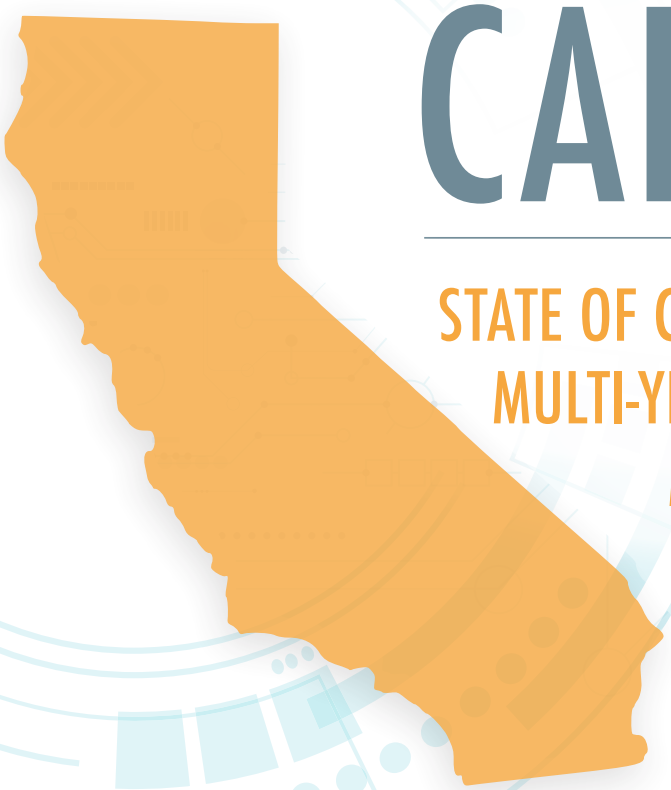


CAL-SECURE

STATE OF CALIFORNIA EXECUTIVE BRANCH MULTI-YEAR INFORMATION SECURITY MATURITY ROADMAP 2021

California Department of Technology

TABLE OF CONTENTS

State of California Executive Branch Five-Year Information Security Maturity Roadmap 2021

LETTER FROM THE GOVERNOR OF CALIFORNIA

Digital innovation provides a path forward as we advance our commitment to a “California for All”. As cybersecurity threats evolve, we remain dedicated to protecting the privacy and security of all Californians' information. In order to be accountable to this commitment, we must prepare for cyberattacks of any scale.

The California Homeland Security Strategy and the State Technology Strategic Plan: Vision 2023, make it clear that a collaborative approach is needed to identify, manage, and mitigate cybersecurity risks. It is critical that California prioritize its resources in order to manage the most significant cyber risks and safeguard the services for the residents that depend on them.

To address these challenges, we have developed Cal-Secure, a multi-year cybersecurity roadmap for California. Designed to be flexible and innovative, Cal-Secure enables the state to manage existing and future threats more effectively. Cal-Secure defines a path for state entities to strengthen their cybersecurity measures so that they may continue to provide critical services without interruption.

California’s cybersecurity community is committed to protecting the essential services provided by state entities and the privacy of the residents’ information. We will accomplish this by strengthening our cybersecurity maturity and preparedness and enabling state entities to combat threats so that they may continue to serve the residents of California.

Gavin Newsom
California Governor

EXECUTIVE SUMMARY

The California Department of Technology (CDT) and its Office of Information Security (OIS) are pleased to release 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 to 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. Each goal is explained in detail in each of its accompanying section and initiatives are explained in detail in both the section it is assigned to as well as in the Annex and Enclosures.

Another core aspect of Cal-Secure is the multi-year Horizon Map (located on pages 13-14) 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.

CAL-SECURE ROADMAP PRIORITIES TO REDUCE RISK

PEOPLE
World-Class Cybersecurity Workforce

- Develop job roles, job categories, knowledge, skills, and abilities (KSAs)
- Expand cybersecurity training opportunities
- Increase opportunities to source cybersecurity talent

PROCESS
Federated Cybersecurity Oversight

- Provide effective cybersecurity oversight of California’s Executive Branch
- Support Agency and entity cybersecurity strategy development
- Promote agile, collaborative statewide cybersecurity governance

TECHNOLOGY
Effective Cybersecurity Defenses

- Define baseline cybersecurity capabilities for California’s executive branch
- Foster cybersecurity by design through IT modernization
- Collaboratively tackle cybersecurity threats

FOUNDATIONAL GUIDANCE

Cal-Secure is designed to further the goals of the California HSS and the State Technology Strategic Plan: Vision 2023 by enhancing and maturing cybersecurity capability at all levels of California's Executive Branch, from statewide executive branch cyber and information security governance to the security awareness and training of the state workforce. The 15 key Cal-Secure initiatives align with the Vision 2023 goals listed below and support strengthening cybersecurity and preparedness across the state.

