State of California

Department of Technology

Phishing Exercise Standard

Statewide Information Management Manual – 5320-A

June 2025

Table of Contents

Document History 2

Introduction 3

Purpose 3

Scope 3

Compliance 3

Definitions 4

Simulated Phishing Exercises 4

Exercise Planning 4

Acquiring Products and Services for Exercise Simulation 5

Validation of Domain Name 5

Plan Elements 5

Exercise Metrics and Reports 7

Required Approvals and Advanced Notifications 8

Relationship to Incident Reporting and Response Lifecycle 9

NIST CSF Function and Category 10

References 10

Document History

Revision	Date of Release	Owner	Summary of Changes
v.1	October 2020	Office of Information Security (OIS)	New Standard in support of SAM Section 5320
v.2	November 2021	OIS	Provided additional phishing techniques and exercise planning coordination requirements.
v.3	June 2025	OIS	Aligned plan elements with SIMM 5300-A, updated format, removed items related to general phishing and not the simulated phishing exercise plan, removed OIS and Cal-CSIC approval requirement for phishing exercises.

Introduction

Purpose

Protecting the California state government from malicious social engineering attacks requires technical measures and awareness from an information security and privacy-focused workforce. Regular simulated phishing exercises provide a valuable way to assess personnel security and privacy awareness and their ability to identify, respond to, and report phishing attempts.

This Phishing Exercise Standard supports State Administrative Manual (SAM) 5320 by establishing specific requirements for state entities to coordinate simulated phishing exercises with the California Cybersecurity Integration Center (Cal-CSIC) and other requirements for execution.

Scope

This standard applies to all California state entities, including agencies, departments, divisions, bureaus, boards, and commissions, as defined in Government Code (GC) Section 11546.1.

Compliance

As outlined in GC Section 11549.3, the Office of Information Security (OIS) is entrusted with creating, issuing, and maintaining policies, standards, and procedures, overseeing information security risk management for 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 OIS-issued information security and privacy policies and all relevant laws, regulations, rules, and standards governing their agency or 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).

Definitions

Phishing: A digital form of social engineering that uses authentic looking but bogus emails to request information from users or direct them to a fake website that requests information.

Social Engineering: The act of exploiting human behavior and emotions, rather than using technical methods, to bypass security measures and deceive an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust.

Simulated Phishing Exercises

Simulated phishing exercises serve as a protective measure focused on individuals to help safeguard against phishing attacks. As outlined in SAM 5320 - Training and Awareness for Information Security and Privacy, these simulations are crucial for awareness and training and essential to a mature information security program. They can reveal departmental vulnerabilities and highlight the need for further security and awareness training to prevent future phishing attempts.

Regular simulated phishing exercises allow state entities to assess personnel's understanding of social engineering techniques and their ability to mitigate potential threats. To ensure their effectiveness, these exercises should be thoughtfully designed to reflect realistic scenarios and mimic communications and content that personnel are likely to encounter, incorporating relevant personal or environmental factors. These exercises aim to simulate the collection of personal, sensitive, or confidential information that, if exploited, could result in harm or loss for the state entity or its individuals.

Exercise Planning

State entities must have a documented simulated phishing exercise plan and policy that outlines their exercise requirements that also aligns with SIMM 5300-A, State-Defined Security Parameters for NIST SP 800-53.

Acquiring Products and Services for Phishing Exercise Simulation

When conducting phishing exercises, using another entity's logos, trademarks, or domains in the phishing templates may lead to legal action for trademark or copyright infringement. Some third-party security & awareness training vendors attempt to remove liability by scraping images from the internet for the use of their templates. Additionally, some vendors transfer liability to the state entity through disclaimers.

If state entities choose to use pre-made vendor templates, they must work with their internal legal department to understand the risks associated with third-party logos, trademarks, or domains to reduce liability. State entities should not send out any phishing campaigns that they are uncomfortable defending.

State entities should inform personnel, either in a phishing exercise policy communicated to personnel or on a page displayed following a phishing exercise, that any third-party logos, trademarks, and domains used in the phishing exercise are for training purposes only and, as such, constitute fair use.

Validation of Domain Name

Ownership of all domain names must be validated for the proposed phishing campaign templates by conducting a domain lookup on the ICANN website using https://lookup.icann.org/ to help prevent ownership disputes. Ownership of ca.gov domain names must be validated using https://domainnamerequest.cdt.ca.gov/ before using them in proposed phishing campaign templates. Refer to SAM Sections 5195 and 5195.1 for the Internet Domain Name Policy and Requirements.

Plan Elements

State entities are responsible for developing and executing phishing simulation exercise plans. If a state entity receives a security boundary from another state entity, as defined in their SIMM 5330-A Designation Letters, the entity providing the security boundary must also provide phishing simulation exercises.

The state entity's Information Security Officer (ISO) shall collaborate with their Human Resources (HR) and Legal departments, and their Agency Information Security Officer

(AISO), to develop and implement phishing simulation exercises that align with organizational policies, workforce considerations, and risk management strategies. This partnership ensures that phishing awareness initiatives are conducted in an ethical, effective, and legally compliant manner, mitigating potential risks such as personnel stress, privacy concerns, and legal implications. Phishing campaigns must not violate workplace policies, labor laws, or union agreements such as creating undue anxiety by falsely implying disciplinary actions, financial repercussions, or personal consequences. In situations where a state entity provides a security boundary to another state entity, that entity is also responsible for coordinating with the Legal and HR department of both entities to ensure appropriate phishing exercises are provided to the state entity receiving service.

