State of California

California Department of Technology

Office of Information Security

Security Event Notification and Response Standard

SIMM 5335-A

March 2021

REVISION HISTORY

REVISION	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Release	**March 2021**	**California Information Security Office**	**New Standard in support of SAM Sections 5335, Information Security Monitoring, and 5345, Vulnerability Management and Threat Management.**

TABLE OF CONTENTS

I. INTRODUCTION

Each Agency/state entity is responsible for continuous monitoring of its networks and other information assets for vulnerabilities and signs of attack, anomalies, and suspicious or inappropriate activities. Agencies/state entities shall continuously identify, investigate reports of, and remediate vulnerabilities affecting their information technology (IT) assets before they can be exploited. (SAM Sections 5335, 5335.1 and 5335.2). The California Department of Technology (CDT) Office of Information Security (OIS), Security Operation Center (SOC), provides continuous monitoring of the California Government Enterprise Network (CGEN) and will notify customers when it detects security events.

II. DEFINITIONS

Security Event

An observable occurrence in a network or system, such as a detected vulnerability, or observed signs of attack, anomalies, and suspicious or inappropriate activities.

Incident

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Threat

A circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation.

Vulnerability

A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

III. PROCESS AND PROCEDURES

SOC continuous monitoring and critical notification processes require a timely exchange for the benefit of all parties. Agencies/state entities shall employ the SIMM 5335-A protocols in response to Security Event Notifications (SENs).

A. Security Operations Center Security Event Notification Process

Step 1

The SOC will assess events triggered from its monitoring tools, assign a confidence level, and create a security event notification (SEN) record in the California Compliance and Security Incident Reporting System (Cal-CSIRS). Cal-CSIRS will send an email notification to the impacted Agency/state entity with the corresponding SEN record number.

Step 2
For all Critical and High events, the SOC analyst will also attempt to reach one of the designees (ISO, CIO, AISO or their backup) by telephone until all telephone numbers provided on the Designation Letter (SIMM 5330-A) have been exhausted.

Step 3
The notified Agency/state entity will login to and use Cal-CSIRS, within the response timeframes specified in Section III, sub-section D to:

a. acknowledge receipt of the SEN;
b. investigate to determine if the event is a confirmed vulnerability or incident, or a false positive, and communicate its findings to the SOC;
c. report confirmed incidents in the California Compliance and Security Incident Reporting System (Cal-CSIRS), and associate the Cal-CSIRS incident record with the corresponding SEN record;
d. provide determination details. Detailed information about how the Agency/state entity makes its determination are needed to tune the tools, prevent additional false positives, and allow the SOC to take proactive measures on behalf of the entity in future events. The notified Agency/state entity may request SOC assistance with making a determination.
e. work with the OIS, California Highway Patrol (CHP), and California Cybersecurity Integration Center (Cal-CSIC) as necessary and in accordance with Incident Reporting and Response Instructions (SIMM 5340-A), and Requirements to Respond to Incidents Involving a Breach of Personal Information (SIMM 5340-C) to investigate and resolve incidents and associated corrective action plans to prevent recurrence in a timely manner.

Figure 1 below is an illustration of the SOC SEN Workflow Process as described in Section III, sub-section A above.

