Audit Report

Department of State Police

March 2013

OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

- This report and any related follow-up correspondence are available to the public through the Office of Legislative Audits at 301 West Preston Street, Room 1202, Baltimore, Maryland 21201. The Office may be contacted by telephone at 410-946-5900, 301-970-5900, or 1-877-486-9964.

- Electronic copies of our audit reports can be viewed or downloaded from our website at http://www.ola.state.md.us.

- Alternate formats may be requested through the Maryland Relay Service at 1-800-735-2258.

- The Department of Legislative Services – Office of the Executive Director, 90 State Circle, Annapolis, Maryland 21401 can also assist you in obtaining copies of our reports and related correspondence. The Department may be contacted by telephone at 410-946-5400 or 301-970-5400.

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Karl S. Aro
Executive Director

Thomas J. Barnickel III, CPA
Legislative Auditor

March 20, 2013

Senator James C. Rosapepe, Co-Chair, Joint Audit Committee
Delegate Guy J. Guzzone, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have audited the Department of State Police (DSP) for the period beginning February 1, 2009 and ending December 19, 2011. DSP comprises the Maryland State Police, the Office of the State Fire Marshal, and the State Fire Prevention Commission.

Our audit disclosed that DSP lacked adequate controls over collections and related billings. For example, independent verifications that Finance Office collections were subsequently deposited were not documented, and reconciliations of license applications received with the related collections were not performed. In addition, we noted that controls over DSP's information systems should be improved. In part, we noted that critical DSP network security devices were not operational or properly monitored and sensitive personally identifiable information was not properly secured. In addition, controls over DSP equipment should be improved.

DSP's response to this audit is included as an appendix to this report. We wish to acknowledge the cooperation extended to us during the course of this audit by DSP.

Respectfully submitted,

Thomas J. Barnickel III, CPA
Legislative Auditor

301 West Preston Street · Room 1202 · Baltimore, Maryland 21201
410-946-5900/301-970-5900 · Fax 410-946-5999/301-970-5999
Toll Free in Maryland 877-486-9964 · Fraud Hotline 877-FRAUD-11

Table of Contents

* **Denotes item repeated in full or part from preceding audit report**

Background Information

Agency Responsibilities

The Department of State Police (DSP) operates under the provisions of Title 2 of the Public Safety Article of the Annotated Code of Maryland. The Code provides that DSP shall safeguard the lives and the safety of all persons within the State, protect property, and assist in securing to all persons the equal protection of the laws. DSP provides these services through a headquarters unit located in Pikesville, Maryland and 22 barracks and detachments located throughout the State. In addition, DSP includes the State Fire Marshal and the State Fire Prevention Commission. According to the State's records, during fiscal year 2012, DSP's operating expenditures totaled approximately $289.7 million.

Special Fund Deficit Balance

DSP has a longstanding special fund deficit balance totaling approximately $5.1 million that, as of December 5, 2012, had not been resolved. During the fiscal year 2005 budget closeout, DSP mistakenly transferred special funds to the State's General Fund (since it did not have legal authority to retain any remaining balance in this special fund), instead of reversing a previously recorded accrued revenue transaction when the funds were received. When this mistake was discovered during fiscal year 2006, DSP was left with a deficit special fund balance of $5.6 million. Since fiscal year 2006, excess revenues of $500,000 were retained in the fund, which reduced the negative balance to the current $5.1 million. DSP submitted a request during the 2012 legislative session, and in several preceding years, for a deficiency appropriation to eliminate this deficit, but without success. DSP has again requested funds to cover this deficit for consideration during the current (2013) legislative session. This issue was commented upon in our preceding fiscal compliance audit report and also has been commented upon in our seven preceding annual budget closeout reviews.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the 14 findings contained in our preceding audit report dated January 20, 2010. We determined that DSP satisfactorily addressed 11 of these findings. The remaining 3 findings are repeated in this report.

Findings and Recommendations

Cash Receipts and Receivables

Finding 1
DSP lacked adequate procedures and controls over collections and related billings.