ROADMAP OVERVIEW

Cal-Secure outlines an innovative information, privacy, and cybersecurity roadmap that incorporates hundreds of hours of feedback from the state government security community and has several key features:

- California established in the HSS the goal of Strengthen Security and Preparedness across Cyberspace. The California HSS is the framework for prioritizing and developing statewide homeland security capabilities. The HSS enhances safety and preparedness with state, federal, local, tribal, and private sector stakeholders. 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 this HSS goal.
- Cal-Secure is broken into three strategic categories that must be equally addressed by the Executive Branch – People, Process, and Technology. Each category contains strategic priorities to address their respective critical shortfalls or concerns. Each category also contains five key initiatives that are specific targets or deliverables, which, when achieved, will make a measurable impact on the success of the strategic priorities.
- The Technology category has the additional feature of having a defined prioritized list of baseline cybersecurity capabilities that all state entities are required to achieve over the next five years. While these capabilities are already required by policy, this roadmap removes any ambiguities related to prioritization by establishing a roadmap with specific milestones.
- Cal-Secure has a Horizon Map on pages 13-14 which is split into two components. The left side of the map lists all baseline capabilities that entities must utilize within their organizations and the given prioritization for completion over the next five years. The right side of the Horizon Map lists all initiatives found in each of the three strategic categories and OIS's prioritization for completion.
- This document is designed to be utilized by state government agencies and entities in the development of their individual strategies and roadmaps based upon high-level priorities that will provide the tactical and operational means to achieve the initiatives and standards in Cal-Secure. This approach allows all state departments to prioritize efforts towards maturity regardless of their existing baseline capabilities currently fully implemented.

PEOPLE

World-Class Cybersecurity Workforce

We will develop and unify California's diverse, innovative cybersecurity workforce to safeguard the data and systems used to deliver public services.

Across the nation, governments and other organizations are facing a shortage in the cybersecurity workforce. Approximately 521,000 cybersecurity jobs nationwide went unfilled as of February 2021. California led the country with 66,000 cybersecurity job openings between October 2019 and September 2020.[1] As a result, California's HSS has statewide objectives to make cybersecurity workforce development and training a priority. To help address this challenge, California's executive branch must take a proactive approach to increase training opportunities for existing staff, as well as increase the pipeline of candidates to fill critical positions.

Some of these pipelines and opportunities exist today; however, we will need to provide additional investments and develop partnerships throughout the coming years. Behind these initiatives will be a "one government" approach that brings together key stakeholders across California's executive branch.

ROADMAP PRIORITIES

- **Develop job roles, job categories, knowledge, skills, and abilities**
- **Expand cybersecurity training opportunities**
- **Increase opportunities to source cybersecurity talent**

KEY INITIATIVES

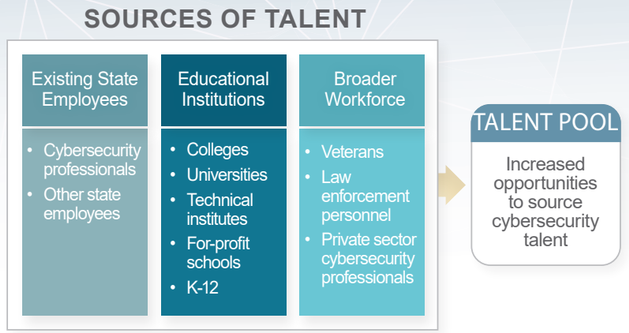
- **Develop pipelines for cybersecurity professionals**
- **Align cybersecurity roles with the National Initiative for Cybersecurity Education (NICE) framework**
- **Create a cybersecurity career path toolkit**
- **Expand tailored workshops for the state cybersecurity workforce**
- **Promote innovative programs for cybersecurity skill and leadership development**

1. ISC2. 2019 Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)2 Cybersecurity Workforce Study, 2019. https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019, accessed February 22, 2021.

   Cyberseek.org. "Cybersecurity Supply/Demand Heat Map." https://www.cyberseek.org/heatmap.html, accessed February 22, 2021.

Increase opportunities to source cybersecurity talent

California is home to many sources of cybersecurity talent including the state workforce, educational institutions, military, law enforcement, and the private industry. California's executive branch must build and expand partnerships with these organizations to create a diverse pipeline of cybersecurity professionals seeking careers in state service. These pipelines should focus not just on higher level educational opportunities but also include students from kindergarten through high school.

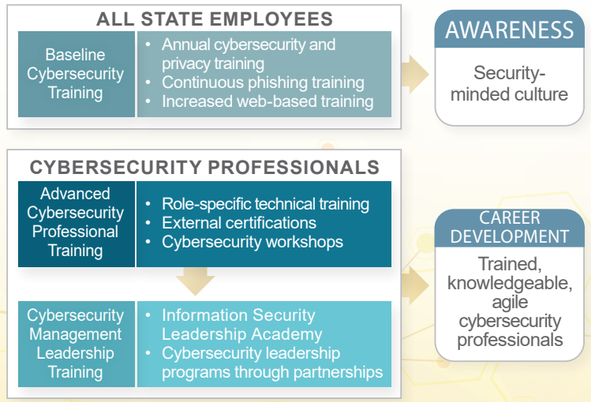


Develop job roles, job categories, knowledge, skills, and abilities

To align the workforce with California's current and future cybersecurity needs, California's Executive Branch must update its cybersecurity talent model and career paths. Organizational design, leadership alignment, and employee perspectives will be key factors to consider in this process. State cybersecurity practitioners will understand their role within California's cybersecurity workforce, along with the requirements to transition to new roles or jobs over time. Clearly defined cybersecurity roles, job categories, knowledge, skills, and abilities (KSAs) are fundamental to a modern cybersecurity talent model. California will develop these fundamental plans using industry best practices, such as the NICE workforce framework.