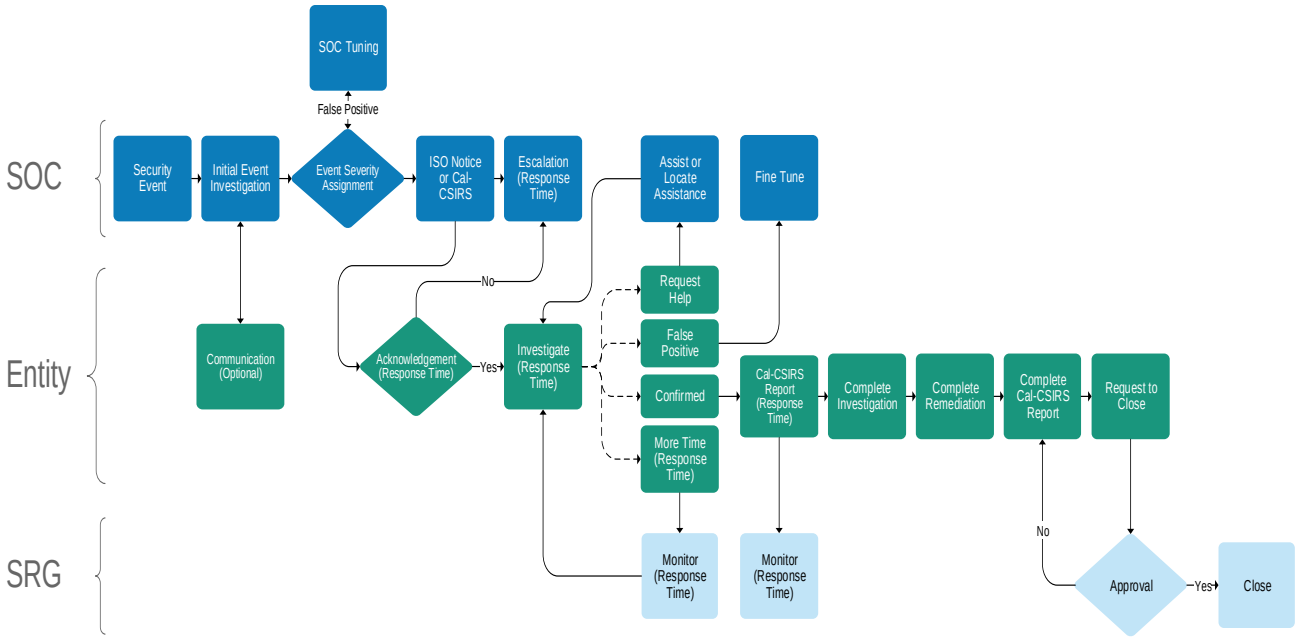

Figure 1 - Illustration of the SOC SEN Workflow Process.

B. Event Levels

A level is assigned to each SEN by SOC analysts to communicate the importance of the SEN; **NOT incident severity/impact**. The assigned level is to help the recipient entity understand how fast they need to respond to the SEN. The levels are Critical (Red), High (Orange), and Medium (Yellow). Table 1 below provides the criteria used to assign levels and examples for each:

Event Level	Criteria Used to Assign Level and Examples
Critical (Red)	**Exceptional events observed with 100% level of confidence of inbound and outbound attack traffic, traffic beaconing out, exfiltration of data, malicious payload, detonation of payload, ransomware.** **Example: Early signs of Ransomware events, such as an asset observed trying to reach a Domain Controller and/or file shares, or lateral movements associated with establishing elevated privileges.**
High (Orange)	**Observed with a very high level of confidence indicators of compromise (IOCs), such as inbound attack traffic typically associated with malicious and successful attacks, but SOC unable to determine if entity has its own line of defense in place to block or stop attack.** **Example: An Active Distributed Denial of Service (DDoS) attack, but SOC is unaware of entity's layered defense.**
Medium (Yellow)	**Observed vulnerabilities with imminent threat and very high level of confidence they can and will be exploited if not remediated. Do not yet see inbound attack traffic.** **Example: Meltdown Spectre or Emotet vulnerabilities**

Table 1 – Event levels, the criteria used to assign levels and examples for each.

C. Investigative Support Capabilities

Agencies/state entities must have internal incident response and recovery plans (SAM Sections 5340 and 5325.1) and be able to support investigative response and recovery activities when needed. The CHP, OIS, and Cal-CSIC coordinate with each other and the reporting Agencies/state entities during response activities, but may not be able to provide investigative and forensic assistance for all events.

D. Response Timeframes

The established response timeframes are described as follows:

1. The targeted maximum total response timeframe for a Critical (Red) level SEN is three and one-half (3.5) hours comprised as follows:
    a. **one (1) clock hour** from the time an initial SEN was sent to an Agency/state entity to acknowledge receipt of the SEN; and
    b. **two (2) clock hours** from the time a SEN is acknowledged to make a false positive or confirmed incident determination, unless requested help or more time needed is provided; and
    c. **thirty (30) clock minutes** from the time a positive determination is made to create the Cal-CSIRS incident record and associate it with the corresponding SEN record.