Analysis
DSP lacked adequate procedures and controls over collections and the related billings in the Finance Office and the Licensing Division. During fiscal year 2011, Finance Office and Licensing Division collections totaled approximately $14.7 million and $1.2 million, respectively. Our review disclosed the following conditions:

- Independent verifications that the Finance Office collections were subsequently deposited were not documented. We were advised by DSP personnel that the deposit verifications were performed; however, the verifications were not documented. As a result, DSP lacked assurance that all Finance Office collections were subsequently deposited. The Comptroller of Maryland's *Accounting Procedures Manual* requires an employee independent of the collections function ensure that all collections were subsequently deposited. A similar condition was noted in our preceding audit report.

- DSP did not periodically reconcile applications processed as recorded on its automated licensing system with the related collections recorded on the State's accounting system. Our comparison of the fiscal year 2011 recorded collections and the fees that should have been received based on the number of handgun permit applications processed per DSP's automated licensing system disclosed a difference of approximately $149,000. Specifically, collections recorded on the State's accounting system totaled $274,828 whereas expected collections based on the number of applications processed and the related application fee totaled $424,290. We were advised by DSP management that this difference was attributable to certain system deficiencies and to coding errors made by DSP when recording receipts in the State's accounting records (which we confirmed via limited testing). The automated licensing system is used to issue various licenses, such as handgun permits. A similar condition was noted in our preceding audit report.

- Monthly billings to certain firearms dealers for application fees were not issued in a timely manner. As a result, remittances from the dealers were not received as required by law. Our test of 10 invoices issued in fiscal year 2012 totaling $5,060 disclosed that all 10 invoices were issued between 26 and 42 days after the end of the month when they should have been issued. We also noted that DSP did not issue invoices to any dealers from October 2010 through February 2011, although retroactive invoices were issued beginning in March 2011. Certain firearms dealers with higher sales volumes participate in a program that allows the dealer to fax in applications for firearms throughout the month and at the end of the month DSP is to invoice the dealer for the applications received. The Public Safety Article of the Annotated Code of Maryland requires firearms dealers participating in the fax-in application program to pay the total application fees collected by the fifteenth day of the month following collection.

- DSP did not maintain a control account over the accounts receivable for the billings issued to firearms dealers.

Recommendation 1
We recommend that DSP ensure that

a. an employee independent of the collections function verify and document that all recorded collections were subsequently deposited (repeat),
b. an employee independent of the collections function periodically reconcile the applications received with the related billings and collections and investigate any differences (repeat),
c. billings to firearms dealers are issued in a timely manner, and
d. a control account is established and maintained over firearms dealer billings.

Information Systems and Control

DSP's Information Technology Division is responsible for information technology and communications management in support of field troopers, investigators, support personnel, allied law enforcement agencies, state and local government agencies, and the citizenry. DSP's information technology environment includes an integrated computer network that provides connections to a number of servers and workstations. Key network resources include the citation system, which is used for citations, warnings, field observation reports, and vehicle safety equipment repair orders. Other key network resources include Internet connectivity and firewalls used to protect segments of the network.

Finding 2
Database monitoring, program change controls, and backup procedures over the citation system were inadequate.

Analysis
Database monitoring, program change controls, and backup procedures over the citation system were inadequate. Specifically, we noted the following conditions:

- The database supporting the citation system was not configured to log any database security activity other than activity performed using a few privileged accounts. Examples of database activities which should be logged and analyzed include, but are not limited to, direct changes to critical data tables, changes to database security settings, and use of certain critical privileges. In addition, for actions that were logged, DSP did not review these logs. A similar situation was commented upon in our preceding audit report.

- Program change control procedures over this application's computer programs did not include a comparison report of identified program changes for programs moved to production or a technical review of the related program source code for propriety. A similar situation was commented upon in our preceding audit report.

- The citation system database was not backed up at an offsite facility. Full backups of this database were created but were retained in the same room that houses the production database. If the facility that houses both the production and backup versions of the database was destroyed by a disaster, it is highly uncertain if all critical information could be recreated.

The State of Maryland Department of Information Technology's (DoIT) *Information Security Policy*, requires that information systems generate audit records to ensure accountability for security-relevant events and that audit records are routinely reviewed for suspicious activities or suspected violations. In addition, this *Policy* requires that agencies shall implement an appropriate process to ensure that changes to systems are controlled. Finally, the State of Maryland *IT Disaster Recovery Guidelines* state that backup procedures should designate the method of transporting data offsite, and a description of the offsite storage facility.