Expand cybersecurity training opportunities

As a baseline, all state employees must have an awareness of cybersecurity and privacy risks, and how to recognize and respond to common threats such as phishing. Advanced training, tailored to the KSAs in California's cybersecurity talent model, is needed for employees in cybersecurity roles. Cybersecurity professionals in leadership and management positions should participate in programs through CDT, such as the Information Security Leadership Academy, as well as professional development opportunities through community organizations and partnerships.



PROCESS

Federated Cybersecurity Oversight

We will provide effective oversight supported by a flexible governance model.

Collaboration and planning are a cornerstone of California's HSS to ensure the security, reliability, integrity, and continuity of critical cyber information, records, communications systems and services. A clearly defined, empowered, and efficient governance model is critical to the success of all initiatives associated with this roadmap. California's cybersecurity governance structure has evolved over time, moving from a centralized governance structure to a highly federated one. However, as entities have become more independent, some have become "islands of excellence" by continually seeking to improve cybersecurity maturity, while others have become "islands of neglect," as a lack of resources and training have caused their cybersecurity programs to fall behind.

To address this issue, Cal-Secure outlines a hybrid model that uses an empowered agency level governance structure, along with oversight by OIS. New cybersecurity and privacy policies, processes, and decisions made at the agency level are communicated and applied at the entity level. This hybrid governance model will encourage collaboration and communication between California's cybersecurity leadership, as well as the development of strategic plans at all levels.

ROADMAP PRIORITIES

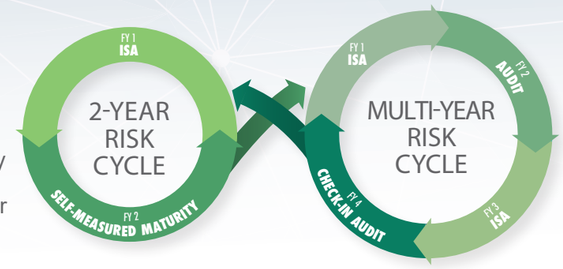
- **Provide effective information, privacy, and cybersecurity oversight of the Executive Branch**
- **Support agency and entity cybersecurity strategy and roadmap development**
- **Promote agile, collaborative statewide cybersecurity governance**

KEY INITIATIVES

- **Create tools for cybersecurity strategy and roadmap development at state agencies and entities**
- **Formalize the cybersecurity governance structure**
- **Transform state information, privacy, and cybersecurity policies and standards**
- **Modernize cybersecurity procurement**
- **Create multi-tiered cybersecurity governance bodies**

Provide effective information, privacy, and cybersecurity oversight of the Executive Branch

The goal of the continuous Oversight Lifecycle is to ensure that all entities finish better than when they started in both cybersecurity maturity and organizational risk mitigation. The state has defined oversight processes that adapt to the risk level of agencies and entities. Entities at less risk follow a two-year cycle, consisting of alternating Independent Security Assessments (ISAs), risk surface reduction consultation and self-measured cybersecurity maturity assessments. The remainder of the entities manage cybersecurity risk through a comprehensive multi-year Oversight Lifecycle consisting of alternating ISAs and audits providing continuous technical and policy guidance.

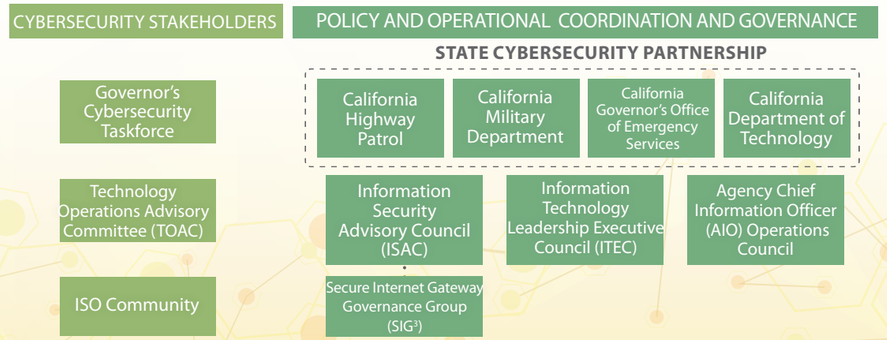


Support agency and entity cybersecurity strategy development

California's cybersecurity governance model is designed to disseminate the roadmap and standards defined by the statewide leadership in collaboration with the Cal CSIC, in order to position agency ISOs to adapt this roadmap to the needs and requirements of their entities. The outcome is to enable agency ISOs to manage cybersecurity risks as this roadmap is implemented. Through implementation at the entity level, each organization can tailor roadmaps and guidelines provided by the state to meet their business needs and goals.

Promote agile, collaborative statewide cybersecurity governance

California has evolved its cybersecurity governance model to a multi-tiered structure that encourages communication and coordination among state cybersecurity leadership, agencies, and entities. This multi-tiered structure facilitates the use of agency-level capabilities and strategies to tackle industry-specific threats by providing California's cybersecurity leadership with a stronger network of resources and improved channels for feedback while leveraging Cal-CSIC as California's overall coordinating hub ofcybersecurity activities. See the Cybersecurity Governance Structure figure in the Annex C for a detailed depiction of the California's executive branch cybersecurity governance structure broken down by state, agency and entity levels.



TECHNOLOGY

Effective Cybersecurity Defenses

We will invest in technology and services to enhance cybersecurity capabilities at all state entities.