The following elements must be included in the state entity's Phishing simulation exercise plan:

- Use of fictional state entity name(s), brand/logo(s), image(s), etc. State entities may mockup or use vendor-provided templates and logos that closely resemble a legitimate brand or logo.
- Pre- and post- Phishing exercise steps to control and properly manage the Phishing exercise must be documented and followed to prevent unauthorized disclosure, minimize unintended risks, and ensure that test emails do not persist beyond their intended purpose. Exercise steps include:
    - Implement email containment and restrictions.
    - Enforce access and distribution controls.
    - Coordinate IT efforts and whitelist approved domains.
    - Remove and clean up unauthorized emails.
    - Ensure data protection and privacy compliance.
    - Monitor for post-incident misuse and security breaches.
    - Conduct a thorough post-test review.
- Prepare pre- and post- Phishing exercise communication messages and protocols. This includes reinforcing the information and instructions personnel will receive from awareness training, such as looking for poor grammar and typos.

- Phishing campaign content must not contain inappropriate material, other state entity names or logos, or union names or logos without express written consent from those entities.
- Adaptive learning features, which include artificial intelligence systems that learn and personalize phishing exercises based on personnel's user history, must be enabled for phishing simulations to ensure tailored exercises are provided to individual personnel, if applicable.
- Domain blocks must be configured to prevent test emails from being forwarded outside the state entity.
- Design phishing simulations that closely mimic the style of communications personnel commonly encounter, accurately reflecting the real threats personnel are likely to face or experience.
- State entities must implement a continuous monitoring approach for phishing simulations, ensuring that all personnel participate in Phishing exercises at least once per quarter. State entities have the discretion to determine how to distribute, segment and schedule these Phishing exercises, so long as they achieve full personnel participation within the quarter. It is recommended that exercises and align with learner groups by functional role, with a role-based approach to distribute to minimize impact to day-to-day business activities and processes.
- Phishing exercise cadence should align with the organization's risk appetite and maturity, with adaptive learning enabled to strengthen awareness. Personnel who consistently fail to meet baseline passing standards should receive targeted training to reinforce awareness and mitigate vulnerabilities.

Phishing Exercise Metrics and Reports

State entities must develop key performance indicators (KPIs) and performance thresholds to measure phishing exercise effectiveness. These thresholds and metrics must align with the Phishing Practical Exercise scoring criteria in SIMM 5300-A, State-Defined Security Parameters for NIST SP 800-53.

Metrics must be tracked during a simulated phishing exercise, and a summary report should be created to assess the campaign and compare its effectiveness over time. Reports shall remain easily accessible as they may be requested during an audit.

Personnel who fail to reach the minimum baseline threshold determined by the state entity shall be required to undergo additional training.

Report metrics include but are not limited to the following:

- Total number and percentage of personnel who opened the email.
- Total number and percentage of personnel who clicked on a link within the email.
- Total number and percentage of personnel who clicked on the button see a response.
- Total number and percentage of personnel who entered credentials on the phishing site.
- Total number and percentage of personnel who ran the malicious payload delivered via the phishing site.
- Total number and percentage of personnel who provided sensitive information during the exercise.

Required Approvals and Advanced Notifications

Prior to conducting phishing exercises, coordination must take place with state oversight entities and all potentially impacted organizations. The following are the required approvals and notifications that must be obtained and made before launching a phishing exercise.

- Obtain written approval before using the names or logos of other unions, government organizations, or state entities.
- Obtain written approval from the Information Security Officer (ISO) or Chief Information Officer (CIO) before scheduling any simulated phishing exercise.
- At least 72 hours (three business days) before an exercise, notify Cal-CSIC via email at CalCSIC.SecurityAlerts@caloes.ca.gov. The 72-hour (three business days) advanced notification must include ISO or CIO approval and a copy of the phishing email and date of distribution, including the email header. Do not initiate a phishing exercise without

providing the required 72-hour (three business days) advance notification to Cal-CSIC.

Relationship to Incident Reporting and Response Lifecycle

State entities must plan for phishing incidents and have appropriate response plans and playbooks. These plans must comply with SAM 5340, Information Security Incident Management, SIMM 5340-A – Incident Reporting and Response, and SIMM 5340-C – Requirements to Respond to Incidents Involving a Breach of Personal Information.

Effective phishing incident response requires careful planning, organization, training, and systematic procedures. Plans for incident response during simulated phishing exercises must include preparation for an incident, detection, analysis, containment, eradication, recovery, and application of lessons learned.

Phishing attacks must have an associated playbook and be included in every state entity's incident response plan.

All successful phishing attacks must be reported in California Compliance and Security Incident Reporting System (CAL-CSIRS). However, phishing simulations conducted internally by the state entity for workforce training purposes are not considered successful phishing attacks and should not be reported in CAL-CSIRS.

NIST CSF Function and Category

Function	Category
Govern	Organizational Context (GV.OC) Oversight (GV.OV) Policy (GV.PO)
Identify	Risk Assessment (ID.RA) Improvement (ID.IM)
Protect	Awareness and Training (PR.AT) Data Security (PR.DS)
Detect	Adverse Event Analysis (DE.AE) Continuous Monitoring (DE.CM)
Respond	Incident Management (RS.MA Incident Analysis (RS.AN) Incident Mitigation (RS.MI)
Recover	Incident Recovery Communication (RC.CO)

References

ICANN Domain Lookup: https://lookup.icann.org/

Ownership validation of CA.gov domains: https://domainnamerequest.cdt.ca.gov/

NIST Cybersecurity Framework 2.0: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

State Administration Manual (SAM) Information Technology - Office of Information Security: https://www.dgs.ca.gov/Resources/SAM/TOC/5300

Statewide Information Management Manual (SIMM): https://cdt.ca.gov/policy/simm/