Recommendation 2

We recommend that DSP establish adequate controls over the citation system. Specifically, we recommend that DSP

a. enable database logging of direct changes to critical data tables, changes to database security settings, and use of critical system privileges, and that reviews of these logs are performed, documented, and retained for future reference (repeat);

b. create and review comparison reports of program changes prior to moving programs into production status, perform technical reviews of changes for propriety, and ensure that program change reviews and approvals are documented and retained for future reference (repeat); and

c. store backup copies of its citation system database at a secure offsite location.

Finding 3

Critical devices used to secure the DSP network were not operational, or properly administered and monitored.

Analysis

Critical devices used to secure the DSP network were not operational, or properly administered and monitored. Specifically, we noted the following conditions:

- DPS did not have intrusion detection prevention system (IDPS) protection for its network. At the time of our review, IDPS protection for the DSP network had not existed for the seven-month period since the date when the second of two IDPS appliances employed by DSP failed. An IDPS system can aid significantly in the detection/prevention of and response to potential network security breaches and attacks. In addition, DoIT's *Information Security Policy* states that intrusion detection/prevention tools and techniques must be employed to monitor system events, detect attacks, and identify unauthorized use of information systems and/or confidential information.

- An insecure connection protocol was used for administration of the DSP firewalls. In addition, remote administrative connections to these firewalls were not restricted to those originating from only authorized firewall administrators' workstations. Finally, five shared accounts were used to administer these firewalls. Use of shared accounts precludes individual accountability for actions performed with these accounts.

- DSP personnel advised us that they performed daily manual reviews of the voluminous firewall logs; however, there was no documentation supporting these reviews. In addition, based on the size of these firewall logs, it is neither effective nor efficient to manually review the logs and, therefore, the use of an automated script to identify significant security events for review would be more practical. Furthermore, the firewalls were not configured to send alerts to administrators regarding serious operational concerns detected by the devices. DoIT's *Information Security Policy* requires that agencies maintain comprehensive audit logs and implement review procedures of these logs.

Recommendation 3
We recommend that DSP

a. evaluate its network security risks and, based on these risks, implement continuous IDPS coverage to effectively protect all critical portions of its network;

b. allow access to the firewalls via only secure protocols, restrict remote access to the firewalls to only network administrators' workstations, and use only unique user accounts to administer the firewalls; and

c. configure the firewalls to send alerts to administrators concerning the devices' operational status, regularly review the firewall logs using an automated process, investigate unusual entries noted during such reviews, and document and retain support for these reviews and investigations for subsequent verification purposes.

Finding 4
Sensitive personally identifiable information was not adequately secured.

Analysis
Sensitive personally identifiable information (PII) was not adequately secured. Specifically, the sensitive PII was stored in plain text files on a host server within a network segment containing publicly accessible servers. We identified a plain text file that, as of March 6, 2012, contained 1,612,930 records processed by the citation system application that included the name, address, and date of birth of individuals. Over 779,000 of these records also contained driver license numbers and over 176,000 records also contained social security numbers. This sensitive PII is commonly sought by criminals for use in identity theft. These records were at risk because the host server was placed in a network segment with publicly accessible servers which, if compromised, could be used to attack the host server.

DoIT's *Information Security Policy* requires that confidential information be protected with administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.

Recommendation 4
We recommend that DSP

a. either encrypt the plain text files or remove these files from the host server, and
b. segregate its publicly accessible and non-public servers to help ensure that all non-public servers are adequately protected.

Equipment

Finding 5
DSP did not establish adequate controls over its equipment.

Analysis
Adequate controls were not established over DSP's equipment. The equipment balance reported to the Department of General Services (DGS) as of June 30, 2011 totaled approximately $116.1 million (excluding vehicles). Specifically, our review disclosed the following conditions:

- The value of inventory reported to DGS on the Annual Report of Fixed Assets did not accurately reflect the value of the DSP equipment. Specifically, the fiscal year 2010 and 2011 reports did not include motor vehicles, which, according to DSP detail records totaled approximately $41 million as of June 30, 2009.

- A control account for motor vehicles was not maintained to provide a continuous summary of transactions and a total dollar value control over amounts in the detail records.

- DSP had not completed annual physical inventories of sensitive equipment as required. Specifically, according to the DSP record of inventories, as of August 2012 the calendar year 2011 physical inventory of sensitive equipment had not been conducted for 76 of the 121 locations that were scheduled for an inventory. In addition, for the 45 locations that were inventoried, the results of the inventory were not reconciled to the detail records.