California's HSS lays out the priority to implement and maintain procedures to detect malicious activity, and conduct technical and investigative-based countermeasures, mitigations, and operations against existing and emerging cyber-based threats.

Cal-Secure defines three technology-related priorities of the Executive Branch to enhance the ability of state entities to safeguard the data and systems used to provide services to the public. First, the roadmap defines the basic baseline set of technical cybersecurity capabilities required for all state entities, along with a roadmap for prioritizing their implementation. Secondly, the strategy aligns with the State's IT modernization effort that aims to modernize legacy business processes and systems throughout the state. Lastly, Cal-Secure calls for the collaboration of the California Department of Technology Security Operations Center (CDT SOC), Cal-CSIC, and all state entities to tackle threats across the state. The CDT SOC, Cal-CSIC and state entities provide continuous security monitoring of threats at endpoints and on the California Government Enterprise Network (CGEN), dramatically and efficiently improving the state's cybersecurity posture and ability to quickly mitigate cybersecurity risk.

ROADMAP PRIORITIES

1. **Define baseline cybersecurity capabilities for state entities**
2. **Foster cybersecurity by design through IT modernization**
3. **Collaboratively tackle cybersecurity threats**

KEY INITIATIVES

- **Create a portfolio of Cybersecurity as-a-Service offerings**
- **Implement the Unified Integrated Risk Management platform**
- **Provide all state entities with security operations services**
- **Define cybersecurity technology requirements through community-led groups**
- **Integrate cybersecurity into the IT Modernization Roadmap**

Define baseline cybersecurity capabilities for state entities

The following tables contain basic baseline technical cybersecurity capabilities, a priority for adoption, and alternative models for implementation. These baseline capabilities are required across all of California's Executive Branch and are designed to raise the state cybersecurity maturity to a minimum level to reduce risk. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) was utilized to organize the baseline as it provides the industry standard for cybersecurity modeling and aligns with NIST Special Publications 800-53 and the State Administrative Manual section 5300.

WHAT THE STATE PROVIDES

CALIFORNIA GOVERNMENT ENTERPRISE NETWORK (CGEN)*	STATEWIDE DATA CENTER MANAGED SERVICES	CALIFORNIA CYBERSECURITY INTEGRATION CENTER (CAL-CSIC)
• CGEN Edge Detection • CGEN Edge Protection • Distributed Denial-of-Service (DDoS) Protection • Initial Incident Response Management • Network Forensics • Access control services • Software Defined Network	• Endpoint Protection • Email Threat Detection • Network Threat Detection and Prevention • Internal Lateral Movement Monitoring • Web Application Firewall and Protection • Secure Application Integration and Continuous Deployment (DevSecOps)	• Complex Incident Response Coordination • Statewide Cyber-Exercise • Threat Information Sharing • Prioritize and Communicate Threats • Attack Surface Mapping • Threat Intelligence Integration

* All California Executive Branch entities must utilize CGEN per Government Code (GC) 11546.3 (a&b). These capabilities come with this service.

PHASED ORDER OF PRIORITY OF CYBERSECURITY CAPABILITIES *

ONE	TWO	THREE	FOUR	FIVE
• Anti-Malware Protection • Anti-Phishing Program • Multi-Factor Authentication • Continous Vulnerability Management	• Asset Management • Incident Response • Continuous Patch Management • Privileged Access Management • Security and Privacy Awareness Training • Security Continuous Monitoring 24x7 • Cloud Security Monitoring	• Data Loss Prevention • Log Management • Network Threat Detection • Network Threat Protection • Threat Intelligence Platform • Application Security • Operational Technology Security	• Disaster Recovery • Enterprise Sign-On • Mobile Device Management • Application Development Security • Application Whitelisting • Software Supply Chain Management	• Identity Lifecycle Management • Insider Threat Detection • Network Access Control • Enterprise Encryption • Mobile Threat Defense

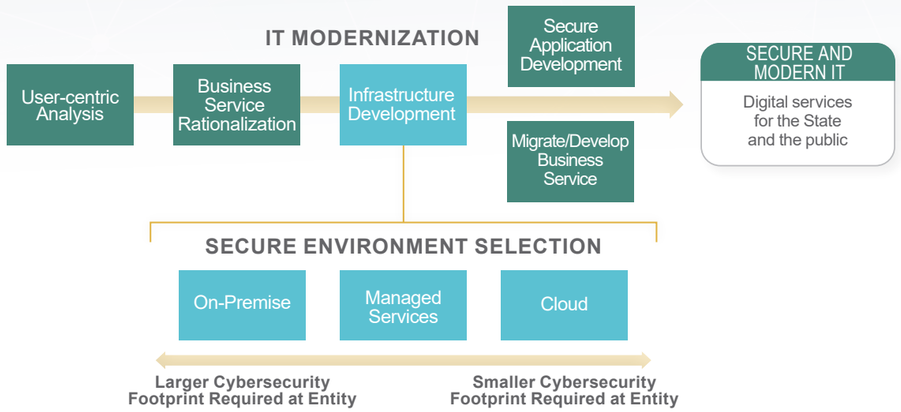
* For a more detailed definition of each capability see Annex A.

