the Eastern District of Virginia; the District Court for the District of Columbia; the Eastern District of Pennsylvania; the Southern District of New York; the Southern District of Texas; the Northern District of Illinois; the Southern District of Florida; and the District of Arizona, that knowledge of the official change control process for the PTS application was deficient. In most cases, neither the

system administrator nor the criminal clerk were aware of the existence of a change request form or how to process a request according to the existing policy.

Also in the USMS's response to recommendation 6, the USMS states that the audit report text does not substantiate the information in the last paragraph of page 12 of the draft report where the discussion of the ineffective management of modifications to application software is expanded to include unauthorized changes made by knowledgeable programmers. On page 16 of our report, we state that, "At the USMS's headquarters, only one individual is assigned to code, test, and implement changes to the PTS application." This example substantiates the audit report text because according to the Department's Order 2640.2E, components are directed to integrate security into various stages of a system's life cycle and to ensure that changes to any system are controlled. Changes to a system include changes requested by users as well as changes made by knowledgeable programmers. We presented this information on page 16 under Segregation of Duties because it represented a good example of failure to segregate duties among staff although it also applies to the ineffective management of modifications to application software. We disagree that this vulnerability should be excluded from the report. In order to resolve and close this recommendation, the USMS should provide documented evidence to us that PTS users are informed of the policies and procedures for requesting changes to the application.

7. **Resolved.** The USMS states that it has taken steps through the development of JDIS to address the problem of PTS's outdated programming software and database management system. In order to close this recommendation, the USMS should provide documented evidence to us that the outdated versions of the PTS's application programming software and database management system have been removed from the production environment and replaced with current versions that are supported by the vendor.
8. **Unresolved.** The USMS provided an attachment to its response to demonstrate that duties have been segregated to minimize functional incompatibility. The attachment lists duties for positions within the USMS such as end users, system administrators, and the information systems security officer as they relate to computer security. While valuable, the information only partially addresses the conditions described on pages 15 through 17 of the report that

enumerate problems with procedures that affect critical processes performed by the PTS application's end users and the application programmer.

In this report, we provide the FISCAM guidance under the "Segregation of Duties" section that requires entities not only to segregate incompatible duties, but also to establish related policies. We also provide FISCAM guidance that requires entities to control personnel activities through formal operating procedures and supervision and review. Our recommendation applies to our observations during field site visits that duties were not sufficiently segregated among staff and that sufficient procedural guidance does not exist for the record creation process. Specifically, district office operations allow an end user to create a prisoner record, manipulate that record, and commit changes to information contained in the PTS database with no management oversight or approval prior to the completion of a transaction, or shortly thereafter. This condition creates the situation where a single individual has complete control over the input, processing, and output stages of the information cycle. We also provided the example of the condition existing at USMS headquarters wherein one individual can code, test, and implement software changes thereby having complete control over the PTS's system life cycle.

We have reviewed the information provided as Attachment 2 to the USMS response. The additional procedural steps added to the Cellblock Operations Manual 99-47 address the conditions described in this report pertaining to controlling personnel activities through formal operating procedures. However, none of the information provided ensures that duties affecting the application's life cycle are sufficiently segregated or that supervisory review of data is assigned to anyone at the district office level. In order to resolve and close this recommendation, the USMS should provide to us documented evidence that policies and procedures for segregating duties are developed and enforced to provide assurance that distinct functions are performed by different individuals and that no individual has complete control over the PTS's processing functions.

- 9a. **Unresolved.** The USMS contends that system administrators are fully aware of required actions and responsibilities in the event of an emergency situation and the USMS requested that we provide specific examples of where this may not be accurate. We reviewed both the USMS system security plan for the PTS

application and the contingency plan for the application in order to gain an understanding of emergency procedures in place to protect the application and minimize service interruptions. We found that emergency procedures and contact information established for the PTS application are contained in the contingency plan for the application; however, the USMS headquarters confirmed that it had not disseminated the contingency plan to the district offices. We found that none of the system administrators at the sites had been provided a copy of the contingency plan containing emergency procedures and contact information. In addition, we found that the USMS has not tested the contingency plan for PTS to actually verify that employees can perform their necessary duties in the event of an emergency. We found the following conditions at the sites indicated in the chart below:

### Emergency Procedures Deficiencies

| Specific Conditions                           | E/VA | DC/DC | E/PA | S/NY | S/TX | N/IL | S/FL | D/AZ |
|-----------------------------------------------|------|-------|------|------|------|------|------|------|
| No emergency contact list on site             | X    |       | X    | X    | X    | X    | X    |      |
| No knowledge of the existing contingency plan | X    | X     | X    | X    | X    | X    | X    | X    |

**Source:** OIG working papers

In order to resolve and close this recommendation, the USMS should provide evidence to us that it has tested the contingency plan and disseminated the plan to system administrators to ensure that employees involved in emergency response procedures are identified and trained in their emergency roles and responsibilities.

- 9b. **Unresolved.** The USMS provided information regarding the location of its contingency plans on the USMS intranet. However, this electronic posting does not provide assurance that in the event of an emergency where access to files located on network servers are not available, that individuals at the site would know who to contact. In order to resolve and close this recommendation, the USMS should provide to us documented evidence that emergency contact lists are maintained on-site.
- 10. **Unresolved.** The USMS requested additional information regarding specific sites where backup tapes were not being rotated off-site. We found that this condition existed at the Eastern

District of Pennsylvania and the Southern District of New York. The USMS provided a corrective action plan to reinforce backup tape rotation policies at the locations identified. In order to resolve and close this recommendation, the USMS should provide us with documented evidence that PTS's backup tapes are properly rotated and stored at an off-site location.

11. **Resolved.** The USMS states that the PTS contingency plan will be tested, but does not specify a milestone date for this action. In order to close this recommendation, the USMS should provide us a milestone date for the annual testing of the PTS contingency plan as required by the Department and confirmation of the results of the test once completed.
- 12a. **Unresolved.** The USMS states that key source document requirements are already in place and that district office management will be directed to review data collection activities. We agree that modifications made to the Cellblock Operations Manual 99-47 provide guidance to improve data collection procedures. However, the revised Cellblock Operations Manual does not define, specifically, the minimum source documents required during the record creation process, such as two photographs of the inmate to aid the USMS with proper inmate identification and the medical form USM-552 to document health related issues disclosed during the initial interview with the inmate. In order to resolve and close this recommendation, the USMS should provide evidence to us that policies and procedures to establish key source document requirements have been developed.
- 12b. **Unresolved.** The USMS states that the record creation process is standardized throughout the USMS and states that the PTS User's Manual and associated policy directives address this condition. However, during our site visits we found that the USMS had not established controls over source documents nor provided for their proper authorization because the USMS had not provided adequate data rules for employees or set standards for consistency during the record creation process. In order to resolve and close this recommendation, the USMS should provide evidence to us that policies and procedures were developed to standardize the record creation process throughout the USMS for the PTS.
13. **Unresolved.** The USMS's response states that the OIG calls for a supervisor to sign off on a handwritten USM-129/312. This is not an accurate interpretation of our recommendation. We

recommended that a "control" be implemented to ensure that transactions are supported by properly authorized source documents, but we did not mandate that supervisors sign off on handwritten USM-129/312s. In the report, we simply presented supervisory authorizations on source documents as an example of a control. We observed at the Eastern District of Virginia that the handwritten USM-129 was used as a form of authorization control and offered this as an example of what worked effectively at one office, but did not suggest this practice as an overall solution. The determination of what specific control would be feasible for implementation throughout the USMS was left to the discretion of the USMS. To resolve and close this recommendation, the USMS should provide us with documented evidence that it has implemented a control to ensure that before information is entered into the system, transactions are supported by properly authorized source documents.

14. **Unresolved.** The USMS agrees that sufficient auditing is not conducted, but states that this deficiency is not due to the lack of management's requirement to do so. We reviewed the certification and accreditation documentation for the PTS application provided by the USMS in June 2003. On Form 6, Item 14a and b of the Risk Assessment Report for PTS/USMS-ABS dated June 2003, the USMS responded affirmatively that it has defined audit requirements for the PTS application and that the application has the capability to identify the creator of data and processes. In order to resolve and close this recommendation, the USMS should provide documentation to us evidencing that audit trails for the PTS application are maintained and reviewed as required by the Department.
15. **Resolved.** The USMS states that global database searches will be possible through the upcoming JDIS initiative. In order to close this recommendation, the USMS should provide documented evidence to us indicating that the PTS application has been modified to perform automatic global database searches of all its district office databases.
16. **Resolved.** The USMS indicates that erroneous data is collected through jail utilization and population projection reports reviewed by the Prisoner Services Division. The USMS does not indicate, however, what types of erroneous data are captured or what actions are taken to correct and investigate such data. Specifically, this audit report refers to the need to collect and review