- DSP did not always record equipment acquisitions and disposals in the detail equipment records on a timely basis. Specifically, our test of 15 equipment acquisitions totaling $977,000 purchased during our audit period disclosed that 4 of the purchases, totaling $82,000, had not been recorded in the detail records as of March 2012. For example, one purchase totaling approximately $45,000 was for computer equipment acquired in calendar year 2009. In addition, during our test of the physical existence, we identified one item with a cost of $17,000 that was returned to the manufacturer as defective which had not been removed from the detail equipment records.

Similar conditions have been commented upon in our five preceding audit reports dating back to January 1998.

DGS' *Inventory Control Manual* requires the maintenance of an independent control account for all categories of equipment to properly reflect all transactions and that the detail records be reconciled to the related control account balance. In addition, the *Manual* requires that periodic physical inventories be conducted, that variances be investigated and resolved, and that related documentation be retained for audit and verification purposes. Finally, the *Manual* requires the recordation of all capital equipment items in the detail records for identification and control purposes.

Recommendation 5
We recommend that DSP comply with the requirements of the Department of General Services' *Inventory Control Manual* (repeat).

Audit Scope, Objectives, and Methodology

We have audited the Department of State Police (DSP) for the period beginning February 1, 2009 and ending December 19, 2011. The audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

As prescribed by the State Government Article, Section 2-1221 of the Annotated Code of Maryland, the objectives of this audit were to examine DSP's financial transactions, records and internal controls, and to evaluate its compliance with applicable State laws, rules, and regulations. We also determined the status of the findings included in our preceding audit report.

In planning and conducting our audit, we focused on the major financial-related areas of operations based on assessments of materiality and risk. The areas addressed by the audit included procedures and controls over handgun registrations and DNA samples, as well as payroll, cash receipts, accounts receivable, information systems, confiscated and forfeited property, and equipment inventories. Our audit procedures included inquiries of appropriate personnel, inspection of documents and records, and observations of DSP's operations. We also tested transactions and performed other auditing procedures that we considered necessary to achieve our objectives. Data provided in this report for background or informational purposes were deemed reasonable, but were not independently verified.

Our audit did not include an evaluation of internal controls for federal financial assistance programs and an assessment of DSP's compliance with federal laws and regulations pertaining to those programs because the State of Maryland engages an independent accounting firm to annually audit such programs administered by State agencies, including DSP.

DSP's management is responsible for establishing and maintaining effective internal control. Internal control is a process designed to provide reasonable assurance that objectives pertaining to the reliability of financial records, effectiveness and efficiency of operations including safeguarding of assets, and compliance with applicable laws, rules, and regulations are achieved.

Because of inherent limitations in internal control, errors or fraud may nevertheless occur and not be detected. Also, projections of any evaluation of internal control to future periods are subject to the risk that conditions may change or compliance with policies and procedures may deteriorate.

Our reports are designed to assist the Maryland General Assembly in exercising its legislative oversight function and to provide constructive recommendations for improving State operations. As a result, our reports generally do not address activities we reviewed that are functioning properly.

This report includes findings that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect DSP's ability to maintain reliable financial records, operate effectively and efficiently, and/or comply with applicable laws, rules, and regulations. Our report also includes findings regarding significant instances of noncompliance with applicable laws, rules, or regulations. Other less significant findings were communicated to DSP that did not warrant inclusion in this report.

DSP's response to our findings and recommendations is included as an appendix to this report. As prescribed in the State Government Article, Section 2-1224 of the Annotated Code of Maryland, we will advise DSP regarding the results of our review of its response.

APPENDIX

MARTIN O'MALLEY
GOVERNOR

ANTHONY G. BROWN
LT. GOVERNOR

STATE OF MARYLAND
MARYLAND STATE POLICE
1201 REISTERSTOWN ROAD
PIKESVILLE, MARYLAND 21208-3899
410-486-3101
TOLL FREE: 1-800-525-5555
TTY: 410-486-0677

COLONEL
MARCUS L. BROWN
SUPERINTENDENT

March 13, 2013

Mr. Thomas J. Barnickel, III
Legislative Auditor
Department of Legislative Services
Office of Legislative Audits
301 West Preston Street, Room 1202
Baltimore, MD 21201

Dear Mr. Barnickel:

Thank you for the opportunity to review the draft findings and recommendations outlined in the final audit report for the period February 1, 2009 to December 19, 2011 for the Maryland Department of State Police. The Department's Inspection and Compliance Division has worked closely with all stakeholders to ensure that each recommendation was considered and corresponding corrective actions immediately addressed. The Department recognizes that three of the findings were repeated from the previous triennial audit; however, please know that significant progress has been made since the last audit was conducted. We have also seen a significant decrease from the fourteen deficient findings as published in the January 2010 public report to now only having five findings in this 2013 report.