CYBERSECURITY CAPABILITY DEPLOYMENT OPTIONS

AGENCY / ENTITY SOLUTION	Some entities may choose to meet the baseline by building cybersecurity capabilities into their environments, whether on-premise or in the entitiy's cloud tendency.
CENTRALIZED SERVICES	CDT will offer select cybersecurity capabilities as a service to provide the choice to subscribe to services that meet the requirements of the baseline.
THIRD-PARTY SOLUTION	Entities may choose to engage third-party cybersecurity providers for retainers, managed services, and subscriptions for cybersecurity capabilities that are not core competencies for that entity

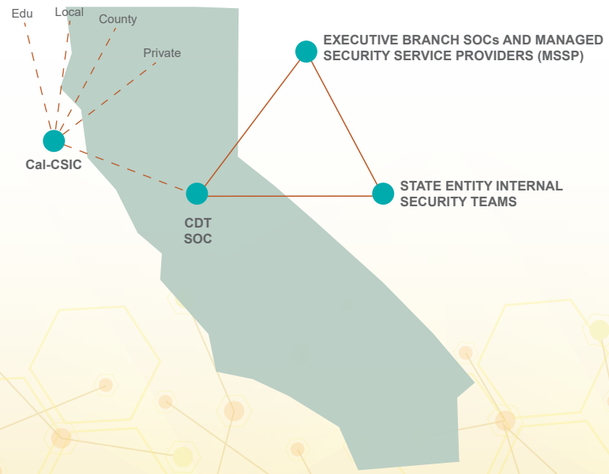
Foster cybersecurity by design through IT modernization

A key component of Cal-Secure is the tie-in to the state's IT modernization effort. Cal-Secure not only focuses on reducing risks to existing systems and networks, but also on ensuring security is built into the innovation and modernization of future state efforts.



Collaboratively tackle cybersecurity threats

By sharing core capabilities and leveraging our partnership with the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, the state will dramatically increase its ability to detect, protect, and respond to cybersecurity threats. California's Executive Branch must create a constellation of existing security operations groups with the CDT SOC as the primary 24x7 operational security component. By the end of 2023 all state entities, regardless of size or business, must be part of this collaborative constellation network.



SUCCESS MEASURES

Measuring progress is a key component of California's Executive Branch Security roadmap. All initiatives and priorities in Cal-Secure directly align with the OIS Foundational Framework (Statewide Information Management Manual (SIMM) 5330-B), and the California Cybersecurity Maturity Metric (SIMM 5300-C), and the California HSS. In addition to this metric, the following table depicts key aspirational metrics as targets for improvement.

Within the next five years we aspire to...

PEOPLE

We will develop and unify California's diverse, innovative cybersecurity workforce to safeguard the data and systems used to deliver public services.

- Significantly reduce the average phishing click rate
- Increase talent pool partnerships
- Greatly increase the number of available cybersecurity training events and workshops

PROCESS

We will create a flexible governance model to measure progress, define policies and standards, and make informed decisions.

- Enable the Executive Branch to have the capability to identify risks continually across IT infrastructure
- Build a collaborative and informed Executive Branch security community
- Help build Executive Branch Agency and entity strategic plans and roadmaps
- Establish a continuous process improvement to maximize capabilities for technology and people

TECHNOLOGY

We will invest in technology and services to enhance the cybersecurity capabilities of the Executive Branch.

- Link together and obtain threat data from the Executive Branch assets
- All planned cybersecurity capabilities implemented and continuously managed across all state assets
- Eliminate the use of unsecured technology