information on erroneous data, such as rejected transactions and input errors or omissions, to determine if errors cause threats to the PTS application or render the system vulnerable to compromise. Our findings indicate that all eight sites visited failed to collect statistics on the frequency of error messages generated by the system. In order to close this recommendation, the USMS should provide to us documented evidence of how erroneous data is collected and reported back to the USMS management for investigation and correction.

17. **Unresolved.** The USMS contends that there is no “unauthorized” employee from which sensitive privacy information should be protected and asserts that a background investigation suffices as authorization to access PTS data. However, an examination of PTS’s certification and accreditation documents indicates that the USMS does distinguish between “authorized” and “unauthorized” users.

Specifically, in the PTS/USMS-ABS System Security Plan, Section 1.8, System Interconnection/Information Sharing, the USMS states that “Not all Marshals users are authorized access to PTS, but all users who are authorized to connect to PTS do so through MNET.” In the security plan’s Section 4. 2, Logical Access Controls, the USMS explicitly states that “Controls exist in the PTS system to authorize and restrict users from performing particular functions.” The document further states that “Access rights are granted based on the determination of USMS district management.”

In the PTS’s system security plan, section 1.10, General Description of Information Sensitivity, the USMS defines the requirement for confidentiality as high and further states that “Inappropriate disclosure of the information of the information could have negative impact on the safety of prisoners in USMS custody and the law enforcement officials assigned to transport and guard them. Furthermore, inappropriate disclosure could place the families of prisoners in USMS custody at risk as well as USMS employees assigned to protect and transport prisoners. All Privacy Act information within PTS must be protected. . . The requirement for confidentiality is **HIGH**.” Protection of system data includes output reports and considering the USMS’s own categorization of its requirement for confidentiality as high, USMS’s protection of system output must be commensurate with its confidentiality category. In order to resolve and close this recommendation, the USMS should provide to us documented evidence that output

reports containing sensitive privacy information are protected from unauthorized persons.

18. **Unresolved.** The USMS requests that additional information be provided regarding instances where the PTS application allowed simultaneous updates of the same record by more than one user. We witnessed this condition at the following locations: the District Court for the District of Columbia; the Eastern District of Pennsylvania; the Southern District of New York; and the District of Arizona. In order to resolve and close this recommendation, the USMS should provide us documented evidence that each installation of the PTS application protects against simultaneous updates of the same record by more than one end-user.
19. **Resolved.** The USMS agrees with our recommendation that adequate and proper source documents be maintained in prisoner file folders to substantiate employee activities. The USMS submitted a revised Cellblock Operations Manual 99-47 that enumerates in Section C.3, Prisoner Records, specific documents that must be maintained in prisoner files. In order to close this recommendation, the USMS should provide documented evidence to us that an internal review process has been formalized to ensure that adequate and proper source documents be maintained in prisoner file folders to substantiate employee activities.
- 20a. **Resolved.** The USMS agrees with our recommendation to implement integrity assurances and quality control measures to require periodic spot-checking and validation of output from the PTS. We have accepted the USMS's proposed resolution to Recommendation 19 that refers to Recommendation 12a. The proposed resolution to Recommendation 12a states that the USMS will include, during its Program Review's internal audits, a review of prisoner's files to compare the contents with reports of the USM-129/312 generated by PTS. In order to close this recommendation, the USMS should provide documented evidence to us that policies and procedures to implement quality control measures require the periodic spot-checking and validation of output from the PTS have been developed.
- 20b. **Resolved.** As stated previously, we accept the USMS's proposed resolution to Recommendation 19 that refers to its proposed resolution to Recommendation 12a. The proposed resolution to Recommendation 12a states that output will be checked as a requirement during Program review's internal audits to confirm

that processing of information is correct. In order to close this recommendation, the USMS should provide documented evidence to us that policies and procedures have been developed to implement quality control measures to confirm that the correct information is processed in PTS.