STATE ADMINISTRATIVE MANUAL

MANAGEMENT MEMO

	NUMBER: **MM 08-02**
SUBJECT: **RESTRUCTURE OF SAM 4840-4845, CREATION OF NEW SAM SECTIONS 5300-5399, REVISED FORMS AND INSTRUCTIONS**	DATE ISSUED: **FEBRUARY 19, 2008**
	EXPIRES: UNTIL RESCINDED
REFERENCES: STATE ADMINISTRATIVE MANUAL (SAM) 4840-4845: SAM Section 4819.32; Government Code Section 11549.3	ISSUING AGENCY: OFFICE OF INFORMATION SECURITY AND PRIVACY PROTECTION

BACKGROUND AND PURPOSE

The purpose of this Management Memo is to provide the renumbered, restructured sections of SAM and information regarding the Statewide Information Management Manual (SIMM) forms and instructions.

Government Code 11549.3 transfers the responsibility and authority of the State Administrative Manual (SAM) Sections 4840-4845 to the State and Consumer Services Agency, Office of Information Security and Privacy Protection.

SAM Sections 4840-4845 have been restructured to leverage the International Organization for Standardization (ISO) 27002 framework for information security management. These sections have been renumbered to 5300-5399 and the content has been moved to its appropriate new section. No policy additions or changes were made.

Additionally, annual compliance forms (SIMM 70A, 70B, and 70C), the Operational Recovery Plan Documentation for Agencies Preparation Instructions (SIMM 65A), Agency Information Security Incident Notification and Reporting Instructions (SIMM 65B), and Agency Information Security Incident Report (SIMM 65C) have been updated and a new Operational Recovery Plan Transmittal Letter (SIMM 70D) has been added.

POLICY

The changes indicated in the restructure of SAM Sections 4840-4845 will be reflected in the new framework, to be published in the March 2008 timeframe, and renumbered to SAM Sections 5300-5399. The new SAM Sections 5300-5399 will be available under WHAT'S NEW at www.infosecurity.ca.gov until SAM is updated in March.

The restructure includes new language to introduce the new SAM Sections, and some minor edits for clarification; however, no new policy additions or changes have been included.

Attachment A provides a SAM Restructure Cross Reference Sheet that identifies the new SAM structure, the new SAM Section titles, and lists the previous SAM Section(s) where the content was located.

ROLES AND RESPONSIBILITIES

All agencies are required to adhere to these policies. Agencies include all state agencies, departments, offices, boards, commissions, institutions, and special organizational entities unless otherwise specifically exempted by law or state policy, as stated in the new SAM Section 5300.2.

Agencies are responsible to review and update their internal policies to ensure they reflect and incorporate the appropriate SAM Sections of 5300-5399.

Agencies are required to use the updated and new SIMM forms and instructions. Submission of the non-revised forms will not meet the filing requirements and will be returned to the agency.

DESCRIPTION OF SAM RESTRUCTURE AND RENUMBERING, AND SIMM CHANGES

SAM Restructure and Renumbering: The sections of SAM 4840-4845 were moved to the new framework in SAM Sections 5300-5399. No new policy was added; however, introductions to new sections were included to provide an overview of that section. Attachment A is a cross reference of the new sections with a reference to the former sections of SAM. Definitions previously found in SAM Section 4840.4 were removed from SAM and placed on the Office's web site at www.infosecurity.ca.gov.

SAM Section 4841.8, Access to Information by the Legislative Analyst's Office and 4841.9, Access to Information by the California State Auditor have been renumbered to 4804 and 4806, respectively. These sections will remain with the Department of Finance.

SIMM Changes: Agency compliance forms and instructions, and a new transmittal letter for operational recovery plans (ORP) were updated to reflect the name change of the Office, new language for compliance, and new SAM references. The SAM reference changes will be made to the on-line forms; however, the content change on the compliance documents include:

Compliance Forms

The Statewide Information Management Manual (SIMM) forms due to our Office by January 31st of each year include the Agency Designation Letter (SIMM 70A) and the Agency Risk Management and Privacy Program Compliance Certification (SIMM 70C). Below is a brief description of the changes:

Agency Designation Letter (SIMM 70A) - There are three major changes to this form.

1) SAM Section renumbered from 4840-4845 to 5300-5399
2) Agencies must identify support functions they provide to other entities.
3) Agency directors can authorize an individual to sign security-related designations, incident reports, operational recovery plan certifications, and compliance certifications on their behalf.

Agency Risk Management and Privacy Program Compliance Certification (SIMM 70C) - There are three major changes to this form.

1) SAM Section renumbered from 4840-4845 to 5300-5399
2) Revised to inform the signer that the "agency director has ultimate responsibility for information technology security, risk management, and privacy within the agency."
3) Provides for the director or authorized designee to indicate that their agency has implemented a fully developed risk management program or that it has not yet implemented all required components. Agencies indicating they have not yet fully implemented all required components must attach a remediation plan that identifies the components along with a timeline for compliance.

