

Policy/Guidelines Update

PG004_2019

January 2019

TO:

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

SUBJECT:

Endpoint Protection Standard

BACKGROUND

The California Department of Technology (CDT) Office of Information Security (OIS) has developed the Endpoint Protection Standard (SIMM 5355-A). This policy introduces required minimum endpoint protection standards as part of a defense in depth security strategy. Effective immediately, Agencies/state entities must ensure that endpoints for their respective organization(s) include the endpoint protections outlined in SIMM Section 5355-A. If an Agency/state entity has already acquired or implemented a solution that does not currently meet this standard, the Agency/state entity must identify the deficiency and include a remediation plan in its next Plan of Action and Milestones (POAM) submission.

PURPOSE

The purpose of this Policy/Guidelines Update is to announce:

- New SIMM Section 5355-A Endpoint Protection Standard which includes minimum requirements for endpoint protection.
- Updated SAM Section 5355 Endpoint Defense to include reference to Endpoint Protection Standard (SIMM 5355-A).

REFERENCES

The following reference materials are associated with this policy/guideline update. Statewide Information Management Manual (SIMM) is available on CDT's website. The State Administrative Manual (SAM) is available on the Department of General Services website.

- SAM Section 5355
- SIMM Section 5355-A

QUESTIONS

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