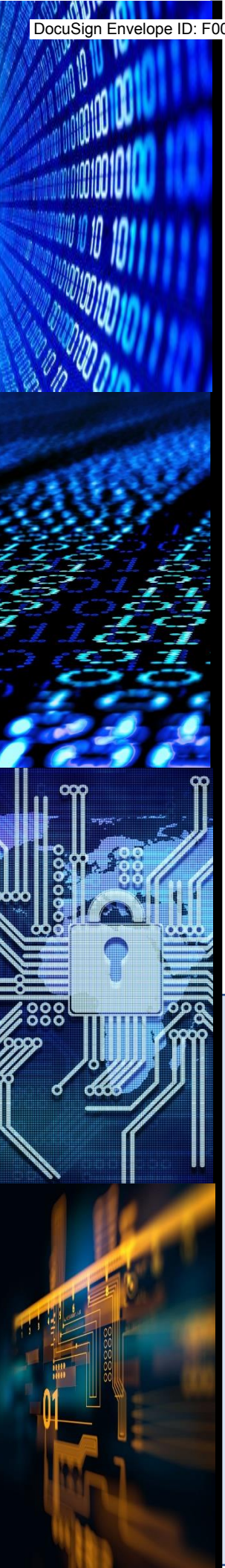


CALIFORNIA
STATE AND LOCAL CYBERSECURITY GRANT PROGRAM
CALIFORNIA CYBERSECURITY PLAN

September 2023

Approved by California Cybersecurity Task Force on 20 September 2023
Version 1.5.5

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LETTER FROM CALIFORNIA CYBERSECURITY TASK FORCE

Greetings,

The California Cybersecurity Task Force is pleased to present to you the 2023 California Cybersecurity Plan as required by the State and Local Cybersecurity Grant Program (SLGCP). The Cybersecurity Plan outlines the vision, mission, goals, and objectives for California. The Cybersecurity Plan also serves as an annex to the broader California Homeland Security Strategy and represents the state's latest step in its continued commitment to improving cybersecurity across California at the state, tribal, and local levels.

Representatives from the California Cybersecurity Task Force Cybersecurity Investment Planning Subcommittee collaborated to develop the Cybersecurity Plan with actionable and measurable goals and objectives that have champions identified to ensure completion. These goals and objectives focus on governance, personnel, planning and technology. They are designed to support our state in adopting new technologies and navigating the ever-changing cybersecurity landscape. They also incorporate the SLCGP required plan elements.

As we continue to enhance cybersecurity, we must remain dedicated to improving our resilience among disciplines and across jurisdictional boundaries. With help from cybersecurity practitioners, we will work to achieve the goals set forth in the Cybersecurity Plan and become a model for cybersecurity, preparedness, and resilience.

Sincerely,

DocuSigned by:
Liana Bailey-Crimmins
1CB8A3C6D0D54CA...

Liana Bailey-Crimmins Director and Chief Information Officer and Co-Chair of Cybersecurity Planning Committee
California Department of Technology

DocuSigned by:
Nancy Ward
3E94DD66F24F422...

Nancy Ward
Director and Co-Chair of Cybersecurity Planning Committee
California Governor's Office of Emergency Services

INTRODUCTION

The Cybersecurity Plan is a three-year strategic planning document required by the U.S. Department of Homeland Security's State and Local Cybersecurity Grant Program (SLGCP) that contains the following components:

- **Vision and Mission**: Articulates the vision and mission for improving cybersecurity resilience interoperability over the next one-to-three-years.
- **Organization, and Roles and Responsibilities:** Describes the current roles and responsibilities, and any governance mechanisms for cybersecurity within California as well as successes, challenges, and priorities for improvement. This also includes a strategy for the cybersecurity program and the organization structure that identifies how the cybersecurity program is supported. In addition, this section includes governance that identifies authorities and requirements of California's cybersecurity program. The Cybersecurity Plan is a guiding document and does not create any authority or direction over any of California's or local systems or agencies.
- **How feedback and input from local governments and associations was incorporated.** Describes how inputs from local governments are used to reduce overall cybersecurity risk across the eligible entity. This is especially important in developing a holistic cybersecurity plan.
- **Cybersecurity Plan Elements:** Outlines technology and operations needed to maintain and enhance resilience across the cybersecurity landscape.
- **Funding:** Describes funding sources and allocations to build cybersecurity capabilities within California along with methods and strategies for funding sustainment and enhancement to meet long-term goals.
- **Implementation Plan:** Describes California's plan to implement, maintain, and update the Cybersecurity Plan to enable continued evolution of and progress toward the identified goals. The implementation plan must include the resources and timeline where practicable.
- **Metrics:** Describes how California will measure the outputs and outcomes of the program across the state.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework[1], included in Figure 1, helps guide key decision points about risk management activities through various levels of an organization from senior executives to business and process level, as well as implementation and operations. The NIST Framework played a significant role in designing and developing this plan.

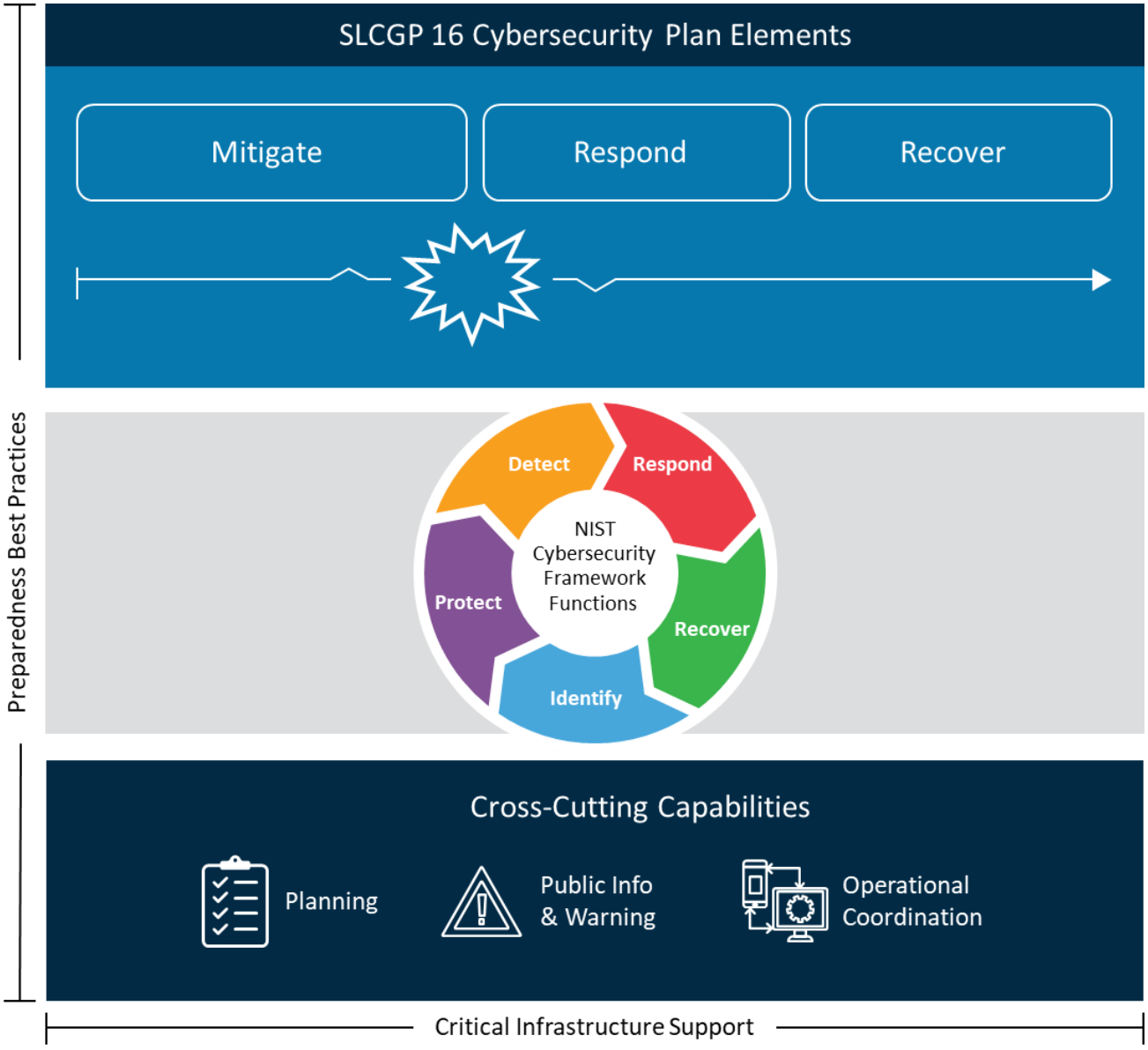


Figure 1: Achieving Cyber Resilience Through Comprehensive Cybersecurity Plans

[1] https://www.nist.gov/cyberframework/getting-started

Vision and Mission

This section describes California's vision and mission for improving cybersecurity:

Vision:

To enhance and mature cybersecurity capability throughout California by improving people, process, and technology.

Mission:

Reduce the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public and private sector computer networks. Use a risk-based approach to best utilize SLCGP funds to address cybersecurity gaps uniquely identified and prioritized by California's state, local, and tribal government agencies.

Cybersecurity Program Goals and Objectives

California's Cybersecurity goals and objectives include the following.

California Cybersecurity Program
Goal 1: Develop and establish baseline governance structures across California's jurisdictions, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
Objective 1.1: Help establish cybersecurity governance structures across jurisdictions and assist with implementation of cybersecurity programs within each jurisdiction to evaluate cybersecurity maturity of existing programs in alignment with Cybersecurity Performance Goals established by CISA and standards set by the National Institute of Standards and Technology (NIST).
Objective 1.2: Develop, implement, or revise, and test cybersecurity plans across jurisdictions, including cyber incident response plans, with clearly defined roles and responsibilities.
Objective 1.3: Prioritize asset (e.g., devices, data, software) protections and recovery actions across the state based on each asset's criticality and business value.
Goal 2: Government jurisdictions across California understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
Objective 2.1: Physical devices and systems, and software platforms and applications, operated by government or on behalf of government are inventoried across California.

