

Procedures/Standards Update

PS011_2021

January 2021

TO:

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

SUBJECT:

Vulnerability Management Standard

BACKGROUND

The California Department of Technology's (CDT's) Office of Information Security (OIS) has developed the Vulnerability Management standard (SIMM 5345-A) document. This procedure/standard introduces required minimum vulnerability management standards. Effective immediately, state entities must ensure that vulnerability management technologies and processes used for their organization(s) include the protection, detection, investigative support, containment, and remediation capabilities outlined in SIMM 5345-A. If a state entity has already acquired or implemented a solution, which does not currently meet this standard, the state entity must identify the deficiency and remediation plan for correcting the deficiency on refresh in its next Plan of Action and Milestones (POAM) submission.

PURPOSE

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

- Updated SAM Section 5345 to include reference to the new Vulnerability Management Standard (SIMM 5345-A).
- New SIMM Section 5345-A, which includes the protection, detection, investigative support, containment, and remediation capabilities.

REFERENCES

The following reference materials are associated with this Procedures/Standards update. SIMM is available on the Department of Technology's website located at <https://cdt.ca.gov/policy/simm/>. SAM is available on the Department of General Services' website located at <https://www.dgs.ca.gov/Resources/SAM>.

- SAM Section 5345
- SIMM Section 5345-A

QUESTIONS

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