CALIFORNIA DEPARTMENT OF TECHNOLOGY NUMBER: DATE ISSUED:

Procedures/Standards Update

PS006_2019 **December 2019**

TO:
Chief Information Officers (CIO)
Information Security Officers (ISO)
Agency Chief Information Officers (AIO)
Agency Information Security Officers (AISO)

SUBJECT: **MINIMIUM SECURITY LEVELS**

BACKGROUND

State Administrative Manual (SAM) Chapter 5300 was updated in late 2013 to reaffirm the adoption of Federal Information Processing Standards (FIPS) with direct reference to supporting the National Institute of Standards and Technology (NIST) Special Publications (SP), including NIST SP 800-53. These standards promote the implementation of higher authority policies contained in the SAM.

Many of the NIST SP 800-53 security controls reference a variable labeled <*Organization-Defined*>; for which the entity is expected to select a value that is appropriate for the organization and its risk management strategy. As part of a more comprehensive risk management strategy, the state has determined that a minimum security level value was needed for some of the NIST SP 800-53 security controls. To standardize these values across state entities, the Information Security Advisory Committee (ISAC) membership surveyed security industry best-practices and their representative entities; seeking consensus of the minimum values.

The California Department of Technology (CDT), Office of Information Security (OIS) has developed the State-Defined Security Parameters for NIST SP 800-53 Controls. This policy sets minimum security levels and provides state entities specific direction for specifying organization-defined values referenced in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. Agencies/state entities must continue to categorize information systems in accordance with FIPS Publication 199, and document categorization with appropriate rationale.

Effective immediately, Agencies/state entities must implement the minimum security control levels specified in the State-Defined Security Parameters for NIST SP 800-53 Controls (SIMM 5300-A) and appropriate for the categorization. Agencies/state entities may tailor above SIMM 5300-A standards. Any exceptions or variations tailoring below these standards must be documented and supported by the state entity variance policy and risk assessment process outlined in SAM 5305.7, and Plan of Action and Milestones (POAM) when applicable.

PURPOSE

The purpose of this Procedures/Standards update is to announce:

- Updated SAM Section 5300.5
- New SIMM Section 5300-A

SIMM 5300-A contains detailed security control content and classified as confidential. Therefore, it will be available to designated personnel listed on SIMM 5330-A at OIS Extranet (Agency.Net). Vendor access will only be provided under Non-Disclosure Agreement during state entity

procurement processes. State entity procurement officials should consult with their designated Information Security Officers or Agency Information Security Officers about vendor access and SIMM 5300-A information handling protocols.

SAM/SIMM REFERENCES

The following reference materials are associated with this procedures/standards update. This SIMM is available to authorized Designees on the Department of Technology's, OIS Extranet (Agency.Net). The State Administrative Manual (SAM) is available on the Department of General Services website located at: http://sam.dgs.ca.gov/.

- SAM Section 5300.5
- SIMM Section 5300-A

QUESTIONS

Questions regarding this announcement should be directed to the Department of Technology, Office of Information Security at security@state.ca.gov.