Objective 2.2: Each jurisdiction across California understands and documents cybersecurity risk to their operations and assets.
Objective 2.3: Each jurisdiction across California has the capacity to conduct vulnerability scans and can develop and implement a risk-based vulnerability management plan.
Objective 2.4: Across jurisdictions in California, capabilities are in place to monitor assets to identify cyber incidents.
Objective 2.5: Processes are in place to take corrective action based on insights derived from deployed capabilities (e.g., SIEM systems, endpoint detection and monitoring, vulnerability scans/assessments, incident response findings, etc.).

Goal 3: Implement highest priority cybersecurity protections commensurate with risk across California's government jurisdictions.
Objective 3.1: Jurisdictions across California adopt fundamental cybersecurity best practices, at least to the Initial stage of the CISA Zero Trust Maturity Model (Version 2.0) or the "Tier 2: Risk Informed" implementation tier of the NIST Framework for Improving Critical Infrastructure Cybersecurity, as applicable.
Objective 3.2: Jurisdictions can reduce gaps identified through an assessment and planning process and apply increasingly sophisticated security protections commensurate with risk.
Objective 3.3: Create and operationalize a portfolio of cybersecurity as-a-service offerings at the state level, i.e., security operations center services, to address gaps in a cost-effective manner.

Goal 4: Develop and unify California's diverse, innovative cybersecurity workforce to safeguard the data and systems used across jurisdictions to deliver public services.
Objective 4.1: Personnel across jurisdictions and job categories are appropriately trained in cybersecurity necessary to recognize and respond to cybersecurity risks and understand their roles and responsibilities within established cybersecurity policies, procedures, and practices.
Objective 4.2: California jurisdictions adopt the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.
Objective 4.3: Better align each jurisdiction's workforce with current and future cybersecurity needs by updating cybersecurity talent models and career paths to include cybersecurity job roles, job categories, knowledge, skills, and abilities.
Objective 4.4: Build and expand partnerships with educational institutions and private industry to create a diverse pipeline of cybersecurity professionals seeking careers in public service.

CYBERSECURITY PLAN ELEMENTS

This Cybersecurity Plan incorporates elements from the following California plans. The Cybersecurity Plan builds upon those elements and includes data and information from the cybersecurity capability assessment and gap analysis required by the SLGCP.

- Cal-Secure Roadmap - California Department of Technology and California Cybersecurity Integration Center[2]
- California Homeland Security Strategy Goal 3: Strengthen Security and Preparedness across Cyberspace[3]
- California Emergency Support Function 18[4] (ESF-18)

Manage, Monitor, and Track

California's strategy for managing, monitoring, and tracking information systems, applications, and user accounts will encompass security control assessment, security status monitoring, and security status reporting in support of timely risk-based decision making throughout organizations across the state. This will include developing governance, risk management, privacy, and compliance programs across state and local agencies and jurisdictions to ensure formal processes and documented programs are in place. For example, agencies and jurisdictions will build and sustain capabilities to find and filter out actionable information that is valuable in data protection efforts to detect and investigate suspicious user activity, while maintaining appropriate user privacy. Special attention will be given to any systems and technology that are no longer supported by the manufacturer to effectively protect, detect, respond to, and recover from cybersecurity threats targeting those legacy systems.

For state government systems, state agencies will seek to implement SIMM 5300 and work closely with the Department of Technology Office of Information Security to ensure they are aware of the latest standards.

Both state agencies and local governments will be aware of CISA's Cross-Sector Cybersecurity Performance Goals and the NIST Cybersecurity Framework to understand the basis of state standards and provide guidelines where SIMM guidance is not applicable or not specified.

Monitor, Audit, and Track

At present, each state entity is responsible for continuous monitoring of its networks and other information assets for signs of attack, anomalies, and suspicious or inappropriate activities. Going forward, California will implement a behavioral anomaly detection strategy that will involve the continuous monitoring of state and local networks and systems for unusual events or trends. This will involve looking in real-time for evidence of compromise, rather than for the cyberattack itself. This early detection of potential cybersecurity incidents will be key to helping reduce the impact of these cyber incidents on state and local networks and systems.

State agencies and local governments will be encouraged to request services from the CDT SOC and the Cal-CSIC to provide or supplement monitoring and tracking of network traffic. Likewise, the California

[2] See Cal-Secure at https://cdt.ca.gov/wp-content/uploads/2021/10/Cybersecurity_Strategy_Plan_FINAL.pdf
[3] See 2021-2024 California Homeland Security Strategy Executive Summary
[4] See California Emergency Support Function 18 - Cybersecurity

Military Department provides Independent Security Assessments which may be provided at no cost to some agencies.

All agencies will be encouraged to identify gaps in this area and reach out to the Cal-CSIC, CDT, and/or CISA if they are unsure how to initiate plans for improving monitoring, auditing, and tracking of network traffic and activity.

Enhance Preparedness

California will approach securing cyberspace as a whole community, and whole of government responsibility, not just an information technology sector duty. This approach will emphasize people and procedures, as much as equipment and software. The state recognizes that cyberspace operates both independently and interactively with the physical world, and therefore requires a broad set of capabilities that function seamlessly in both environments. Securing cyberspace across California will involve all facets of preparedness (prevention, protection, mitigation, response, and recovery), and requires multiple Core Capabilities, beyond just "cybersecurity," to ensure the functionality, security, and resiliency of cyberspace.

California will build and sustain resources to integrate capabilities to the extent possible through planning, organization building, equipment acquisitions, training of personnel at all levels and responsibilities, and exercises to test and evaluate the whole community's ability to secure cyberspace. This will include building the state's capacity to collectively respond to cyber incidents through the following:

- Conducting cybersecurity awareness training and exercises, and coordinating through the Cal-CSIC to increase awareness about cyber hygiene and best practices
- Conducting cybersecurity training and exercises to continuously validate planning concepts and operations
- Establishing and maintaining working relationships with local, county, state, federal, and commercial entities to support the improvement of state response capabilities and improve coordination
- Monitoring information and potential threats using multiple information pathways (e.g., open-source intelligence, coordination with fusion centers)
- Conducting cyclical analysis of risk to assess and achieve operational benchmarks
- Overseeing the implementation of processes to mitigate against the impacts of cyber incidents, including, but not limited to:
    - Performing recurring data backup
    - Maintaining off-site data storage
    - Maintaining awareness of alternate facilities and information
    - Performing security device configuration reviews
    - Continuously reviewing networks and services policies and procedures
- Developing and revising incident handling and reporting plans, protocols, and policies on a continuous basis, and subsequently publicizing those changes with relevant audiences
- Identifying resources to support incident preparedness, response, and recovery and training stakeholders on available resources
- Maintaining and updating all local, county, tribal, state, federal, and commercial contact lists and test contact methods on at least a quarterly basis
- Maintaining and training cyber incident response teams
- Increase local government access to and participation in regional cybersecurity exercises

Assessment and Mitigation

Protecting every aspect of cyberspace is impossible, and the importance of assets and systems varies; sometimes dramatically. To that end, California will focus on identifying high value assets consistent with Federal Information Processing Standard (FIPS) 199 by giving special consideration to the capability, intent, and specific targeting of high value information systems by potential or actual adversaries. Given the differences in cyber risk and risk tolerance at the local, tribal, and state levels, one-size-fits-all security measures will be less effective than risk-based solutions that can be tailored.

California's risk management strategy will be built around reducing the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of its information, and/or information systems. The state's risk management approach will be centered on the NIST Cyber Security Framework's (CSF's) risk management tiers. The tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives.

Mitigation activities related to cybersecurity and information technology will be undertaken to reduce the likelihood or impact of a cyber incident. These mitigation activities include conducting policy workshops, technical testing, information sharing, threat assessment, risk analysis and alerting, penetration testing, control assessments, and gap analysis. Cal OES will ensure that emergency functions are integrated in mitigation plans and activities including cyber and will provide information to emergency functions regarding mitigation activities relevant to their core functions.

State agencies and local governments will be encouraged to request assessment and mitigation services from the CDT SOC and the Cal-CSIC to provide or supplement continuous cybersecurity vulnerability assessments and threat mitigation practices. Likewise, the California Military Department provides Independent Security Assessments which may be provided at no cost (aside from any SLCGP funding) to some agencies.

Best Practices and Methodologies

In 2021 the California Department of Technology (CDT) and its Office of Information Security (OIS) released Cal-Secure, the California Executive Branch's first five-year information security maturity roadmap. The roadmap was created through a collaborative process with the California Cybersecurity Integration Center (Cal-CSIC) and its four critical partners: the California Governor's Office of Emergency Services (Cal OES), California Highway Patrol (CHP), California Department of Technology (CDT), and California Military Department (CMD) and the state government security community. It is built on industry-leading best practices and frameworks and addresses critical gaps in the state's information and cybersecurity programs. The roadmap is intended to outline capabilities the State must adopt and achieve in a prioritized fashion. The end goal of this roadmap is to ensure California's Executive branch has a world-class cybersecurity workforce, an empowered and right-sized federated cybersecurity oversight governance structure, and effective cybersecurity defenses for all technology including critical infrastructure.

The California Homeland Security Strategy (HSS) has established the goal of Strengthen Security and Preparedness across Cyberspace. The core tenets of Cal-Secure are based upon the key objectives of the California HSS and provide California's executive branch a roadmap to prioritize their contributions to help California reach its goals resulting in the increase of security maturity levels. Cal-Secure is broken into three roadmap categories – people, process, and technology, which the executive branch will focus on throughout the next five years to improve its cybersecurity maturity and identify and manage risks to the state. This plan outlines success measures that the state will achieve upon completion of the Cal-Secure objectives. Each category is equally important to achieve in order to ensure the success of the five-year plan. To achieve these goals, Cal-Secure identifies nine key priorities (three per roadmap category) and 15

forward- leaning initiatives. Another core aspect of Cal-Secure is the multi-year Horizon Map which provides an actionable and prioritized sequence for each Cal-Secure initiative and baseline cybersecurity capability required by state entities. Each capability will shift closer in the timeline depending on risk situations and current maturity levels of departments. At the close of each fiscal year, entities will be required to attest that they have achieved the required capabilities and OIS will provide an update on the implementation status of Cal-Secure initiatives.