CAL-SECURE MULTI-YEAR HORIZON

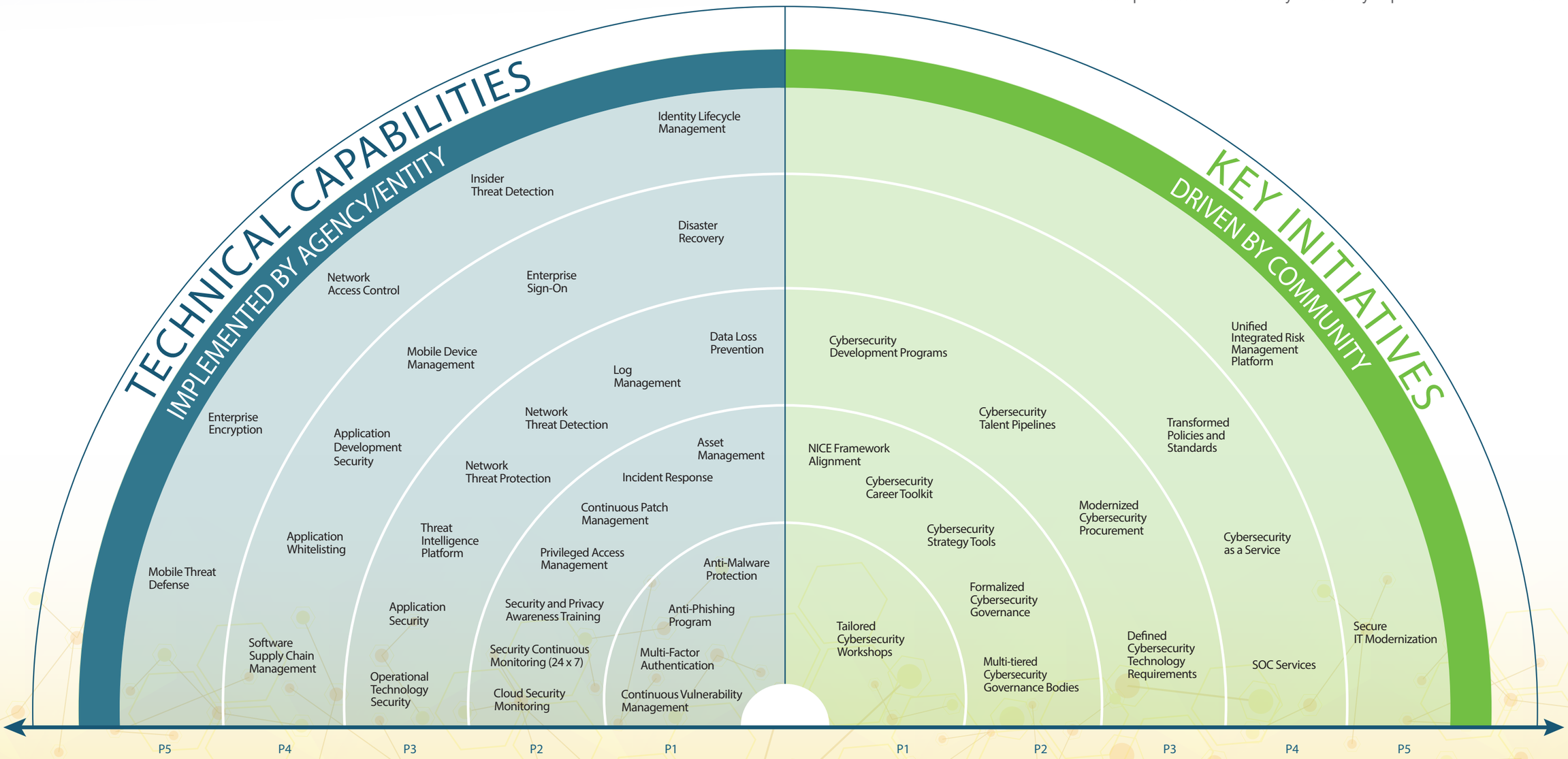
The Horizon Map pictured below, contains a prioritized roadmap depicting all strategic cybersecurity initiatives and capabilities detailed in Cal-Secure. The left side of the diagram contains the technical cybersecurity capabilities required of all Agencies and entities. They are arranged in priority order so Agencies and entities can build and operationalize each capability in order to increase maturity.

The right side depicts the statewide and Agency or entity cybersecurity initiatives necessary to improve cybersecurity maturity more broadly. These innovative initiatives are targeted at transforming California's privacy and cybersecurity across people, process, and technology.

Implementation of Cal-Secure and realization of the state's security end state will require resources and leadership from the entire security community. To help guide the State Executive Branch to this end each element of the strategy is prioritized and sequenced to provide maximum impact to the state's security posture, as well as to ensure that ample time is allowed for planning, resource establishment, and implementation.

OIS will work with the Department of General Services and the vendor community to streamline the procurement and implementation of each technical apability when possible.

Note: Annex A and B contain descriptions of each of the cybersecurity capabilities and initiatives below.



ANNEX A

GLOSSARY

Agency Chief Information Officer (AIO)
The AIO is responsible for IT, including IT assets, projects, and infrastructure, through the oversight and management of the CIO and development of Agency Enterprise Architectures.

AIO Operations Council
A customer-focused body comprised of executive leadership to provide customer-centered input on shared services, rates and opportunities for cross-agency collaboration.

Agency Information Security Office (AISO)
The AISO is responsible for adapting the cybersecurity strategies from the Office of Information Security to the needs and requirements of individual Agency entities, cybersecurity architectural guidance, and cybersecurity risk identification and management.

Anti-Malware Protection
The automated technical capability to detect and block malicious activity from trusted and untrusted applications, and dynamically respond to security incidents and alerts.

Anti-Phishing Program
A collection of security controls, including technological capabilities to detect and prevent email-based phishing attacks, as well as the process of training employees to identify and deal with potential phishing email threats.

Application Development Security
Security as part of the software development lifecycle to ensure application confidentiality, integrity and availability. It includes the people, processes, policies and practices to build security into application development and is the responsibility of all stakeholders and project staff, not just the software developers.

Application Security
Application security incorporates specific security measures, policies, processes and controls into all phases of the application lifecycle including design, development, testing, implementation, upgrade and maintenance.

Application Whitelisting
The use of whitelists (a list of explicitly allowed applications) to control the applications permitted to execute on a host, thereby preventing the execution of malware, unlicensed software, and other unauthorized software.

Asset Management
The effective tracking and managing of IT assets for an entity's program and enterprise IT infrastructure and production systems, including the ability to identify and classify entity owned hardware and software, telecommunications, maintenance costs and expenditures, support requirements (e.g. state staff, vendor support), and the ongoing refresh activities necessary to maintain the entity's IT assets.

California Cybersecurity Integration Center (Cal-CSIC)
Cal-CSIC serves as the central organizing hub of state government's cybersecurity activities, including overarching cybersecurity strategy, intelligence analysis, information sharing, and incident response.

California Foundational Framework
The Foundational Framework, as documented in SIMM 5330-B, is comprised of 30 security objectives to assist California's Executive Branch with prioritization of their information security efforts. It is used to consistently measure and mature the Executive Branch's security compliance.

