State of California

California Department of Technology

Office of Information Security

Email Threat Protection Standard

SIMM 5315-A

October 2018

REVISION HISTORY

REVISION	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Release	**October 2018**	**California Information Security Office**	**New Standard in support of SAM Section 5315, Information Security Integration**

TABLE OF CONTENTS

I. INTRODUCTION

State entities must ensure that email services for their organization(s) include the email threat protections included in this standard.

II. MINIMUM EMAIL THREAT PROTECTIONS

At a minimum the email solution used by state entities must 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.

A. 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 (see https:/dmarc.org) to implement appropriate levels of protection via the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) protections.
2. Use vendor provided threat intelligence to inform all aspects of protections provided.
3. Provide email "spoofing" protections that detect if internal or external domains are being spoofed.
4. Implement domain reputation protections.
5. 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[1].
6. Protect remote access sessions using multi-factor authentication.
7. Ensure all email operations, mail stores, and administration activity reside within the continental U.S.
8. 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.

B. 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] Encryption methods shall comply with SAM Section 5350.1, SIMM Sections 5305-A and 5360-A, and FIPS 140-2 validated algorithms and modules.

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 both 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 time of click reputation and analysis of target site and/or downloadable content, informing users of unsafe links or blocking access thereto.

C. Investigative Support Capabilities

The investigative support function must 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 must 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 must:

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 needed 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.

D. Containment Capabilities

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

E. Remediation Capabilities

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

III. 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 individual 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.

IV. QUESTIONS

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

California Department of Technology
Office of Information Security
Security@state.ca.gov