California state law enacted in 2023 requires all state agencies to adopt and implement information security and privacy policies, standards, and procedures based upon standards issued by the National Institute of Standards and Technology and the Federal Information Processing Standards, as specified (includes: NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations[5]; FIPS 199 Standards for Security Categorization of Federal Information and Information Systems[6]; FIPS 200 Minimum Security Requirements for Federal Information and Information Systems[7]). State agencies are required to perform a comprehensive, independent security assessment every two years and they are authorized to contract with the Military Department, or with a qualified responsible vendor, for that purpose. State agencies are required to certify annually to the state legislature that the agency is in compliance with all adopted policies, standards, and procedures and to include a plan of action and milestones, as specified. State agencies under the oversight of Office of Information Security within the Department of Technology are under more stringent standards specified in the Statewide Information Management Manual (SIMM) section 5300 Information Security. While local governments are not required to apply SIMM 5300 standards, they are encouraged to make use of this guidance where it is helpful.

Cal Secure and SIMM 5300 correspondence with the SLCGP cybersecurity best practices is shown in the following table:

SLCGP Cybersecurity Best Practice	Cal Secure	SIMM 5300
Implement multi-factor authentication	MFA is Phase 1 technology priority	SIMM 5360-C & SIMM 5360-D
Implement enhanced logging	Inherent in multiple phases, including key initiative to implement Unified Integrated Risk Management platform	SIMM 5300-C
Data encryption for data at rest and in transit	Enterprise encryption is a Phase 5 technology priority	SIMM 5300-C
End use of unsupported/end of life software and hardware that are accessible from the Internet	Integration of cybersecurity into the state's IT Modernization Roadmap of legacy systems is a key initiative	SIMM 5300-C

[5] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
[6] https://csrc.nist.gov/pubs/fips/199/final
[7] https://csrc.nist.gov/pubs/fips/200/final

Prohibit use of known/fixed/default passwords and credentials	Existing state standard but goes further with Enterprise Sign-On and multiple initiatives to ensure more effective monitoring and enforcement	SIMM 5300-C
Ensure the ability to reconstitute systems (backups)	Inherent in multiple initiatives, derived from Homeland Security Strategy to ensure continuity of critical systems	SIMM 5300-C & SIMM 5325-A
Migration to the .gov internet domain	While not specified as a strictly cybersecurity service, it is part of CDT's active service portfolio	Not strictly a focus of SIMM 5300, but is addressed in State Administrative Manual (SAM) 5195.1 & 5195.2

NIST Principles

California will use the NIST Cybersecurity Framework's business drivers to guide cybersecurity activities while helping entities across the state consider cybersecurity risks as part of their risk management processes. This will include the following.

- Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- Develop and implement the appropriate safeguards to ensure delivery of mission critical services.
- Develop and implement the appropriate activities to identify the occurrence of a cyber incident.
- Develop and implement the appropriate activities to take action regarding a detected cyber incident.
- Develop and implement the appropriate activities to maintain plans for resilience, and to restore any capabilities or services that were impaired due to a cyber incident.

Supply Chain Risk Management

California will engage in a coordinated effort to build trusted relationships and communicate with internal and external stakeholders to enhance supply chain security. Consistent with NIST guidelines, the state's cyber supply chain risk management (C-SCRM) activities will include identifying and assessing risks, determining appropriate risk response actions, developing C-SCRM plans at the state and local level to document response actions, and monitoring performance against those plans. Because supply chains can differ significantly across and within organizations in a state as large and diverse as California, C-SCRM plans will be tailored to the individual program, organizational, and operational contexts of state and local agencies and jurisdictions.

Tools and Tactics

California will engage its State Threat Assessment System and partnerships with CISA, U.S. Secret Service, FBI, Multi-State Information Sharing and Analysis Center (MS-ISAC), and others to continuously gain knowledge and share information on cyber adversary tools, tactics, and techniques. This will include regular engagements to share information and experiences, as well as deploying actual tools to facilitate a

more in depth understanding of adversary tactics, techniques, and procedures through malicious code analysis, etc.

Specifically regarding MS-ISAC services, California has significant engagement but this can be increased:

- Counties, Election/Voter Offices (City & County Included) are 100% enrolled
- Public Utility Districts (Energy & Water) are 100% enrolled
- 45.9% of Cities are not fully subscribed to DHS-CISA/CISecurity/MS-ISAC Services
- 51.5% of School Districts are not fully subscribed
- 78.2% of Tribal Governments are not fully subscribed, and there are 81 additional groups seeking federal recognition]
- 93.9% of Special Districts are not fully subscribed

Safe Online Services

Californians share their personal information, data, and resources with their government. They must be confident that the government will keep their information private and secure, and that the government will steward their resources, preventing fraud and abuse. Delivering options for a common approach to identity verification and authentication is at early stages and requires significant work to understand the public's needs and expectations for privacy and security, how and when government shares information, transparency about information and information sharing, and informed consent.

To that end, California will strive to deliver easy-to-use, fast, dependable, and secure public services, ensure public services are equitable and inclusive, make common technology easy to access, use, and reuse across levels of government, and build digital government more quickly and more effectively. For example, among those jurisdictions eligible to receive funds under the SLCGP who have not previously migrated to the .gov domain, one approach under consideration is a managed service to assist with this migration beyond the basic setup and hosting services already provided. Where they have not yet or migration is not feasible at this time, local governments will ensure relevant NIST standards are adhered to, CISA guidelines are followed, and useful components of state SIMM 5300 are applied. Where insufficient resources are an obstacle, local governments will identify these shortfalls to their state legislature representatives, the Cal-CSIC, and CISA.

Continuity of Operations

The State of California will provide guidance to local and tribal entities for developing continuity plans. This guidance will be broadly applicable to continuity after any hazard but can be applied to cybersecurity. The California Continuity Planning Guidance and Plan Template posted on the Cal OES website provides direction to state agencies and departments in developing their continuity plans and programs. The planning resources and tools included in this program can be used whether an organization is starting from the very beginning of the planning process or merely updating plans already in place. To ensure capability in all the key planning element areas, a Continuity Plan Evaluation Checklist has been created and included in the Continuity Planning Guide. The Continuity Plan Evaluation Checklist is a self-certification that has been developed to help maintain a continuity plan that reflects the most current state/federal continuity planning standards. The Checklist documents the organization's Continuity Program and Plan status.

Workforce

California has been a leader in resource typing of personnel and equipment for decades and will employ a similar approach and strategy to implementing the NICE Workforce Framework across the state. California will take a proactive approach across levels of government to develop consistent yet flexible job roles, job categories, knowledge, skills, and abilities standards for the cyber workforce; increase opportunities to source cybersecurity talent; and increase training opportunities for existing staff. To achieve this, additional investments and new partnerships must be developed throughout the coming years. At the state level, for example, California will develop a "one government" approach that brings together key stakeholders across California's executive branch. The Department of Technology provides a Cybersecurity Boot Camp and Information Security Leadership Academy and has partnered with other state agencies in the state's "Work For California" program to streamline hiring, particularly for those with technology skills or aptitude.

Finally, the California Cybersecurity Task Force Workforce Development and Education Subcommittee (CCTF WDE) has been formulating numerous initiatives to improve California's cybersecurity workforce, including K-12 and college-level training, as well as certificate and degree programs. The CCTF CIPS and WDE subcommittees will continue to align these efforts with the NICE Workforce Framework and develop innovative solutions to address the states cybersecurity workforce gaps.

Two pathway approaches to cybersecurity professional preparation and development (for hiring, advancement, and retention) developed by the CCTF WDE Subcommittee include:

1. Traditional- (i.e., academic-K-12, degrees, certificates, industry recognized certifications; and workforce opportunities like internships and pre/registered apprenticeships programs).
2. Non-traditional (i.e., non-academic education program, microcredentials, industry recognized certifications; and workforce opportunities like internships & pre/registered apprenticeship programs).

Articulating and championing these approaches will help ensure development and implementation of an "academic" track of California cybersecurity workforce preparation (including degrees and certificates) as well as providing a non-traditional "professional-career track." This critical cybersecurity workforce recruiting, hiring, advancement and retention effort should fully integrate the NICE Cybersecurity Workforce Framework in California.

Continuity of Communications and Data Networks

The State of California will provide guidance to local and tribal entities for developing continuity plans. This guidance will be broadly applicable to continuity after any hazard but can be applied to cybersecurity. The guidance will include considerations for redundancy and continuity in communications and information technology that are relevant to cybersecurity planning and operations. This will include ensuring alternate telecommunications services are in place, including necessary agreements to permit the resumption of information asset operations for essential missions and business functions when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

California's ESF-18 Cybersecurity Annex provides an organizational framework for support and coordination among the CA-ESF 18 stakeholders for cyber incident coordination including cyber terrorism, cyber incidents involving critical infrastructure information systems, technological emergencies, or other emergencies or disasters with impacts on information technology (IT) capabilities or secure data and privacy information in the State of California. Cal OES manages several programs to ensure resiliency and continuity of the state's 911 and emergency services communications systems. The Cal-CSIC will work with

the Department of Technology, other state agencies, local governments, and key telecommunications industry providers to increasingly integrate cyber, physical, and cyber-physical threat assessments where this applies to communications and data networks.

Assess and Mitigate Cybersecurity Risks and Threats to Critical Infrastructure and Key Resources

California has a high number of Internet-facing industrial control networks which operate and regulate critical infrastructure including oil facilities, electricity, and Internet backbone lines. A cyberattack on any of these or on the emergency services sector could cause severe disruption and loss of life. California has developed and will use Emergency Support Function (ESF) 18 to coordinate resources to prepare, mitigate, respond, and recover from a significant cybersecurity event that impacts critical infrastructure and key resources, among other events.

ESF-18 will continue to be revised to further address legacy and physical systems not traditionally viewed in the cyber domain, but which continue to be digitized and increasingly exposed to cybersecurity threats, along with stakeholders with responsibility for systems with increasing cyber components. The Cal-CSIC will work with the State Threat Assessment Center to increasingly integrate cyber, physical, and cyber-physical threat assessments.