2. The targeted maximum total response timeframe for a High (Orange) level SEN is seven (7) business hours comprised as follows:
    a. **two (2) business hours** from the time an initial SEN was sent to an Agency/state entity to acknowledge receipt of the SEN; and
    b. **four (4) business hours** from the time a SEN is acknowledged to make a false positive or confirmed incident determination, or help or more time needed is provided; and
    c. **one (1) business hour** from the time a positive determination is made to create the Cal-CSIRS incident record and associate it with the corresponding SEN record.

3. The targeted maximum total response timeframe for a Medium (Yellow) level SEN is eight (8) business hours comprised as follows:
    a. **two (2) business hours** from the time an initial SEN was sent to an Agency/state entity to acknowledge receipt of the SEN; and
    b. **four (4) business hours** from the time a SEN is acknowledged to make a false positive or confirmed incident determination, or help or more time needed is provided; and
    c. **two (2) business hours** from the time a positive determination is made to create the Cal-CSIRS incident record and associate it with the corresponding SEN record.

Figure 2, on the following page is an illustration of the response timeframes for Critical (Red), High (Orange), and Medium (Yellow) level SENs as described in Section III, sub-section D above.

Timeframe for Acknowledgement			Timeframe for Determination			Timeframe for Cal-CSIRS Reporting			Timeframe for Completing All	
From the time an initial notification was sent an Entity Acknowledges Initial SEN Notification (Email or Cal-CSIRSSEN) Within…		Plus (+)	From the time the Entity acknowledges the initial SEN Entity Makes Determination as Positive, False Positive, or Help or More Time Needed Within…		Plus (+)	From the time, a Positive determination is made Entity Opens a Cal-CSIRS Incident Report Within…		Equals (=)	Entity Maximum Time Target	
Critical (Red)	1 Clock hours	Plus (+)	Critical	2 Clock hours	Plus (+)	Critical	30 Clock minutes	Plus (+)	Critical	3.5 Clock hours
High (Orange)	2 Business hours	Plus (+)	High	4 Business hours	Plus (+)	High	1 Business hour	Plus (+)	High	7 Business hours
Medium (Yellow)	2 Business hours	Plus (+)	Medium	4 Business hours	Plus (+)	Medium	2 Business hours	Plus (+)	Medium	8 Business hours

Figure 2 - Illustration of the Security Event Notification response timeframes.

E. SEN Notification Format and Distribution Protocols

For all Critical and High level events, the SOC Analyst will attempt to reach one of the designees (ISO, CIO, AISO or their backup) by telephone until contact is made or telephone numbers provided on the Designation Letter (SIMM 5330-A) for those individuals have been exhausted. Telephone messages will be left when there is an option of leaving a message. In addition, an email will be sent.

The SEN email subject line format will include the assigned level, such as:

> SUBJECT: Cal-CSIRS Notification: A Security Event Notification – SOC-[0123] requires your attention. The SEN Level is: [CRITICAL]

Table 2 on the following page illustrates the telephone notification and distribution protocols by each SEN level as described in Section III, sub-section E above.

Level	From	Initial SEN (Order of Telephone Attempts to Reach Live Person)	Initial SEN (Email) Distribution
Critical (Red)	**SOC Analyst**	1. Designated entity ISO; 2. Designated entity backup ISO; 3. Designated entity CIO; 4. Designated entity backup CIO; and 5. Designated AISO. 6. Designated entity backup AISO.	1. Designated entity ISO; 2. Designated entity backup ISO; and 3. Entity established SOC notify group email address.
High (Orange)	**SOC Analyst**	1. Designated entity ISO; 2. Designated entity backup ISO.	1. Designated entity ISO; 2. Designated entity backup ISO; and 3. Entity established SOC notify group email address.
Medium (Yellow)	**SOC Analyst**	1. Designated entity ISO; and *2.* Designated entity backup ISO.	1. Designated entity ISO; 2. Designated entity backup ISO; and 3. Entity established SOC notify group email address.