Attached please find a copy of the Department's responses to the draft findings report. This document highlights all of the actions that have been taken to ensure full compliance towards all mandated policies and procedures. Please note, our Department's Inspection and Compliance Division remains committed to working with your office in a proactive, constructive, and professional manner.

Should you need any further assistance, please contact Captain Dalaine Brady, Commander, Inspection and Compliance Division, at 410-653-8230 or by email at dalaine.brady@maryland.gov. I look forward to working with you on all matters of mutual concern.

Sincerely,

Marcus L. Brown
Superintendent

MLB:MJC:db

Attachment

cc: Captain Dalaine Brady, Commander, Inspection and Compliance Division
Mr. Mark J. Carter, Director, Strategic Planning Command

Findings and Recommendations

Cash Receipts and Receivables

Finding 1
DSP lacked adequate procedures and controls over collections and related billings.

Recommendation 1
We recommend that DSP ensure that

a. an employee independent of the collections function verify and document that all recorded collections were subsequently deposited (repeat),

b. an employee independent of the collections function periodically reconciles the applications received with the related billings and collections and investigates any differences (repeat),

c. billings to firearms dealers are issued in a timely manner, and

d. a control account is established and maintained over firearms dealer billings.

Agency Response: DSP concurs with the recommendations.

Response to Recommendation a.
Agency Response: DSP concurs with the recommendations

Effective November 2012, the Department's Finance Division has implemented internal control procedures to ensure that an employee independent of the collections function verifies and documents daily deposits in the deposit log in accordance with the Comptroller of Maryland's Accounting Procedures Manual.

Response to Recommendation b., c., d:

In the last triennial public audit report covering May 1, 2006 to January 31, 2009 the Office of Legislative Audits recognized the Licensing Division's lack of system automation. Until automation is accomplished and to ensure compliance with the recommendations, the Department has put in place manual processes outlined in Licensing Division's internal policies that were updated and effective December 1, 2012.

Beginning December 1, 2012, no later than the 5th of each month, the supervisor assigned to the Maryland Automated Firearms Services System Section, Administrative Unit will compare the number of Applications/Affidavits recorded in the master record that he/she maintains against the number of applicants listed in the record initiated by the Fiscal Accounts Clerk. Note: The master record represents the control account and provides a breakdown for the number of dealer faxes received by the Division. The comparison of the

two records should be exact and the amount of money received should be equal to the number of billable applications.

The results of the monthly reviews are documented by the supervisor assigned to the Maryland Automated Firearms Services System Section, Administrative Unit. A copy of these review summaries will be made available for inspection upon future audits. It should be noted that the record initiated by the Fiscal Accounts Clerk is created so that the supervisor has view access only and does not have the rights or permissions required to enter or edit information.

To ensure collections are properly coded, the Licensing Division Command has provided to each employee and acknowledged receipt of the Program Cost Account (PCA) codes as provided by DSP Finance Division.

Finding 2
Database monitoring, program change controls, and backup procedures over the citation system were inadequate.

Recommendation 2
We recommend that DSP establish adequate controls over the citation system. Specifically, we recommend that DSP

a. enable database logging of direct changes to critical data tables, changes to database security settings, and use of critical system privileges, and that reviews of these logs are performed, documented, and retained for future reference (repeat);
b. create and review comparison reports of program changes prior to moving programs into production status, perform technical reviews of changes for propriety, and ensure that program change reviews and approvals are documented and retained for future reference (repeat); and
c. store backup copies of its citation system database at a secure offsite location.

Agency Response: DSP concurs with the recommendations.

a. The audit trail parameter is set to store the audit log; logging of direct modifications to critical project is enabled; logging of the use of critical system privileges is enabled. Logs will be reviewed by the Section Quality Assurance employee. These processes are documented in internal policies.
b. DSP uses a change control system. The change management process is delineated in internal polices placed into effect in May 2012.
c. Backup copies of the citation database are being moved off site for secure storage.