Cyber Threat Indicator Information Sharing

California will monitor information and potential threats using multiple information pathways, e.g., Open-Source Intelligence [OSINT], coordination with fusion centers, etc. Cal-CSIC will facilitate information and resource sharing among partners, and facilitate cyber coordination among state, local, and federal governmental partners, emergency management, State Threat Assessment Center (STAC), and the five Regional Fusion Centers (RFCs) in the state - the Central California Intelligence Center (CCIC), the Joint Regional Intelligence Center (JRIC), the Northern California Regional Intelligence Center (NCRIC), the Orange County Intelligence Assessment Center (OCIAC), and the San Diego Law Enforcement Coordination Center (SD-LECC).

California will seek to create an integrated analysis of threat trends and events, identify, and assist with the mitigation of knowledge gaps, implement methods to degrade or mitigate adversary threat capabilities. To achieve this, California will focus on the following.

- Collecting evidence and gathering intelligence to assist with attribution
- Linking related incidents, and identifying additional possible affected entities
- Identifying threat pursuit and disruption opportunities, and developing and executing courses of action to mitigate the immediate threat
- Facilitating information sharing and coordination with asset response efforts
- Ensuring information is collected in a way that can best facilitate, as appropriate, law enforcement investigations, federal/state/local government regulatory actions, legislative fact-finding, and civil proceedings

Department Agreements

The Regional Fusion Centers (RFCs) request state support for cybersecurity incidents through Cal-CSIC, as stipulated by California state law. Beyond this relationship, RFCs can also look to Cal-CSIC as a resource for information and other resources that may be needed to respond to and recover from a cyber incident.

The Cal-CSIC develops memorandums of understanding (MOU) to establish data sharing agreements with state and federal agencies and industry partners. The Cal-CSIC will continue to expand these partnerships

where necessary to facilitate information flow and to break down stovepipes. The Cal-CSIC will attempt to deconflict and minimize data sharing burdens on local governments (for example, where there are existing requirements from regulatory agencies) while maximizing participation so that information is accessible, relevant, and timely. All entities will recognize data-sharing is a two-way street and strive to access all available services while also identifying and sharing their own relevant indicators with the Cal-CSIC and federal agencies as appropriate.

The Cal-CSIC will continue to use forums like the California Cybersecurity Task Force (CCTF) and various working groups to encourage and participate in informal collaboration, while constantly seeking to expand formal partnerships.

Leverage CISA Services

At present, the Cal-CSIC works closely with state and regional CISA representatives to ensure available services are known and to coordinate cybersecurity initiatives. This coordination also ensures that between the Cal-CSIC and CISA, cybersecurity services are distributed most efficiently throughout the state. The Cal-CSIC will be a conduit for feedback from local governments and state agencies on the availability and quality of CISA services.

Going forward, California will continue to avail itself of the wide variety of services offered by CISA, including the agency's Cybersecurity Advisor program, Cyber Resilience Reviews (CRR™), External Dependencies Management (EDM) Assessments, Cyber Infrastructure Surveys, Cyber Education and Awareness, Federal Virtual Training Environment (Fed VTE), and the Stop. Think. Connect™ program, etc. The approach will be to determine the needs across sectors, agencies, and jurisdictions with the offerings to ensure each entity in need is able to quicky acquire the services offered.

Information Technology and Operational Technology Modernization Review

California will modernize legacy business processes and systems throughout the state. The state recognizes the need to optimize technology infrastructure and investments, foster digital services, and use data to inform decision-making. California will ensure security is built into the innovation and modernization of future state IT efforts. Government modernization will lead to improved and equitable decisions, services, and outcomes for Californians. California will modernize and improve the way in which individuals engage with state government. Significant efforts include:

- Developing a new CA.gov portal providing essential digital services in one website.
- Researching the development of a Digital ID system to be used across all state departments.
- Accepting credit card payments at all public-facing state departments.
- Migrating state department websites to CDT's Web Enterprise Platform and evaluating compliance with the Americans with Disabilities Act accessibility requirements.
- Transitioning all state forms to be signed and submitted electronically.
- Creating an all-electronic process for regulations submitted by departments to the Office of Administrative Law for approval.

These and other efforts will make it easier for individuals to obtain much needed information and services.

The Cal-CSIC will continue to leverage the CCTF to improve awareness of Operational Technology ("OT") risks and use this forum to engage industry and system operators to ensure risks are understood by all and so that all stakeholders can connect with appropriate resources.

Cybersecurity Risk and Threat Strategies

As required by state law, the Cal-CSIC will leverage the CCTF (of which the SLCGP planning committee is a part) to develop a statewide cybersecurity strategy. This strategy will encompass all existing strategic efforts and plans including the state Homeland Security Strategy Goal 3, Cal-Secure, ESF-18, and the SLCGP Cybersecurity Plan.

Through California's State Threat Assessment System (STAS), the California Cybersecurity Integration Center (Cal-CSIC), and CA-ESF 18 framework, the state will strive for effective information sharing, coordination, situational awareness updates, and mutual understanding of cyber risk and threats across levels of government and with the private sector. This will include how the information sharing process will be carried out. The process will incorporate all stages of information sharing, including how information is processed, analyzed, and disseminated before, during, and after a cyber incident. Cal-CSIC will serve as the central organizing hub of state government's cybersecurity activities, including overarching cybersecurity strategy, intelligence analysis, information sharing, and incident response.

Rural Communities

As stated in the FY23 SLCGP Notice of Funding Opportunity (NOFO):

> *Per 49 U.S.C. 5302 "rural" is any area with a population of less than 50,000 individuals. To meet the 25% rural pass-through requirement for SLCGP, the eligible subrecipient must be a local government entity within a rural area (a jurisdiction with a population of less than 50,000 individuals).*

Rural communities are assured adequate access to projects under the SLCGP by virtue of their representation on the state's planning committee and outreach activities that will be done by the planning committee as a whole and individual members of the planning committee. Rural governments are represented through direct participation in the planning committee by membership in the CCTF CIPS subcommittee. Additionally, their interests are represented through membership in state organizations including the Rural County Representatives of California (RCRC) and the California Special District Association (CSDA), who also participate in the planning committee. This is especially important for small jurisdictions with very limited time and personnel available to participate in SLCGP planning efforts.

Special emphasis was placed on analysis of small and rural local government needs in the capability gap survey performed for SLCGP. Prioritization of each of the 16 required elements was partly based on weighing more heavily areas where respondents were at the Foundational and Fundamental levels. Rural governments tend to be much more limited in not just cybersecurity capabilities but basic IT functions, and often lack a cybersecurity program entirely, let alone any need for improving those programs. SLCGP efforts will be prioritized which focus on starting cybersecurity programs for these local governments or helping grow nascent ones beyond the Foundational/Fundamental levels.

Many rural areas are serviced by county governments and special districts, and these should be key partners in ensuring cybersecurity services are effectively delivered to rural populations, or that they benefit from cybersecurity improvements to local governments.

The State in coordination with the Cybersecurity Task Force, state organizations mentioned above, and other partners will need to make a concerted outreach effort to ensure local government entities are aware of SLCGP and able to use the services and funds provided through it. School districts with less than 20,000 – 30,000 students likely do not have dedicated Cybersecurity staff – RFCs may be able to assist in outreach.

The State, specifically the Cal-CSIC and CDT, will need to follow-up with local government entities using their services to ensure they are being delivered effectively and in a timely manner. The Cal-CSIC and CDT should also strive to funnel feedback on CISA and MS-ISAC services to those organizations and champion improvements where necessary.

FUNDING & SERVICES

The State of California SLGCP Planning Committee intends to focus on the following initiatives, with the corresponding cyber assessment element number in parentheses, to strengthen cybersecurity across the State using the first two years of SLGCP funds.

- (3) Enhance the preparation/response/resiliency of information systems/apps/user accounts
- (4) Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk
- (14) Develop and coordinate strategies to address cybersecurity risks & threats
- (8) Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity)
- (10) Assess and mitigate, Critical Infrastructure and Key Resources ("CIKR") risks & threats impacting local jurisdictions
- (7) Ensure continuity of operations including by conducting exercises
- (15) Ensure rural communities have adequate access to, and participation in plan activities

These focus areas drive the projects detailed in Appendix B: Project Summary Worksheet.

Distribution to State Government Agencies

Of the 20% reserved for state government, 25% will go to Cal OES as the SAA to perform Management and Administration of the grant. The other 75% will go to other state agencies to cover the costs of enrolling them in cybersecurity services provided by CDT and the Cal-CSIC.

Distribution to Local Governments

The State of California intends to use at least 80% of the funding received through SLCGP to deliver services and capabilities to local government entities as described in **Appendix B: Project Summary Worksheet**, with at least 25% going to rural areas as defined below. The State of California does not intend to provide sub-grants or direct pass through of funds as part of this program. Local governments enrolling in these services will be required to sign an MOU describing the scope of services, local responsibilities, and a consent agreement (to receive services in lieu of cash). However, if local governments decline to receive services in lieu of a cash award, they will be offered the opportunity to participate in a competitive project proposal process. and submit a timely project proposal which meets all the objectives of at least one of the projects identified in this plan.

ASSESS CAPABILITIES

For each of the 16 required plan elements, California assembled respondents from across the state in May 2023 and had them briefly describe their current capabilities and choose their capability level across each of the 16 elements – foundational, fundamental, intermediary, and advanced. Using the NIST CSF,

California developed definitions for those levels to ensure a consistent understanding across all respondents.

As for addressing each element, the state converted each element into a question. For example, for element 1: “manage, monitor, and track information systems, applications, and user accounts” the assessment asked, “at what capability level is your organization able to manage, monitor, and track information systems, applications, and user accounts?” Respondents then picked from among the four capability levels using a drop-down menu or equivalent. Next, they would choose from among the five elements of capability – planning, organization, equipment, training, and exercises – and list those areas they have gaps and needs in.

For the Planning, Organizing, Equipping, Training, and Exercising (“POETE”) areas, respondents could pick none, one, or all, etc. Capturing data by POETE area allowed for a more seamless development of projects from the assessment, since projects will also have to track POETE. Finally, respondents provided a short narrative explaining what those POETE gaps were in more detail. For each of the 16 elements, the data was then rolled-up, analyzed, and presented in a gap analysis report. Please see results from that report in the first part of Appendix A: Cybersecurity Plan Capabilities Assessment.