Table 2 – Illustrates the telephone notification and distribution protocols for each SEN level.

F. Agency/State Entity SEN Acknowledgement/Response Format and Distribution Protocols

Agency/state entities shall acknowledge receipt of SEN and provide investigative findings within timeframes specified in Section III, sub-section D. The entity's acknowledgement and response within the Cal-CSIRS SEN record will include the below information. Information in between brackets ([]) and in italicized font will be provided by Agency/state entity as applicable to each SEN.

- Risk known by entity and remediation [*Planned or in progress*] and will be completed by [Specify date].
- Risk known by Agency/state entity and remediation completed on [*specify date*].
- Receipt of SEN acknowledged, and Agency/state entity is investigating. Agency/state entity will provide status or investigative findings by [*Specify additional timeframe needed to complete investigation when additional time is requested.*].
- Confirmed unknown risk and the following mitigating actions were taken: [*Specify actions taken – e.g., firewall or IPS now blocking.*].
- Confirmed incident report created in Cal-CSIRS and Cal-CSIRS incident record is associated with the corresponding SEN record. [*Specify details of findings and upload any relevant materials that will assist with alerting and mitigating future attacks against others, e.g., email headers and content, system logs, etc.*].

  Confirmed false positive. [*Specify information about the permitted activity and/or environmental factors that generated the false positive*].

Unless otherwise instructed by OIS, the Agency/state entity will use the Cal-CSIRS SEN and Computer Incident Report (CIR) record data fields, workflow buttons, and workflow notes to acknowledge, confirm and report SEN findings. Cal-CSIRS User Guide and training are provided to the Agency/state entity's designated Cal-CSIRS users.

G. Escalation Protocols

1. Escalation Levels and Notifications

When no response is received from the Agency/state entity within the established timeframes, the SEN will be escalated. The first level is escalated to the Statewide Incident Program Manager (SIPM). The second level is escalated to the State Chief Information Security Officer (CISO) and State Deputy CISO. The third level is escalated to the State Chief Information Officer (CIO) and State Deputy CIO.

For all Critical and High level events the Statewide Incident Program Manager (SIPM) will attempt to reach one of the designated individuals or their backup by telephone until contact is made or all telephone numbers provided on the Designation Letter (SIMM 5330-A) have been exhausted. Telephone messages will be left when there is an option of leaving a message. In addition, Cal-CSIRs auto-generated or manually generated emails will be sent.

Table 3 on the following page outlines the three levels of escalation and protocols for distribution of notifications, as described in Section G., sub-section 1 above, when no response is received within established timeframes.

Level	Email From	Email To	Telephone Call/Message To	Email Copies Distributed To
1	**Cal-CSIRS or SOC Analyst**	**Statewide Incident Program Manager (SIPM)**	1. Designated entity ISO; 2. Designated entity backup ISO; 3. Designated entity CIO; and 4. Designated entity backup CIO.	1. Designated entity ISO; 2. Designated entity backup ISO; 3. Entity established SOC notify group email address 4. Designated entity CIO; and 5. Designated entity backup *CIO.*
2	**Cal-CSIRS or SIPM**	**State Deputy CISO / State CISO**	1. Designated entity ISO; 2. Designated entity backup ISO; 3. Designated entity CIO; 4. Designated entity backup CIO; and 5. Designated AISO 6. Designated backup AISO	1. Designated entity ISO; 2. Designated entity backup ISO; 3. Entity established SOC notify group email address Designated entity CIO; and 4. Designated entity backup CIO. 5. Designated AISO 6. Designated backup AISO
3	**Cal-CSIRS or State Deputy CISO / State CISO**	**State Deputy CIO / State CIO**	1. Designated entity ISO; 2. Designated entity backup ISO; 3. Designated entity CIO; 4. Designated entity backup CIO; 5. Designated AISO and Designated AIO 6. Designated backup AISO and Designated backup AIO	1. Designated entity ISO; 2. Designated entity backup ISO; 3. Entity established SOC notify group email address Designated entity CIO; and 4. Designated entity backup CIO. 5. Designated AISO and 6. Designated AIO. 7. Designated backup AISO and designated backup AIO.

