State of California

Department of Technology

Email Threat Protection Standard

Statewide Information Management Manual – 5315-A

May 2026

Table of Contents

Revision History

Revision	Date of Release	Owner	Summary of Changes
Initial release	October 2018	Office of Information Security (OIS)	Initial release
Minor update	January 2025	OIS	Template update and additional protection capabilities added.
Minor update	March 2025	OIS	Update references to FIPS 140-3, update NIST CSF categories
Minor Update	May 2026	OIS	Update requirements on auto-forwarding

Introduction

Purpose

This standard supports State Administrative Manual (SAM) section 5315, Information Security Integration. State entities must ensure that email services for their organization(s) include the email threat protections included in this standard.

Scope

This standard applies to all California State Entities as defined in State Administrative Manual (SAM) 5300.4.

Compliance

As outlined in Government Code (GC) Section 11549.3, the California Department of Technology's (CDT) Office of Information Security (OIS) is entrusted with creating, issuing, and maintaining policies, standards, and procedures, overseeing information security risk management for agencies and state entities, providing information security and privacy guidance, and ensuring compliance with SAM Chapter 5300 and Statewide Information Management Manual (SIMM) section 5300.

State entities must adhere to CDT-issued information security and privacy policies and all relevant laws, regulations, rules, and standards governing their state entity. Compliance may be reflected in audit findings and maturity scores. Non-compliance will be addressed according to the Office of Information Security Policy Compliance and Enforcement Standard (SIMM 5330-H).

As described in GC Section 11549.3.(f) (2), a state agency as defined in GC Section 11000 that is not under the direct authority of the Governor may adopt and implement this policy voluntarily. Such a state agency may discontinue use of this policy at any time.

Minimum Email Threat Protections

At a minimum, the email solution used by state entities shall include the following protection, detection, investigative support, containment, and remediation capabilities. State entities are encouraged to set additional standards as applicable to their business and risk mitigation needs. Examples of additional standards that may be needed are included in Section III of this standard.

Protection Capabilities

The email solution used by state entities shall (at a minimum):

1. Use the Domain-based Message Authentication, Reporting & Conformance (DMARC) authentication and policy enforcement protocol to implement appropriate levels of protection via the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) protections.
2. Adjust SPF records from Soft Fail to Hard Fail.
3. Use vendor provided threat intelligence to inform all aspects of protections provided.
4. Provide email “spoofing” protections that detect if internal or external domains are being spoofed.
5. Implement domain reputation protections.
6. Provide email encryption on demand by entity email users to protect emails containing confidential, sensitive, and/or personal information when required by policy or law. (Encryption methods shall comply with SAM Section 5350.1, SIMM Sections 5305-A and 5360-A, and FIPS 140-3 validated algorithms and modules.)
7. Protect remote access sessions using multi-factor authentication in compliance to SIMM 5360-C.
8. Ensure all email operations, mail stores, and administration activity reside within the continental U.S.

9. Provide data loss protection (DLP) capabilities on outbound email to detect and prevent confidential, sensitive and/or personal information, as defined by business/data owners, from being externally transmitted.

10. Turn off external auto-forwarding rules by default. Exceptions must be approved by entity ISO. When exceptions are granted, periodically review exceptions and spot-check forwarded messages to ensure they are being sent only to authorized addresses (e.g. .gov domains) and that such addresses do not show indications of compromise. Where auto-forwarding exceptions have been allowed, DLP should be used as with all outbound email.

11. Add a notification banner to all inbound email sourcing from and external domain.

12. Apply Domain Name System (DNS) filtering.

13. Adjust link settings to limit who a link can be shared with by establishing a zero-trust framework based on Role Based Access Control (RBAC).

Detection Capabilities

Detection capabilities include machine learning and analytics, application behavior violations, and the validation of internally or externally discovered indicators of compromise (IOCs). Ideally, the solution used will combine alerts into events and prioritize incidents, based on detection confidence level, severity and risk, and prioritize the response activities. At a minimum, the solution used will:

1. Screen all emails against spam, phishing, and malicious intent using heuristics and intelligent learning techniques to quarantine likely malicious and phishing emails.
2. Screen all email attachments using malware analysis, sandbox, and intelligent learning techniques to block malicious attachments including zero-day from delivery.
3. Screen all links contained in email messages to determine that the URL to which the link is targeted is deemed “safe to visit” based on the time of click reputation

and analysis of the target site and/or downloadable content, informing users of unsafe links or blocking access thereto.

Investigative Support Capabilities

The investigative support function shall include the ability to search the entire email store for specific emails or emails that contain specific indicators and provide that list of emails to administrators for further actions if/as needed.

The solution used should also:

1. Provide “logs” of all security related actions (including but not limited to malicious email detections, spam/phishing detections, malicious attachment detections, URL link clicks, DLP hits, etc.) to an entity designated Security Information and Event Management (SIEM) system.
2. Pass pertinent threat information, as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) SP 800-150, to the California Department of Technology.
3. Provide a rich reporting environment that allows for deep investigation message tracing and summarization, including tracking of all URL link clicks in emails.

In further support of investigative capabilities, all state entities should:

1. Establish and maintain an email address for use by the State Security Operations Center (SOC) to notify impacted entities of anomalies and suspected or confirmed incidents.
2. Ensure the email address follows the standardized naming convention of

   “[*Entity Acronym*].SOC.Notifications@[*domain*].ca.gov”

   Example: CDT.SOC.Notifications@state.ca.gov
3. Ensure all individuals who need to acknowledge receipt of a SOC notification within a 2-hour period are included as contacts in the group email address.
4. Provide timely supplemental investigative findings to the SOC.

Containment Capabilities

The system should be capable of manually or automatically quarantining and/or removing emails that are deemed malicious or dangerous in a timely fashion.

Remediation Capabilities

The system should be capable of implementing custom filtering of incoming emails to screen previously detected malicious emails.

Examples of Capabilities Above Minimum Threat Protections

Additional email threat protections which may be needed by state entities include, but are not limited to, the ability to:

- Provision users for remote access to email (by individuals and groups).
- Enforce who can send to group email lists, for example an external entity should not be able to use an entity's internal distribution list.
- Support specific state entity acceptable use policies and standards.

NIST CSF Function and Category

Function	Category
Identify	• ID.AM Asset Management
Protect	• PR.AA Identity Management, Authentication, and Access Control • PR.DS Data Security • PR.PS Platform Security
Detect	• DE.AE Adverse Event Analysis • DE.CM Continuous Monitoring
Respond	• RS.MA Incident Management • RS.CO Incident Response Reporting and Communication • RS.MI Incident Mitigation

References

- Domain-based Message Authentication, Reporting & Conformance (DMARC): https://dmarc.org/
- FIPS 140-3, Security Requirements for Cryptographic Modules: https://csrc.nist.gov/pubs/fips/140-3/final
- SP 800-150, Guide to Cyber Threat Information Sharing: https://csrc.nist.gov/pubs/sp/800/150/final
- State Administrative Manual (SAM) 5300: https://www.dgs.ca.gov/en/Resources/SAM/TOC/5300
- Statewide Information Management Manual (SIMM) 5300: https://cdt.ca.gov/policy/simm/

Questions

Questions regarding the implementation of this standard may be sent to:

California Department of Technology

Office of Information Security

security@state.ca.gov