While state agency representatives across all state government were welcome to participate in the capability gap survey, those under the authority of the Governor are also subject to requirements under the state government Cal-Secure Roadmap. Under Cal-Secure, they were required to participate in a self-assessment (also in May 2023) focused on specific areas designated by the Governor’s Office. See results of that survey in the second part of Appendix A: Cybersecurity Plan Capabilities Assessment.

IMPLEMENTATION PLAN

Organization, Roles, and Responsibilities

As the SAA, Cal OES formed the Cybersecurity Investment Planning Subcommittee (CIPS) within the existing statewide Cybersecurity Task Force (CCTF) to serve as the planning committee for the SLCGP. The CCTF CIPS will continue to operate as a collaborative body under its approved charter to help refine and improve the Cybersecurity Plan throughout the period of performance. The objective-aligned working groups will continue to provide focused effort on specific planning tasks. Cal OES will oversee execution of SLCGP in California, coordinating with other state agencies as well as tribal and local governments to ensure effective, efficient, and timely distribution of funds. The Cal-CSIC will continue to provide cybersecurity expertise and serve as the “hub” of cybersecurity information for the state. CCTF CIPS members will participate in continued planning efforts to the best of their ability, and actively communicate new ideas and suggestions through the working groups to the Cal-CSIC and Cal OES. Cal OES will fulfill all SAA responsibilities with FEMA and the Cal-CSIC will continue to coordinate with CISA on all relevant cybersecurity matters.

Each goal and its associated objectives in this Plan have their own timelines with target completion dates, and one or more owners responsible for overseeing and coordinating their completion. Accomplishing goals and objectives will require support and cooperation from numerous individuals, groups, or agencies, and may be added as formal agenda items for review during regular governance body meetings.

Appendix B: Project Summary Worksheet provides a list of cybersecurity projects to complete that tie to each goal and objective of the Cybersecurity Plan.

Resource Overview and Timeline Summary

Given the first-year funding resources identified below, California will provide readily available in-kind services to address the highest-priority cybersecurity gaps identified by the CCTF CIPS. Cal OES will establish the necessary interagency agreements to ensure the Department of Technology is able to apply SLCGP funds to these efforts. As it falls within Cal OES, the Cal-CSIC will not need such interagency agreements to provide these services and can execute immediately. Upon approval of the Cybersecurity Plan, Cal OES will establish an application process for state agencies, tribal governments, and local governments to enroll in these services in lieu of cash or submit project proposals which align with at least one project specified in the Cybersecurity Plan. All sub-recipients of the SLCGP grant, whether receiving in-kind services or cash, will be required to sign up for the CISA Cyber Hygiene Services. Once each state-level project is approved by FEMA, Cal OES will ensure funds are allocated within 45 days.

Estimated Program Timeline (Referencing California Cybersecurity Program Goals):

1. First six-twelve months: initial application period and enrollment in Cal-CSIC services (Goal 2) and CDT services (Goals 1, 2, 3) pending budget authority and completion of necessary interagency agreements which can take months to develop. Identification of additional project categories that best address remaining gaps and require longer budget planning and vendor engagement. Revise Plan once project costs are finalized. Develop additional projects that still require additional planning, costing, and preparation of budget authorities:
    a. Training and exercise projects using existing state facilities but extending to vendor-provided services (Goals 2, 4)
    b. Prioritize areas that could reduce ransomware vulnerability such as Malicious Domain Blocking and Reporting (MDBR), email hygiene and staff training (Goals 1, 2, 3)
    c. Roving or 'virtual' CISO aka VCISO program to benefit smaller, rural, and/or underserved agencies to jumpstart and mature their agency's cybersecurity program, perhaps in concert with or in addition to CDT's Virtual CISO Advisory Services (Goals 1, 2, 3, 4)
    d. Provide appropriate vulnerability assessments and penetration testing to baseline followed by tailored cybersecurity program initiation and maturation roadmaps accessible to IT staff with limited cybersecurity skills/training (Goals 1, 2, 3)
2. Following six months: enrollment in remaining CDT services as interagency agreements and budget authorities fall into place. Finalize training and exercise plans and required budgets. Revise Plan with additional projects aligned to priority areas identified in gap survey. (Goals 1, 2, 3, 4)
3. Years 2-3: execution of remaining projects once all budgets, budget authorities, and any necessary vendor contracts are in-place. (Goals 1, 2, 3, 4)

Voting Members of Planning Committee	
Nancy Ward	Director, Cal OES
Liana Bailey-Crimmins	State CIO and Director, Department of Technology
Tom Osborne	Deputy Director, Cal OES Homeland Security Division and Acting Commander, Cal-CSIC
Rami Zakaria	CIO, Sacramento County
Carolyn Coleman	Executive Director and CEO, League of California Cities
Tom Schrieber	CIO, Shasta County
Dennis Lingo	Chief Information - Technology Officer, Madera County Superintendent of Schools
Kerrstyn Vega	CCU representative for the Cybersecurity Planning Committee, Coalition of California Urban Area Security Initiatives (CCU)
Mark Lourenco	Information Security Officer, Information Security and Privacy Office, Technology Services Division, California Department of Education
Adam Dondro	CIO, California Health and Human Services Agency (CHHS)
Bob Burris	Deputy Chief Economic Development Officer, Rural County Representatives of California (RCRC)
Jose Gonzalez	CTO, Technology Services, Los Angeles County Office of Education
Jacqueline Wong-Hernandez	Chief Policy Officer, California State Association of Counties (CSAC)
Lea Eriksen	Director / CIO, City of Long Beach
Andrew White	Chief of Police, City of Martinez
Senior Advisors to the Planning Committee	
Vitaliy Panych	State CISO, Department of Technology Office of Information Security
John Cleveland	Deputy State CISO, Department of Technology Office of Information Security
Working Group Leaders	
Dr. Keith Clement	Professor / Homeland Security Certificate of Advance Study Coordinator/ Corrections Option Coordinator, CSU Fresno; and also California Cybersecurity Task Force Workforce Development and Education Subcommittee Chair
Hong Sae	CIO, City of Roseville
Gary Coverdale	CISO - Risk Management, Santa Barbara County
Robert Pittman	CISO, San Bernardino County
CISA Liaison to the Planning Committee	
Mario Garcia	Supervisory Cybersecurity Advisor (Sacramento, CA), CISA, Region 9
SAA SLCGP Project Management Team	
Eric Nehls	Cyber Policy and Strategy Planner, Cal-CSIC, Cal OES
Alissa Adams	Chief, Homeland Security Grants Division, Cal OES
Adam Crawford	Homeland Security Policy Coordinator, Homeland Security Division, Cal OES
Jaydeep Bhatia	California State Threat Assessment Center Analyst, Homeland Security Division, Cal OES
LeAnn Gajunia	Homeland Security Policy Analyst, Homeland Security Division, Cal OES
Joshua Filler	Contractor, Homeland Security Division, Cal OES

California Federal Fiscal Year 2022 SLCGP Award Allocations			
Portion	Federal Share	Non-Federal Cost Share (of Total Project Cost)	Total Project Cost Funds (Fed + SLTT shares)
Total	$7,976,788	10% (WAIVED)	$7,976,788
M&A (5%)	$398,839	10% (WAIVED)	$398,839
Non-M&A (95%)	$7,577,948	10% (WAIVED)	$7,577,948
Non-M&A State Allocation (15%)	$1,196,518	10% (WAIVED)	$1,196,518
Local Government Pass-Through (80%)	$6,381,430	10% (WAIVED)	$6,381,430
Rural Pass Through (subset of local government pass-through, at least 25% of TFA)	$1,994,197	10% (WAIVED)	$1,994,197

METRICS

Cybersecurity Program Metrics			
Program Goal	**Program Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
Goal 1: Develop and establish baseline governance structures across California's jurisdictions, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.	1.1: Establish cybersecurity governance structures and implement a program to evaluate maturity of the cybersecurity program aligned to Cybersecurity Performance Goals established by CISA and the National Institute of Standards and Technology (NIST).	1.1.1: Jurisdictions have established and documented a uniform cybersecurity governance structure that is accountable to organizational leadership and works together to set the vision for cyber risk management.	Jurisdictional chief information officer, or equivalent position, quarterly reporting to Cal-CSIC (target 90%).
		1.1.2. Jurisdictions have identified senior officials to enable whole-of-organization coordination on cybersecurity policies, processes, and procedures.	Senior officials are identified in the jurisdiction's cyber incident response plan under objective 1.2 (target 90%).
	1.2: Develop, implement, or revise, and test cybersecurity plans, including cyber incident response plans, with clearly defined roles and responsibilities.	1.2.1 Jurisdictions develop, implement, or revise, and exercise their cyber incident response plans every two years.	Jurisdictional biennial reporting to Cal-CSIC and within 30 days of completing the cyber exercise (target 90%). Jurisdictional biennial reporting to Cal-CSIC and within 30 days of completing or revising the cyber incident response plan (target 90%).

Cybersecurity Program Metrics			
Program Goal	**Program Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
	1.3: Asset (e.g., devices, data, software) protections and recovery actions are prioritized based on the asset's criticality and business value.	1.3.1 Jurisdictions document their prioritization of systems and network functions and set them for reconstitution according to their impact to essential functions.	Prioritized systems are identified in cyber incident response plans or other cybersecurity plans (target 90%).
Goal 2: Government jurisdictions across California understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.	2.1: Physical devices and systems, as well software platforms and applications, are inventoried.	2.1.1: Jurisdictions establish and regularly update asset inventory.	Assets are inventoried annually by jurisdictions (target 90%).
	2.2: Cybersecurity risk to each jurisdiction's operations and assets are documented and understood.	2.2.1: Jurisdictions conduct an annual cyber risk assessment to identify cyber risk management gaps and areas for improvement once a year.	Jurisdictional annual assessment (target 90%).
	2.3: Vulnerability scans are performed, and a risk-based vulnerability management plan is developed and implemented by each jurisdiction.	2.3.1: Jurisdictions participate in CISA's Vulnerability Scanning service, part of the Cyber Hygiene program or equivalent service provided by the state or commercial provider.	Number of jurisdictions that participate in vulnerability scanning service (target 100%), measured quarterly.
		2.3.2: Jurisdictions effectively manage vulnerabilities by prioritizing mitigation of high impact vulnerabilities and those most likely to be exploited.	Methods for tracking and managing vulnerabilities are documented by jurisdictions (target 90%).
	2.4: Capabilities are in place across each jurisdiction to monitor assets to identify cybersecurity events.	2.4.1: Jurisdictions are able to analyze network traffic and activity transiting or traveling to or from information systems, applications, and user accounts to understand baseline activity and identify potential threats.	Personnel or systems are in place to analyze jurisdictions' network traffic and activity (target 90%).