California Government Enterprise Network (CGEN)
CGEN provides wide-area network (WAN) connectivity through vendor-owned and managed equipment across the California Executive Branch.

Chief Information Officer (CIO)
The CIO is directly responsible for all IT activities within the state entity, portfolio management of the state entity's technology initiatives, and operational oversight of IT functions and personnel.

Cloud Security Monitoring
The continuous security monitoring of cloud infrastructure for potential security vulnerabilities and threats, as well as assuring optimal functioning of the cloud platform while minimizing security risks including costly data breaches.

Data Loss Prevention
The ability to identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) from unauthorized use and disclosure. DLP includes deep packet inspection and analyzing the contextual security of transactions.

Disaster Recovery
The ability of an organization to respond to a disaster or an interruption in services by implementing a disaster recovery plan to stabilize and restore the organization's critical functions.

Enterprise Encryption
Enterprise encryption applies security and access controls directly to structured and unstructured data wherever it exists in the enterprise including on premises, virtual, in the cloud or in a hybrid environment, and at rest, in transit and in motion.

Enterprise Sign-On
Enterprise sign-on eliminates the need to separately authenticate and sign-on to individual applications and systems. It allows the user to authenticate once, and then be subsequently and automatically authenticated when accessing other specified systems.

Honeypot
A honeypot is a decoy computer system for tracking hackers or tracking unconventional or new hacking methods. They are designed to purposefully engage and deceive hackers and identify malicious activity. Multiple honeypots can be set on a network to form a honeynet.

Identity Lifecycle Management
The collection of technologies and practices that provisions and deprovisions users to appropriate levels of access to organizational resources.

Incident Response
An action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. It is a six-step process: 1) preparation, 2) identification, 3) containment, 4) eradication, 5) recovery, and 6) lessons learned.

Independent Security Assessment (ISA)
The ISA is a technical analysis of identified controls designed to measure cybersecurity maturity. Areas within the current ISA include host vulnerability assessments, firewall analysis, host hardening analysis, phishing susceptibility, network penetration testing, websites, web applications, and snapshot analysis of network traffic for signs of threat actor compromise.

Information Security Advisory Council (ISAC)
ISAC is a security-focused body comprised of Agency Information Security Officers to provide input and consultation on security policy, procedures, standards, and guidelines.

Information Security Continuous Monitoring
Information Security Continuous Monitoring is the ongoing monitoring sufficient to ensure and assure effectiveness of security controls related to systems and networks by assessing security control implementation and organizational security status in accordance with organizational risk tolerance and within a reporting structure designed to make real-time, data-driven risk management decisions.

Information Security Leadership Academy (ISLA)
ISLA incorporates security best practices, NIST frameworks, California-specific policy, standards and compliance, and information security program management skills aimed at preparing candidates for the roles of ISO, AISO, or an expanded role within their department's security office.

Information Security Officer (ISO)
The ISO is responsible for security policies, driving security culture and awareness, cybersecurity strategy, implementation of cybersecurity capabilities, and communication with entity leadership and business owners on security requirements and operations under the oversight of the AISO.

Information Technology Leadership Executive Council (ITEC)
ITEC is the central decision-making body comprised of executive leadership to oversee statewide technology strategy, policy, oversight and service offerings.

Insider Threat Detection
A coordinated collection of security capabilities designed to detect the unauthorized disclosure of sensitive information by an entity with authorized access.

Log Management
The process for generating, transmitting, storing, analyzing, and disposing of log data. Log management is essential to ensure computer security records are stored in sufficient detail for an appropriate duration. Sources of log entries include network devices, authentication servers, operating systems, applications, etc.

Mobile Device Management
The fundamental visibility and security controls needed to secure, manage and monitor any entity or employee owned mobile device, such as smartphones or tablets that access an organization's sensitive or confidential information.

Mobile Threat Defense
Threat detection and protection technologies designed for the requirements and vulnerabilities of mobile platforms, such as smart phones and tablets.

Multi-Factor Authentication
Authentication based on two or more of the following: something you know (i.e. password), something you have (i.e. token or smartcard), or something you are (i.e. a biometric).

National Initiative for Cybersecurity Education (NICE) (NIST SP 800-181)
The NICE framework describes cybersecurity work and the knowledge, skills, and abilities (KSAs) needed to complete tasks that can strengthen the cybersecurity posture of an organization and improve communication about how to identify, recruit, develop, and retain cybersecurity talent.

National Institute of Standards and Technology (NIST)
NIST is a non-regulatory federal agency within the US Department of Commerce with the mission to promote innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Network Access Control
Examining incoming connections to an organization's network from remote users and allow or disallow access based on those checks.

Network Threat Detection
Effective monitoring and analyzing of network or system events to find, and provide real-time or near real-time warning of, attempts to access-system resources in an unauthorized manner.

Network Threat Protection
Effective protection against network security threats attempting to harm organizational assets and thwarting attempts to proliferate on an organization's network.

NIST Cybersecurity Framework (CSF)
The CSF consist of standards, guidelines, and best practices to manage cybersecurity-related risk and promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

NIST Risk Management Framework (RMF)
The RMF defines the process that integrates security and risk management activities into the steps of the system development lifecycle (categorize, select, implement, assess, authorize, and monitor).

Office of Information Security (OIS)
OIS is the primary California state authority charged with ensuring confidentiality, integrity, and availability of state systems and applications, and ensuring the protection of state information assets.