Table 3 – Illustrates the notification and distribution protocols for each Escalation level.

2. Escalation Timeframes

The escalation timeframes for SENs labeled Critical (Red) are described below.

a. For no Initial Acknowledgement escalation will be made as follows:
   i. After 1 clock hour for first level escalation (Level 1)
   ii. After 2.5 clock hours for second level escalation (Level 2)
   iii. After 3 clock hours for third level escalation (Level 3)

b. For no Entity Determination escalation will be made as follows:
   i. After 2 clock hours for first level escalation (Level 1)
   ii. After 2.5 clock hours for second level escalation (Level 2)
   iii. After 3 clock hours for third level escalation (Level 3)

c. For no Entity Cal-CSIRS Incident Report associated to Cal-CSIRS SEN record escalation will be made as follows:
    i. After 30 clock minutes for first level escalation (Level 1)
    ii. After 1 clock hour for second level escalation (Level 2)
    iii. After 3 clock hours for third level escalation (Level 3)

The escalation timeframes for SENs labeled High (Orange) are described below.

a. For no Initial Acknowledgement escalation will be made as follows:
    i. After 2 clock hours for first level escalation (Level 1)
    ii. After 2.5 clock hours for second level escalation (Level 2)
    iii. After 3 clock hours for third level escalation (Level 3)

b. For no Entity Determination escalation will be made as follows:
    i. After 4 clock hours for first level escalation (Level 1)
    ii. After 4.5 clock hours for second level escalation (Level 2)
    iii. After 5 clock hours for third level escalation (Level 3)

c. For no Entity Cal-CSIRS Incident Report associated to Cal-CSIRS SEN record escalation will be made as follows:
    i. After 1 clock hour for first level escalation (Level 1)
    ii. After 1.5 clock hours for second level escalation (Level 2)
    iii. After 2 clock hours for third level escalation (Level 3)

The escalation timeframes for SENs labeled Medium (Yellow) are described below.

a. For no Initial Acknowledgement escalation will be made as follows:
    i. After 2 clock hours for first level escalation (Level 1)
    ii. After 2.5 clock hours for second level escalation (Level 2)
    iii. After 3 clock hours for third level escalation (Level 3)

b. For no Entity Determination escalation will be made as follows:
    i. After 4 clock hours for first level escalation (Level 1)
    ii. After 4.5 clock hours for second level escalation (Level 2)
    iii. After 5 clock hours for third level escalation (Level 3)

c. For no Entity Cal-CSIRS Incident Report associated to Cal-CSIRS SEN record escalation will be made as follows:
    i. After 2 clock hours for first level escalation (Level 1)
    ii. After 2.5 clock hour for second level escalation (Level 2)
    iii. After 3 clock hours for third level escalation (Level 3)

The escalation timeframes described in Section G., Sub-section 2 above are illustrated in Figure 4 on the following page.

Escalation	Initial Acknowledgement			Entity Determination			Entity Cal-CSIRS Report		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
Critical (Red)	After 1 Clock hours	After 2.5 Clock hours	After 3 Clock hours	After 2 Clock hours	After 2.5 Clock hours	After 3 Clock hours	After 30 minutes	After 1 Clock hour	After 3 Clock hours
High (Orange)	After 2 Business hours	After 2.5 Business hours	After 3 Business hours	After 4 Business hours	After 4.5 Business hours	After 5 Business hours	After 1 Business hour	After 1.5 Business hours	After 2 Business hours
Medium (Yellow)	After 2 Business hours	After 2.5 Business hours	After 3 Business hours	After 4 Business hours	After 4.5 Business hours	After 5 Business hours	After 2 Business hours	After 2.5 Business hours	After 3 Business hours

Figure 4 – Illustration of escalation timeframes.

H. Remediation Capabilities

Agencies/state entities must be able to support timely remediation and implementation of mitigation measures when vulnerabilities are detected before they can be exploited. (SAM Sections 5335, 5335.1, and 5345)

IV. QUESTIONS

Questions regarding this standard may be sent to:

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