Cybersecurity Program Metrics			
Program Goal	**Program Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
	2.5: Processes are in place across each jurisdiction to action insights derived from deployed capabilities.	2.5.1: Jurisdictions are able to respond to identified events and incidents, document root cause, and share information with partners.	Cyber incident after action reports documenting root cause of the incident (target 90% of jurisdictions document).
Goal 3: Implement highest priority cybersecurity protections commensurate with risk across California's government jurisdictions.	3.1: Jurisdictions adopt fundamental cybersecurity best practices.	3.1.1: Jurisdictions implement multi-factor authentication (MFA), prioritizing privileged users, Internet-facing systems, and cloud accounts.	Number of jurisdictions that implement MFA (target 90%).
		3.1.2: Jurisdictions end use of unsupported/end of life software and hardware that are accessible from the Internet.	Number of jurisdictions that end use of unsupported/end of life software and hardware that are accessible from the Internet (target 90%).
		3.1.3: Jurisdictions prohibit use of known/fixed/default passwords and credentials.	Number of jurisdictions that document the prohibition of using known/fixed/default passwords and credentials (target 100%).
		3.1.4: Jurisdictions ensure the ability to reconstitute systems following an incident with minimal disruption to services.	Number of jurisdictions that can achieve recovery times outlined in cyber incident response and recovery plans (target 90%).
		3.1.5: Jurisdictions migrate to .gov internet domain.	Number of jurisdictions that migrate to .gov internet domain over the next four years (target 90%).

Cybersecurity Program Metrics			
Program Goal	**Program Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
	3.2: Jurisdictions reduce gaps identified through an assessment and planning process and apply increasingly sophisticated security protections commensurate with risk.	3.2.1: Jurisdictions address items identified through assessments and planning process.	Number of jurisdictions that document, through improvement plans, they are addressing items identified through assessments (target 90%).
	Objective 3.3: Create and operationalize a portfolio of cybersecurity as-a-service offerings at the state level, i.e., security operations center services, to address gaps in a cost-effective manner.	3.3.1: The state develops the required documentation and personnel required to provide cybersecurity as-a-service offerings to all jurisdictions that request it.	All jurisdictions requesting cybersecurity as-a-service from the state receive it (target 100%).
Goal 4: Develop and unify California's diverse, innovative cybersecurity workforce to safeguard the data and systems used across jurisdictions to deliver public services.	4.1: Personnel across jurisdictions and job categories are appropriately trained in cybersecurity necessary to recognize and respond to cybersecurity risks and understand their roles and responsibilities within established cybersecurity policies, procedures, and practices.	4.1.1: Jurisdictions require regular ongoing phishing training, awareness campaigns are conducted, and organization provides role-based cybersecurity awareness training to all employees.	Employee training is documented and reported annually (target 90% of employees).
		4.1.2: The jurisdiction has dedicated resources and funding available for its cybersecurity professionals to attend technical trainings and conferences.	The number of jurisdictional cybersecurity professionals attending technical training and conferences is documented and reported annually (target 90%).
	4.2: Jurisdictions adopt the National Initiative for Cybersecurity	4.2.1: Jurisdictions have established cyber workforce	Each jurisdiction's cyber workforce development and

Cybersecurity Program Metrics			
Program Goal	**Program Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
	Education (NICE) Cybersecurity Workforce Framework.	development and training plans, based on the NICE Cybersecurity Workforce Framework.	training plan is reported to Cal-CSIC (target 90%).
	4.3: Better align each jurisdiction's workforce with current and future cybersecurity needs by updating cybersecurity talent models and career paths to include cybersecurity job roles, job categories, knowledge, skills, and abilities.	4.3.1: Jurisdictions have or create cybersecurity career path toolkit.	Each jurisdiction documents development of their toolkit (target 90%).
		4.3.2: Jurisdictions create or update their cybersecurity talent model and career paths.	Each jurisdiction documents creation of or the updating of their cybersecurity talent model and career paths (target 90%).
	4.4: Build and expand partnerships with educational institutions and private industry to create a diverse pipeline of cybersecurity professionals seeking careers in public service.	4.4.1: Jurisdictions formalize and document partnerships with educational institutions.	Each jurisdiction has a formal partnership with at least one educational institution (target 90%).

APPENDIX A: CYBERSECURITY PLAN CAPABILITIES ASSESSMENT

Statewide Capability Gap Survey and Analysis

The State and Local Cybersecurity Grant Program (SLCGP) requires a capability gap assessment/analysis as part of development of the required cybersecurity plan. The SLGCP project management team, led by Cal OES, with the assistance of the California Cybersecurity Integration Center (Cal-CSIC), conducted a survey in June 2023 of potential grant sub-recipients. This survey was designed to assess general cybersecurity maturity levels and capability gaps across the state. These assessments were organized in alignment with the 16 required elements of the cybersecurity plan. The following summarizes the results of that survey.

The survey produced both quantitative and qualitative information. First, the quantitative information was based on a self-assessment of capability levels and gaps for each element and sub-element:

		1	2	3	4	5a	5b	5c	5d	5e	5f	5g	6	7	8	9	10	11	12	13	14	15	16	Avg	
Capability Level	Foundational	14	17	21	31	16	27	31	17	18	9	46	28	45	53	29	23	45	25	44	31	68	51	31.3	median = 33
Capability Level	Fundamental	52	50	54	45	34	46	44	49	35	34	31	39	42	45	45	50	42	39	49	49	20	19	41.5	average = 31.7
Capability Level	Intermediary	48	43	44	37	43	39	40	37	47	57	13	36	32	27	41	43	26	44	21	35	23	34	36.8	max = 68
Capability Level	Advanced	14	18	8	15	35	16	13	25	28	28	34	22	8	2	12	12	15	19	13	13	10	16	17.1	min = 2
	Average	32	32	32	32	32	32	32	32	32	32	31	31	32	32	32	32	32	32	32	32	30	30		
Capability Gap	Planning	56	44	55	65	48	44	56	50	37	35	61	48	73	67	49	58	54	49	58	69	40	47	52.9	median = 45
Capability Gap	Organization	66	56	59	68	45	46	44	55	41	40	47	43	59	75	43	58	58	47	60	61	34	44	52.2	average = 44.4
Capability Gap	Equipment	55	64	45	47	39	72	52	51	34	44	17	20	31	24	44	42	28	14	27	26	21	19	37.1	max = 83
Capability Gap	Training	53	53	56	55	48	43	45	21	40	33	26	29	59	62	38	55	46	43	43	43	19	30	42.7	min = 14
Capability Gap	Exercises	51	46	63	44	22	24	28	15	25	53	17	24	83	43	49	52	40	25	35	39	17	19	37.0	
	Average	56	53	56	56	40	46	45	38	35	41	34	33	61	54	45	53	45	36	45	48	26	32		

Figure 2: Statewide Cybersecurity Capability Levels and Gaps

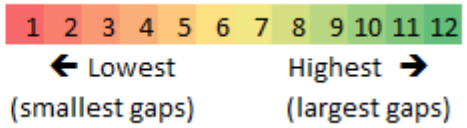
Survey respondents were asked to describe what their overall challenges were for each gap in a short text summary statement. The SLGCP project management team summarized and anonymized those responses in a capability gap analysis report. This

report combined both the quantitative/numeric results and the summarized text responses. This report was shared with the working groups to evaluate which elements needed the most priority.

Using the results of the capability gap survey, the SLGCP project management team analyzed this data and came up with a priority ranking method of the 16 required elements and sub-elements based on three criteria:

1. Capability Level score = count of Foundational + count of Fundamental
2. Capability Gap score = average across POETE areas
3. Working Group priority score: four working groups aligned to each of the four main objectives, composed of cybersecurity or IT professionals formed from the larger subcommittee, identified the areas they thought were most needed/important. They were instructed to base this more on their professional expertise and experience of statewide needs than on their own particular jurisdictions' circumstances. They were also asked to look at a summary of the qualitative results and make a subjective, but informed decision about which areas should be focused on first based on the apparent need across all jurisdictions.

Combining the first two criteria provided a "quantitative composite score": capability level score + capability level score. The project management team then combined that with the working group priority score by multiplying them. This produced the total score, with the highest score being equivalent to the highest (or first) priority ranking, resulting in the priority ranking listed below.

Color Scale for Element Ranking
Gap Composite Scores (Red-Yellow-Green) 

Priority Rank	Element	Element Description	Capability Level (Foundational + Fundamental)	Capability Gap (using average across POETE areas)	Composite Score (level + gap)	WG 1	WG 2	WG 3	WG 4	WG Total	Total Score: Composite Score x WG
1	3	Enhance the preparation/response/resiliency of InfoSys/apps/user accounts	75	56	131	5			3	8	1045
2	4	Continuous cybersecurity vulnerability assessments/threat mitigation prioritized by risk	76	56	132		5		2	7	923
3	14	Develop and coordinate strategies to address cybersecurity risks & threats	80	48	128	4	3			7	893
4	8	Identify/mitigate workforce gaps, enhance recruitment/retention, bolster KSAs (NICE Framework)	98	54	152				5	5	761
5	10	Assess and mitigate, CIKR risks & threats impacting local jurisdictions	73	53	126		4		1	5	630
6	7	Ensure continuity of operations including by conducting exercises	87	61	148				4	4	592
7	15	Ensure rural communities have adequate access to, and participation in plan activities	88	26	114	3	2			5	571
8	5a	Multi-Factor Authentication	50	40	90			5		5	452
9	5d	End use of unsupported/EOL software & hardware accessible from Internet	66	38	104			4		4	418
10	16	Distribute funds, items, services, capabilities, or activities to local governments/agencies	70	32	102	1	1	2		4	407
11	5e	Prohibit use of known/fixed/default passwords and credentials	53	35	88			3		3	265
12	1	Manage, monitor, and track information systems, applications, and user accounts	66	56	122	2				2	244
13	5c	Data encryption for data at rest and in transit	75	45	120			1		1	120
14	13	IT/OT modernization cybersecurity review process	93	45	138					0	0
15	11	Share cyber threat indicators with the State of California & DHS	87	45	132					0	0
16	2	Monitor, audit, and track network traffic and activity	67	53	120					0	0
17	5b	Enhanced logging	73	46	119					0	0
18	9	Ensure continuity of comms & data networks	74	45	119					0	0
19	5g	Migration to .gov internet domain	77	34	111					0	0
20	6	Promote delivery of safe/recognizable/trustworthy online services, including .gov	67	33	100					0	0
21	12	Leverage cybersecurity services offered by DHS (CISA)	64	36	100					0	0
22	5f	Ensure ability to reconstitute systems (backups)	43	41	84					0	0

Figure 3: SLCGP Element Ranking Based on Gap Analysis

Finally, the project management team surveyed the subcommittee again to see which services would be most valuable in addressing these gaps, and selected a manageable threshold of the top services that would best address the highest priorities.

