CALIFORNIA DEPARTMENT OF TECHNOLOGY | NUMBER: | DATE ISSUED:

Procedures/Standards Update

PS014_2021 | **May 2021**

TO:

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

SUBJECT:

California Cybersecurity Maturity Metrics and State-Defined Security Parameters for NIST SP 800-53 Controls

BACKGROUND

The California Department of Technology (CDT) Office of Information Security (OIS) developed the California Cybersecurity Maturity Metrics (SIMM 5300-C) to establish the requirements to objectively measure the effectiveness of each Agency/state entity's cybersecurity program and promote better efficiencies, visibility, and decision-making. To further support information security objectives, OIS updated the California Cybersecurity Maturity Metrics to realign the information sources for five sub-categories to work more effectively with OIS Audit programs and the Independent Security Assessment (ISA).

CDT OIS additionally developed and adopted The State-Defined Security Parameters for NIST SP 800-53 Controls (SIMM 5300-A) in December 2019. 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. Additionally, SIMM 5300-A includes cross reference to current ISA parameters and scoring protocols.

PURPOSE

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

- Revised SIMM Section 5300-C, California Cybersecurity Maturity Metrics (CMM) which provides updates based on California Military Department (CMD) Independent Security Assessment (ISA) (Phase-II) Assessment Criteria v5.0.1 changes, as well as reformatting for document accessibility. The CMD revisions renumbered their ISA tasks and updated control references to specific sub-control references, where applicable, and did not change any ISA parameters or scoring protocols.
- Revised SIMM Section 5300-A, State-Defined Security Parameters for NIST SP 800-53 Controls to address CMD ISA (Phase-II) Assessment Criteria v5.0.1 changes.

Information Security Assessment, Audit and Maturity scores are confidential and are exempt from public disclosure per Government Code 6254.19. 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.

REFERENCES

The following reference materials are associated with this procedures/standards update. SIMM and Technology Letter is available on the CDT's website located at https://cdt.ca.gov/policy/simm/ and https://cdt.ca.gov/policy/technology-letters/. SAM is available on the Department of General Services' website located at https://www.dgs.ca.gov/Resources/SAM/TOC.

- SIMM 5300-C
- SIMM 5300-A
- Technology Letter TL 18-01

QUESTIONS

Direct questions regarding this announcement to the Department of Technology, Office of Information Security at security@state.ca.gov.