DGS

MEMORANDUM

Date: November 18, 2009 File No. 9141

To: Geoff Brandt, State Printer
Office of State Publishing
344 North Seventh Street
Sacramento, CA 95811-0212

From: **Department of General Services**
Office of Audit Services

Subject: **STATE RECORDS CENTER – INFORMATION SECURITY REVIEW**

This report presents the results of our review of the systems of internal control maintained over hard copy media containing confidential, sensitive or personal information that is stored or processed for destruction by the State Records Center (SRC). The SRC's operations are overseen by the Office of State Publishing (OSP). This review was conducted as part of the Office of Audit Services' biennial review of the Department of General Services' (DGS) systems of internal control. Our review was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

As noted on the OSP's website, the Department of General Services (DGS) is statutorily required by Government Code 14767 to provide a facility for the storage, processing and servicing of records. The SRC has been providing State agencies with low-cost storage of records for nearly thirty years. The SRC has evolved into a full service facility, which handles accessions, disposals, rush requests, re-files and vital records vault storage.

The SRC is located in two buildings in West Sacramento. The SRC's total combined storage capacity is 1,058,000 cubic feet, making California's records center the second largest in the nation, second only to the Federal government. The SRC also maintains a Document Destruction Center (DDC), which provides a confidential records destruction service to State agencies. The DDC destroys confidential paper records, microfilm, cassette tapes, magnetic tape and related material by shredding onsite at one of the SRC's buildings.

The objective of our review was to determine the adequacy of the systems of internal control maintained over hard copy media (primarily paper) containing confidential, sensitive or personal information that is stored or processed for destruction by the SRC. The scope of our review primarily involved determining whether sufficient policies and procedures have been implemented to provide reasonable assurance that any hard copy media information assets containing confidential, sensitive or personal information are safeguarded against loss from unauthorized use or disposition. Reasonable assurance is provided when cost-effective actions are taken to restrict deviations to a tolerable level. These actions should result in material errors and improper or illegal acts being prevented or detected and corrected within a timely period by employees in the normal course of performing assigned duties.

Based on the results of our fieldwork that was completed in March 2009, we concluded that the SRC has established adequate systems of internal control over hard copy media containing confidential, sensitive or personal information. The SRC's systems of internal control provide reasonable assurance that hard copy media (primarily paper) under its control is adequately safeguarded in accordance with State and DGS information security requirements. Specifically,

we found that the SRC has implemented sufficient policies and procedures governing the role of its staff in ensuring information security, including the training of employees in their security responsibilities and implementation of procedures which ensure that agency information assets are not accessible to former employees. Further, the SRC has implemented sufficient policies and procedures governing the physical security of its facilities, including controlling the physical access by facility staff and outsiders to information assets that are in storage or being processed for destruction.

It should be noted that during our review we identified areas for improvement with SRC's physical security practices related to its security alarm system and door lock change procedures. Prior to the completion of our audit, we verified that appropriate actions had been or were being taken to improve those practices. Therefore, they are not further discussed in this report.

To determine the adequacy of the systems of internal control for the SRC's records storage and document destruction operations, we reviewed policies and procedures, interviewed parties involved, observed operations and performed other tests as deemed necessary. Our review did not include in-depth effectiveness tests to ascertain whether the control systems were functioning as intended.

Our examination included verifying that the SRC is controlling its information assets in accordance with State Administrative Manual (SAM) Chapter 5300, with our in-depth analysis focused on reviewing compliance with the information security policies contained in SAM Sections 5325 and 5330. SAM Section 5325 is entitled *Human Resources Security* and provides that each State agency is responsible to provide information security roles and responsibilities to its employees, contractors and third party users. SAM Section 5330 is entitled *Physical and Environmental Security* and provides that agencies must take appropriate physical security measures to prevent unauthorized physical access, damage and interruption to its information assets.

Management should be aware that controls cannot prevent all problems because they would not be cost-effective. Moreover, the effectiveness of controls change over time. Limitations which may hinder the effectiveness of an otherwise adequate system of controls include resource constraints, faulty judgments, unintentional errors, circumvention by collusion, and management overrides. The presence of these limitations may not always be detected by an audit.

We greatly appreciated the cooperation and assistance provided by SRC's personnel.

If you need further information or assistance on this report, please contact me at (916) 376-5058, or Gregg Gunderson, Audit Supervisor, at 376-5061.

RICK GILLAM, CPA, CIA
Chief, Office of Audit Services

cc: Scott Harvey, Chief Deputy Director
Rob Cook, Deputy Director, Interagency Support Division
Paul Stangis, Administration Manager, OSP
Danelle Hamilton, Program Manager, OSP
Roman Zeltvay, Manager, SRC
Teresa Soria, Chief Information Security & Privacy Officer, DGS