Preferred State Government Services Survey Results

Following up on the capability gap survey, subcommittee members were asked about a list of services state government could provide that they would be most interested in at this time. These results were compared with the capability gap analysis to narrow down the final list of services and projects.

The survey first asked which funding model would be most preferred: state-government provided in-kind services in lieu of cash, direct cash, or a hybrid (the option to choose). The results of that question indicated a hybrid option was preferred:

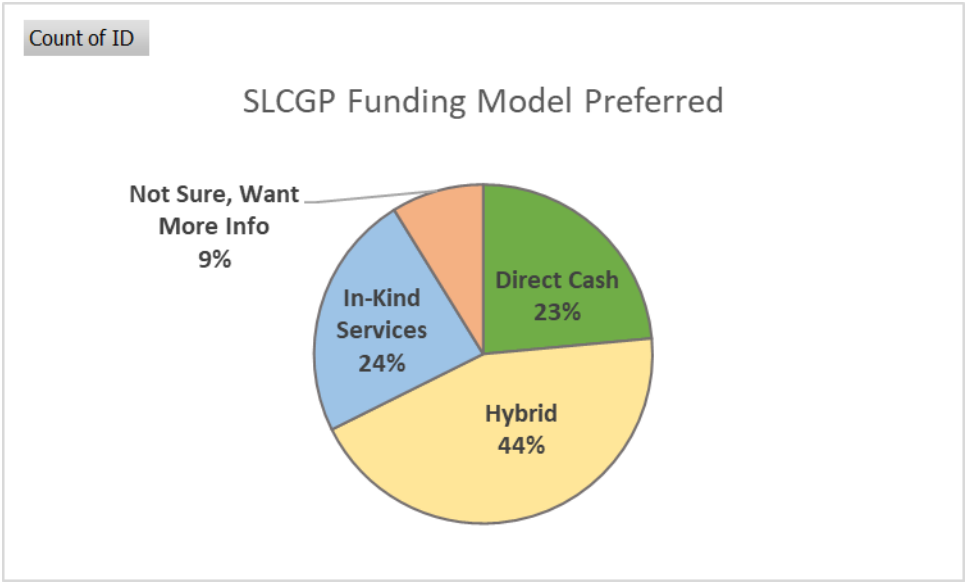
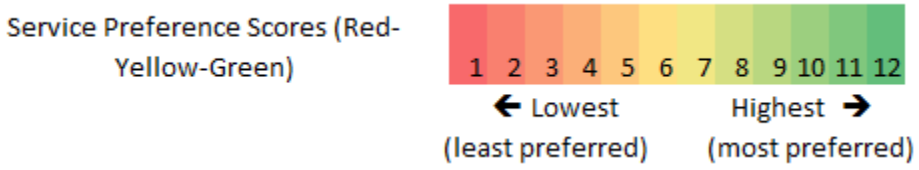


Figure 4: SLCGP Funding Model Preferred Based on Survey

The second part of the survey evaluated interest in each one of a discrete set of services the state could provide. The answers were then scored by weighting the answer options as indicated in the chart below:

Answer Options	No Interest At This Time	Not Sure, Need More Info	Previously Used, No Longer Need	Currently Enrolled	Somewhat Interested	Very Interested	Score
Weight	*0*	*0.1*	*0.2*	*0.3*	*0.4*	*0.5*	
Cal-CSIC DarkWeb Monitoring	16	28	0	2	47	43	43.7
Cal-CSIC Threat Intelligence Products Subscription	11	33	0	15	43	34	42.0
Cal-CSIC Monthly Cyberthreat Briefing	15	23	0	29	36	33	41.9
CDT Security Information and Event Management (SIEM): Microsoft Sentinel and Lighthouse	24	26	0	3	32	51	41.8
CDT Continuous detection and alerting via Security Operations as a Service (SOCaaS)	22	28	1	6	35	44	40.8
CDT Attack Surface Management / CyberSecurity Ratings program (with third-party risk management)	19	33	0	2	44	38	40.5
Cal-CSIC External Vulnerability Scanning (adhoc) with assistance onboarding to CISA's Cyber Hygiene Services	21	25	2	17	33	38	40.2
CMD Independent Security Assessment (note: SLCGP may only offset a small portion of the cost)	22	32	2	2	45	33	38.7
Cal-CSIC Morning Report Subscription	22	28	1	27	29	29	37.2
CDT Virtual CISO Advisory Services to augment personnel	26	36	0	0	43	31	36.3
CDT Vulnerability Disclosure Program/Process for CA.GOV	31	36	0	2	41	26	33.6
CDT Otech Datacenter services IDS/IPS protection and DDoS mitigation service	36	34	0	2	40	24	32.0
Cal-CSIC NetFlow Analysis	28	47	0	1	33	27	31.7
Cal-CSIC RAVEn Program	22	79	0	2	20	13	23.0
CDT Hosting/registration for .ca.gov	62	27	1	14	21	11	21.0

Figure 5: Service Option Ranking Based on Survey



In actual practice, some of these services can be easily bundled as they scale in the same way. For example, Cal-CSIC's DarkWeb Monitoring, Threat Intelligence Products Subscription, Monthly Cyberthreat Briefing and Morning Report Subscription can be bundled with one subscription and scale similarly from a cost standpoint. Likewise, CDT's .ca.gov registration and hosting come with the vulnerability disclosure program/process.

Gap To Service Crosswalk/Matrix

Combining the data above results in this mapping of capability gaps to services. Checkmarks indicate which elements the services address, and the Total Score indicates the degree to which the services are preferred and address the highest priority gaps:

		Gap Analysis Element Ranking																					
		Element	1	2	3	4	5a	5b	5c	5d	5e	5f	5g	6	7	8	9	10	11	12	13	14	15	16	
Services	Services Survey Rank	Element Rank	12	16	1	2	8	17	13	9	11	22	19	20	6	4	18	5	15	21	14	3	7	10	Total Score
Cal-CSIC DarkWeb Monitoring	1			✓	✓	✓					✓			✓				✓	✓				✓	✓	87.0
Cal-CSIC Threat Intelligence Products Subscription	2				✓	✓								✓		✓		✓	✓	✓		✓	✓	✓	44.0
Cal-CSIC Monthly Cyberthreat Briefing	3				✓	✓								✓		✓		✓	✓	✓		✓	✓	✓	29.3
CDT Security Information and Event Management (SIEM): Microsoft Sentinel and Lighthouse	4		✓	✓	✓	✓		✓			✓			✓			✓	✓	✓				✓	✓	33.5
CDT Continuous detection and alerting via Security Operations as a Service (SOCaaS)	5		✓	✓	✓	✓		✓		✓	✓			✓	✓		✓	✓	✓				✓	✓	29.8
CDT Attack Surface Management / CyberSecurity Ratings program (with third-party risk management)	6		✓		✓	✓			✓	✓	✓			✓				✓					✓	✓	15.0
Cal-CSIC External Vulnerability Scanning (adhoc) with assistance onboarding to CISA's Cyber Hygiene Services	7				✓	✓				✓	✓			✓				✓		✓			✓	✓	12.3
CMD Independent Security Assessment	8				✓	✓				✓	✓			✓				✓				✓		✓	7.6
Cal-CSIC Morning Report Subscription	9				✓	✓								✓		✓		✓	✓	✓		✓	✓	✓	9.8
CDT Virtual CISO Advisory Services to augment personnel	10		✓		✓	✓			✓	✓	✓			✓	✓		✓	✓	✓				✓	✓	12.9
CDT Vulnerability Disclosure Program/Process for CA.GOV	11		✓		✓	✓		✓		✓	✓		✓	✓				✓	✓				✓	✓	11.6
CDT Otech Datacenter services IDS/IPS protection and DDoS mitigation service	12		✓	✓	✓	✓								✓	✓		✓	✓					✓	✓	8.1
Cal-CSIC NetFlow Analysis	13		✓	✓		✓								✓				✓					✓	✓	5.5
Cal-CSIC RAVEn Program	14					✓								✓				✓	✓				✓	✓	4.2
CDT Hosting/registration for .ca.gov	15		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓					✓	✓	12.5

Figure 6: Service - Gap - Element Crosswalk & Total Score

State Government Cal-Secure Survey Results

State agencies under the authority of the Governor are subject to requirements under the state government Cal-Secure Roadmap. Under Cal-Secure, they were required to participate in a self-assessment (also in May 2023) focused on specific areas designated by the Governor's Office. The results of that survey revealed some key findings, correlated with SLCGP plan elements below. These findings influenced our priority focus areas for projects but needs of local governments were weighted more heavily.