Operational Recovery

The Operational Recovery Plan Documentation for Agencies Preparation Instructions (SIMM 65A) and the Agency Operational Recovery Plan Certification (SIMM 70B) have been updated, and a new form called Agency Operational Recovery Plan Transmittal Letter (SIMM 70D) has been implemented. Below is a brief description of these changes:

Operational Recovery Plan Documentation for Agencies Preparation Instructions (SIMM 65A)

- SAM Section renumbered from 4843, 4843.1, and 4845 to 5355.1, 5355.2, and 5360.1
- Revised to add two new requirements under the Agency Administrative Information (Section 1.0) that are to be included with Plans ***beginning with the July 2008*** submittal (plans due in January and April 2008 do not have to include these two components; however, they will be required in 2009 by all agencies). The two new elements include:
  - Section 1.3 – Agencies must identify other agencies or entities for which they have recovery activity responsibilities.
  - Section 1.5 – Agencies must identify all state agencies that are expected to provide services as part of the recovery activities

Agency Operational Recovery Plan Certification (SIMM 70B)

- SAM Section renumbered from 4843.1 to 5355.2
- This form was updated to indicate that the new Office name is Office of Information Security and Privacy Protection.

Agency Operational Recovery Plan Transmittal Letter (SIMM 70D) (NEW)

- SAM Section renumbered from 4843.1 to 5355.2
- Certifies that the ORP meets the agency needs and must be included when a full ORP is filed with the Office.
- Includes a cross reference sheet, which is only required if an agency's ORP does NOT follow the SIMM 65A format.

Incident Reporting
The Incident Reporting forms have been updated to include the renumbering of the SAM Section and the new Office name. Instructions and forms include:

Agency Information Security Incident Notification and Reporting Instructions (SIMM 65B)
- SAM Section renumbered from 4845 to 5350.2

Agency Information Security Incident Report (SIMM 65C)
- SAM Section renumbered from 4845 to 5350

IMPLEMENTATION, NEXT STEPS, AND CONTACT INFORMATION

The SAM restructure changes are effective immediately with changes to online version of SAM forthcoming.

The two new requirements in the Operational Recovery Plan Documentation for Agencies Preparation Instructions (SIMM 65A) under the Agency Administrative Information (Section 1.0) are to be included with Plans beginning with the **July 2008** Operational Recovery Plan submittal.

Revised Forms and Instructions are available on the Office of Information Security's Web site at www.infosecurity.ca.gov.

Contact the Office of Information Security at (916) 445-5239.

SIGNATURE

Original SAM Management Memo signed by Scott Harvey (Chief Deputy Secretary, Policy and Planning) for Rosario Marin, Secretary State and Consumer Services Agency

Rosario Marin, Secretary
State and Consumer Services Agency

Attachment

ATTACHMENT A
SAM SECTION 5300-5399 CROSS REFERENCE
MM 08-02

*** NEW language added to explain a new section or edit made to clarify; existing policy was not changed.**

New SAM Section	DESCRIPTION	Old SAM Section(s)/ Comments
5300	INTRODUCTION	*NEW Introduction
5300.1	STATUTORY PROVISIONS	*NEW Introduction, 4840.2, and GO RIM description
5300.2	APPLICABILITY	4840.3, 4819.32 (revised)
5300.3	AGENCY RESPONSIBILITIES	4841, 4841.2
5305	RISK MANAGEMENT	4840, 4842
5305.1	RISK ANALYSIS	4842.1
5305.2	AGENCY RISK MANAGEMENT PROGRAM	4842.2
5310	POLICY MANAGEMENT	4840.1, 4841.2, *NEW language added for clarity
5315	ORGANIZING INFORMATION SECURITY	4842.2
5315.1	AGENCY MANAGEMENT RESPONSIBILITIES	4840, 4841.1, 4841.2, *NEW Form added
5315.2	AGENCY DESIGNATIONS	4845, *added Privacy Program Coordinator reference
5320	ASSET PROTECTION	4841.2
5320.1	OWNERSHIP OF INFORMATION	4841.4
5320.2	RESPONSIBILITY OF OWNERS OF INFORMATION	4841.5
5320.3	RESPONSIBILITY OF CUSTODIANS OF INFORMATION	4841.6
5320.4	RESPONSIBILITY OF USERS OF INFORMATION	4841.7
5320.5	CLASSIFICATION OF INFORMATION	4841.3
5325	HUMAN RESOURCES SECURITY	4842.2
5330	PHYSICAL AND ENVIRONMENTAL SECURITY	4842.2
5335	COMMUNICATIONS AND OPERATIONS MANAGEMENT	*NEW Introduction
5335.1	INFORMATION INTEGRITY AND DATA SECURITY	4841.2, 4842.2
5335.2	PERSONAL COMPUTER SECURITY	4842.2
5340	ACCESS CONTROL	*NEW Introduction, 4841.2
5345	INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT,	*NEW Introduction

New SAM Section	DESCRIPTION	Old SAM Section(s)/ Comments
	AND MAINTENANCE	
5345.1	SOFTWARE LICENSING INTEGRITY	4842.2
5345.2	CRYPTOGRAPHY	4841.2
5350	INCIDENT MANAGEMENT	4841.2, 4845
5350.1	INFORMATION SECURITY INCIDENT REPORTING REQUIREMENTS	4845
5350.2	CRITERIA FOR REPORTING INCIDENTS	4845
5350.3	INCIDENT FOLLOW-UP REPORT	4845
5355	DISASTER RECOVERY MANAGEMENT	*NEW Introduction, 4842.2
5355.1	OPERATIONAL RECOVERY PLANNING	4843
5355.2	AGENCY OPERATIONAL RECOVERY PLAN	4843.1, *NEW Form added
5355.3	ADDITIONAL STATE DATA CENTER REQUIREMENTS	4842.2, 4842.21
5360	COMPLIANCE	*NEW Introduction, 4845
5360.1	COMPLIANCE SUMMARY	4845