Finding 3
Critical devices used to secure the DSP network were not operational, or properly administered and monitored.

Recommendation 3
We recommend that DSP

a. evaluate its network security risks and, based on these risks, implement continuous IDPS coverage to effectively protect all critical portions of its network;
b. allow access to the firewalls via only secure protocols, restrict remote access to the firewalls to only network administrators' workstations, and use only unique user accounts to administer the firewalls; and
c. configure the firewalls to send alerts to administrators concerning the devices' operational status, regularly review the firewall logs using an automated process, investigate unusual entries noted during such reviews, and document and retain support for these reviews and investigations for subsequent verification purposes.

Agency Response: DSP concurs with the recommendations.

a. DSP has installed, configured and placed into production the IDPS systems purchased to replace the failed units.
b. DSP has modified the firewalls to allow only secure, authenticated connections. Access is restricted to the system administrators' subnet, and each user can connect only with his/her unique Active Directory login credentials.
c. Firewalls are included in the Department's event and log server configuration so that all logs are electronically stored and monitored and administrators receive alerts regarding operational status. Reviews of these logs are addressed in corresponding internal policies.

Finding 4
Sensitive personally identifiable information was not adequately secured.

Recommendation 4
We recommend that DSP

a. either encrypt the plain text files or remove these files from the host server, and
b. segregate its publicly accessible and non-public servers to help ensure that all non-public servers are adequately protected.

Agency Response:
DSP concurs with the recommendations.

a. Files being transferred to the host server cannot be encrypted as the related application cannot handle encrypted data. Files to be transferred to the host server are moved to a separate staging server in our DMZ and remain there only long enough for the file assembly to be completed, normally minutes. Once assembled, the data is pushed to the two production servers and the local files are automatically deleted from the staging server. This finding is based on the initial load that remained on the host server after the first file transfer. It has since been removed and all subsequent files as noted above are automatically deleted after they have been sent.

b. MSP maintains only one host server for data transfer and that server is maintained in the DMZ and is used ONLY for the data transfer. This server is segregated from the productions servers that are maintained off site.

Equipment

Finding 5
DSP did not establish adequate controls over its equipment.

Recommendation 5
We recommend that DSP comply with the requirements of the Department of General Services' *Inventory Control Manual* (repeat).

Agency Response:
DSP concurs with the recommendations

Effective fiscal year 2013, DSP will maintain a control account for motor vehicles to provide a continuous summary of transactions and a total dollar value control over amounts in the detail records. In addition, DSP has taken the below corrective action to ensure the total value of motor vehicles is reported on the Annual Report of Fixed Assets:

1. Initiate the collection of motor vehicle information, to include, all acquisition and disposal of vehicles due to auction.
2. Create and maintain both the detail record and control account for motor vehicles that include an initial beginning balance ending fiscal year 2012.
3. Conduct an independent reconciliation of the detail records against the control account to ensure to that all motor vehicles are accounted for on a monthly basis.

In fiscal year 2013, DSP will conduct and complete an annual physical inventory for all capital and sensitive items in all locations. These inventories will be reconciled and any resulting discrepancies will be documented and resolved. DSP has already taken steps to ensure that equipment acquisitions and disposals are recorded in the detail equipment records on a timely basis. Included in department procedures is the requirement to conduct an independent review of the FMIS expenditure detail report by program, organization, and fund to identify capital equipment purchases for entry into the detail equipment records on a monthly basis. In addition, the DSP Property Officer will conduct a periodic physical inventory of excess property for disposal at the Quarter Master Division and other locations and schedule the equipment for proper removal from the detail equipment records in accordance with the DGS Inventory Control Manual.

AUDIT TEAM

William R. Smith, CPA
Audit Manager

Richard L. Carter, CISA
Stephen P. Jersey, CPA, CISA
Information Systems Audit Managers

Robert W. Lembach, CPA
Michael J. Murdzak, CPA
Senior Auditors

Edwin L. Paul, CPA, CISA
Albert E. Schmidt, CPA
Information Systems Senior Auditors

Megan A. Axenfeld
Timothy S. Rice
Nathan H. Suffin
Staff Auditors

Eric Alexander, CPA
Jeffrey T. Zankowitz
Information Systems Staff Auditors