Executive Branch Capability Gap Areas Requiring Attention	Corresponding Plan Element
Compliance with all state Business Continuity and Technology Recovery Program requirements (SAM and SIMM Sections 5325-5325.6)	3, 5f, 7, 9, 10, 14
Presence of unsupported Operating Systems (OS) on state networks	1, 3, 4, 5d, 10, 13
Security patching for all mobile devices in accordance with SIMM 5300-A	3, 4,
Full compliance with annual security training requirements as required by SAM and SIMM Section 5320	8, 10

Constitutional/Independent state government entities, while not required to, also responded to this survey. As potential grant sub-recipients, their responses were also relevant. Findings are summarized here:

Constitutional/Independent Agencies Capability Gap Areas Requiring Attention	Corresponding Plan Element
+Full implementation of all state Business Continuity and Technology Recovery Program requirements as advised by SAM and SIMM Sections 5325-5325.6	3, 5f, 7, 9, 10, 14
+Presence of unsupported Operating Systems (OS) on state networks	1, 3, 4, 5d, 10, 13
+Security patching for all mobile devices as advised by SIMM 5300-A	3, 4,
+Full compliance with annual security training requirements as advised by SAM and SIMM Section 5320	8, 10
+Entered all identified information security risks and findings on a Risk Register and Plan of Action and Milestones (POAM) as advised in SIMM 5305-	1, 3, 4, 6, 10, 14

Mapping Cybersecurity Plan Required Elements and Capability Levels to Projects

COMPLETED BY State of California Cybersecurity Planning Committee			
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities of SLTT within the Eligible Entity** **Note: CSR = Composite Score Rank** **WGPR = Working Group Priority Rank**	**Select capability level from:** Foundational Fundamental Intermediary Advanced	**Project # (s)** *(If applicable – as provided in Appendix B)*
1. Manage, monitor, and track information systems, applications, and user accounts	Gaps due to lack of planning capability across state and local government due to resource constraints (CSR 9, WGPR 12).	Fundamental	3, 4, 5
2. Monitor, audit, and track network traffic and activity	Gaps mainly due to lack of planning capability, equipment, and staff at local government level. (CSR 11, WGPR not rated).	Fundamental	1, 3, 4
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts	Gaps mainly due lack of resources and planning capability at local government level to exercise or test capabilities (CSR 6, WGPR1.	Fundamental	1, 2, 3, 4, 5
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk	Gaps mainly due lack of organizational resources at local government level (CSR 5, WGPR 2).	Fundamental	1, 2, 3, 4, 5
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)	See below		
a. Implement multi-factor authentication	Gaps mainly due to lack of planning capability, organization, equipment, and training at both state and local level but most at intermediary level or advanced (CSR 20, WGPR 7).	Intermediary	5
b. Implement enhanced logging	Gaps mainly due to lack of staff and equipment at local level, most at fundamental level (CSR 15, WGPR NR).	Fundamental	3, 4, 5

c. Data encryption for data at rest and in transit	Gaps mainly due to lack of equipment and planning capability at state and local level (CSR 10, WGPR 13).	Fundamental	5
d. End use of unsupported/end of life software and hardware that are accessible from the Internet	Gaps mainly due to lack of equipment, organization, and planning capability at state and local level (CSR 16, WGPR 9).	Fundamental	4, 5
e. Prohibit use of known/fixed/default passwords and credentials	Gaps mainly due to lack of training and organization at the local level (CSR 21, WGPR 11).	Intermediary	1, 3, 4, 5
f. Ensure the ability to reconstitute systems (backups)	Gaps mainly due to lack of exercising/testing and equipment at the state and local level (CSR 22, WGPR 4).	Intermediary	5
g. Migration to the .gov internet domain	Gaps mainly due to lack of planning capability at the local level (CSR 15, WGPR NR).	Foundational	5
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain	Gaps mainly due to lack of planning capability and organization at the local level (CSR 18, WGPR NR).	Fundamental	1, 2, 3, 4, 5
7. Ensure continuity of operations including by conducting exercises	Gaps mainly due to lack of exercises, training, organization, and planning capability at the state and local level (CSR 2, WGPR 8).	Foundational	4
8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity)	Gaps mainly due to lack of training, organization, and planning capability at the state and local level (CSR 1, WGPR 4).	Foundational	2
9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks	Gaps mainly due to lack of exercises, equipment, and planning capability at the local level (CSR 13, WGPR NR).	Fundamental	3, 4, 5
10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the eligible entity	Gaps mainly due to lack of exercise, training, organization, and planning capability at the local level (CSR 8, WGPR 5).	Fundamental	1, 2, 3, 4, 5

11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department	Gaps mainly due to lack of organization and planning capability at the local level (CSR 4, WGPR NR).	Foundational	1, 2, 3, 4, 5
12. Leverage cybersecurity services offered by the Department	Gaps mainly due to lack of training, organization, and planning capability at the local level (CSR 19, WGPR NR).	Intermediary	2
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives	Gaps mainly due to lack of organization and planning capability at the local level (CSR 3, WGPR NR).	Fundamental	Not in this phase
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats	Gaps mainly due to lack of organization and planning capability at the local level (CSR 7, WGPR 3).	Fundamental	2, 5
15. Ensure rural communities have adequate access to, and participation in plan activities	Gaps mainly due to lack of organization and planning capability at the local level (CSR 14, WGPR 6).	Foundational	1, 2, 3, 4, 5
16. Distribute funds, items, services, capabilities, or activities to local governments	Gaps mainly due to lack of organization and planning capability at the local level (CSR 17, WGPR 10).	Foundational	1, 2, 3, 4, 5

APPENDIX B: PROJECT SUMMARY WORKSHEET

Purpose: The **Project Summary Worksheet** is a list of cybersecurity projects that the entity plans to complete to develop or improve any needed cybersecurity capabilities identified in **Appendix A: Cybersecurity Plan Capabilities Assessment**.

While Virtual CISO Advisory Services did not appear to score as high on the Gap to Service Crosswalk/Matrix, it was specifically highlighted by the Subcommittee Working Groups as potentially addressing many challenges at the local government level, especially for the smaller and more rural governments. For this reason, it was included in the final list here.

	Project Name	Project Description	Related Required Element #	Cost	Status	Priority	Project Type
1	DarkWeb Monitoring	State Government Service Option: Cal-CSIC DarkWeb Monitoring	2, 3, 4, 5e, 6, 10, 11, 15, 16	TBD	future	high	Equip
2	Threat Intelligence Subscription	State Government Service Option: Cal-CSIC Threat Intelligence Products Subscription, Monthly Cyberthreat Briefing, and Morning Reports	3, 4, 6, 8, 10, 11, 12, 14, 15, 16	TBD	future	high	Plan, Equip, Train
3	Security Information and Event Management (SIEM) Capability	State Government Service Option: CDT provisioned subscription to Microsoft Sentinel and Lighthouse	1, 2, 3, 4, 5b, 5e, 6, 9, 10, 11, 15, 16	TBD	future	high	Equip
4	Security Operations Center Capability	State Government Service Option: CDT Continuous detection and alerting via Security Operations as a Service (SOCaaS)	1, 2, 3, 4, 5b, 5d, 5e, 6, 7, 9, 10, 11, 15, 16	TBD	future	high	Organize, Equip
5	Virtual CISO Advisory Services	State Government Service Option: CDT Virtual CISO Advisory Services to augment personnel	1, 3, 4, 5a, 5b, 5c, 5d, 5e, 5f, 5g, 6, 9, 10, 11, 14, 15, 16	TBD	future	high	Plan, Organize, Train

APPENDIX C: ENTITY METRICS

The below table should reflect the goals and objectives the Cybersecurity Planning Committee establishes.

Cybersecurity Plan Metrics			
Planning Goal	**Plan Objectives**	**Associated Metrics**	**Metric Description (Details, source, frequency)**
1. The State of California has an approved Cybersecurity Plan that meets the SLCGP requirements as defined in the NOFO	1.1 Draft the Plan	Draft Plan exists in Document Library	Cal-CSIC confirms Draft Plan is in Document Library
	1.2 Committee Approves Plan	Signed Letter by CIO	Committee Meeting Minutes
	1.3 Submit the Plan to CISA	Confirmation of Receipt	Email from CISA
	1.4 CISA Approves Plan	Statement of Approval	Email from CISA
2. Receive Funding from SLCGP	2.1 Funding received to Execute approved projects	Receipt of funds	Accept and Expend approval from Governor and Council
3. Execute Procurement Process for Each Approved Project	3.1 Execute approved projects	Projects are invoiced and paid Planning Committee establishes baseline evaluation and monitoring requirements for participating entities	Financial Reporting via SAA Per entity and per project deployment is tracked and outcomes measured against baseline
	3.2 Closeout approved projects	Projects are terminated or renewed	Financial Reporting via SAA
4. Process services for Local Entities and Rural areas that request inclusion	4.1 Enroll Local Entities in Services	Number of entities enrolled in each approved project	Financial Reporting via SAA
5. Review, Revise and Update Plan for next FY as required.	5.1 Repeat Objectives for Goal 1 for subsequent FY	See Goal 1	See Goal 1.

APPENDIX D: ACRONYMS

Acronym	Definition
Cal OES	California Governor's Office of Emergency Services
Cal-CSIC	California Cybersecurity Integration Center
CCIC	Central California Intelligence Center
CCTF CIPS	California Cybersecurity Task Force Cybersecurity Investment Planning Subcommittee
CCTF WDE	California Cybersecurity Task Force Workforce Development and Education Subcommittee

Acronym	Definition
CCU	Coalition of California Urban Area Security Initiatives
CDT	California Department of Technology
CHHS	California Health and Human Services Agency
CHP	California Highway Patrol
CIKR	Critical Infrastructure Key Resource(s)
CISO	Chief Information Security Officer
CMD	California Military Department
C-SCRM	cyber supply chain risk management
CSDA	California Special District Association
CSF	Cyber Security Framework
ESF-18	Emergency Support Function 18
FIPS	Federal Information Processing Standard
HSS	California Homeland Security Strategy
JRIC	Joint Regional Intelligence Center
MDBR	Malicious Domain Blocking and Reporting
MOU	memorandum of understanding
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCRIC	Northern California Regional Intelligence Center
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OCIAC	Orange County Intelligence Assessment Center
OIS	Office of Information Security
OSINT	Open-Source Intelligence
POAM	Plan of Action and Milestones
POETE	Planning, Organization, Equipment, Training, Exercises
RCRC	Rural County Representatives of California
RFCs	Regional Fusion Centers
SAM	State Administrative Manual

Acronym	Definition
SD-LECC	San Diego Law Enforcement Coordination Center
SIEM	Security Information (or Incident) and Event Management
SIMM	Statewide Information Management Manual
SLGCP	State and Local Cybersecurity Grant Program
SOC	Security Operations Center
STAC	State Threat Assessment Center