DGS
GENERAL SERVICES

MEMORANDUM

Date: May 4, 2010 File No. 9142

To: Rob Cook, Acting Deputy Director
Interagency Support Division
707 3rd Street, 8th Floor
West Sacramento, CA 95605

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

Subject: **OFFICE OF FLEET AND ASSET MANAGEMENT – 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 processed and/or stored by the Office of Fleet and Asset Management (OFAM). 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.

In addition to media involving employee personnel activities (such as payroll withholding request forms) that are directly processed by most DGS offices and require safeguarding, the OFAM processes a number of documents which are unique to its operations that contain confidential, sensitive or personal information. For example, the OFAM processes pool vehicle dispatch forms and parking applications that contain notice-triggering personal information. Notice-triggering personal information includes specific items or personal information (such as name plus social security number and/or driver's license number) that may trigger a requirement to notify individuals if it is acquired by an unauthorized person.

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 processed and/or stored by the OFAM. 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 September 2009, we concluded that the OFAM has established adequate systems of internal control over hard copy media containing confidential, sensitive or personal information. The OFAM'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 OFAM has implemented sufficient policies and procedures governing the role of its staff in ensuring information security. Further, the OFAM 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.

To determine the adequacy of the systems of internal control for controlling access to OFAM's information assets, we reviewed policies and procedures, interviewed parties involved, observed operations and performed other tests as deemed necessary. Although the focus of our review was on controls maintained at OFAM's Headquarters, we also visited and evaluated the operations of the Sacramento Garage and the Davis vehicle auction yard. 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 OFAM 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 the OFAM'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 (916) 376-5061.

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

cc: Scott Harvey, Chief Deputy Director
Gary Fujii, Assistant Chief, Administrative and Travel Services, OFAM
Richard Shedd, Assistant Chief, Program Services, OFAM
Teresa Soria, Chief Information Security & Privacy Officer, DGS