Operational Technology (OT) Security
Operational Technology (OT) is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. OT is common critical infrastructure in Industrial Control Systems (ICS) such as a SCADA System.

Continous Patch Management
Systematic notification, identification, deployment, installation, and verification of operating system, firmware, and application software patches.

Privileged Access Management
Secure provisioning of privileged access to critical assets, and effective monitoring and maintenance of privileged accounts and access. Privileged access spans a wide range of systems and infrastructure components, such as operating systems, databases, middleware, applications, and network devices.

Secure Internet Gateway Governance Group (SIG^3)
The Secure Internet Gateway Governance Group encompasses the people, process and technology to mitigate risk to state information assets through network monitoring, identification and mitigation of unauthorized activity.

Security and Privacy Awareness Training
Creating awareness and educating employees and other users of information systems on the information security risks associated with the activities related to their job roles, as well as their responsibilities in complying with an organization's security policies and procedures designed to reduce these risks.

Security Operations Center (SOC)
Security operations centers house cybersecurity operations teams that detect threats, share intelligence, and coordinate response activities. California has established a constellation of security operations centers to protect California's Executive Branch.

Software Supply Chain Management
Supply-chain-management software (SCMS) is the software tools or modules used in executing supply chain transactions, managing supplier relationships and controlling associated business processes.

State Administrative Manual (SAM)
The State Administrative Manual (SAM) is a reference resource for statewide policies, procedures, requirements and information developed and issued by specified California state entities.

Statewide Information Management Manual (SIMM)
The SIMM provides the standards, instructions, forms and templates that California's Executive Branch must use to comply with IT policy, including guidelines, models, forms, and templates.

Technology Operations Advisory Committee (TOAC)
An Agency Technology Operational board that discusses cybersecurity related technologies, reviews industry best practices, and shares research to ensure that Executive Branch entities make informed technology resource decisions.

Threat Intelligence Platform
Automated mechanism to aggregate, transform, analyze, interpret, or enrich threat information to provide the necessary context for decision-making processes.

Unified Integrated Risk Management Platform
A platform to simplify, automate, and integrate enterprise, operational, and IT risk management processes and data to make better-informed risk-based decisions.

Continuous Vulnerability Management
Vulnerability Scanning is an inspection of potential points of exploit and weakness on a network or system including outdated software versions, missing patches or misconfigurations and flawed programming.

ANNEX B

CYBERSECURITY INITIATIVES

PEOPLE

Align cybersecurity roles with the NICE framework

Develop cybersecurity job roles and required KSAs that align with NIST NICE workforce framework. NICE is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development.

Create a cybersecurity career path toolkit

Create a cybersecurity career path toolkit that outlines the paths for career progression within the Executive Branch's cybersecurity workforce.

Expand tailored workshops for the Executive Branch's cybersecurity workforce

Enhance existing and develop new OIS sponsored workshops for the Executive Branch's cybersecurity workforce, focused on state specific information, topics, and requirements, including the State Administrative Manual Section 5300 and the SIMM Section 5300.

Promote innovative programs for cybersecurity skill and leadership development

Promote innovative programs for Executive Branch's cybersecurity workers that include technical and generally available cybersecurity training, self-study, and cybersecurity certifications. Promote statewide cybersecurity leadership programs through partnerships with educational institutions and industry organizations.

Develop pipelines for cybersecurity professionals

Partner with Executive Branch programs, industry associations, veterans' organizations, educational institutions, and others to bring awareness to and interest in state cybersecurity careers.

PROCESS

Create tools for cybersecurity strategy development at state Agencies and entities

Create tools to assist Agencies and entities to develop and manage actionable strategic plans that map to Cal-Secure.

Formalize the cybersecurity governance structure

Define the role of the AISO to provide oversight, drive adoption of strategies, and report on cybersecurity risk to state entities. Refine the role of the entity ISO to emphasize cybersecurity management and strategic planning, driving the implementation of baseline cybersecurity capabilities, and attesting to their maturity.

Transform state cybersecurity policies and standards

Update standards, guidelines, and policies allowing ISOs to leverage defined capabilities and policies to implement effective cybersecurity programs.

Modernize cybersecurity procurement

Leverage economies of scale for all state entities for cost-effective procurement of cybersecurity capabilities that meet state cybersecurity requirements and standards. Normalize technological capabilities to promote a higher level of cybersecurity maturity across state entities.

Create multi-tiered governance bodies

Create multi-tiered governance bodies, such as the SIG[3], to mitigate risk to state information assets through network monitoring, identification, and mitigation of unauthorized activity.

TECHNOLOGY

Create a portfolio of Cybersecurity as-a-Service offerings

Implement common Cybersecurity as-a-Service capabilities, such as anti-phishing, security awareness and privacy training, and end-point detection and response.

Implement statewide Unified Integrated Risk Management Plaform

Implement a statewide Unified Integrated Risk Management Platform for integrated risk management and automation of information security programs and oversight.

Provide all state entities with security operations services

Create a constellation of existing state SOCs which act together as a network to share threat information and coordinate response activities.

Define cybersecurity technology requirements through community-led groups

Through community-led working groups, define common cybersecurity technology requirements promoting consistency of technology and services for broader use across state Agencies and entities.

Integrate cybersecurity into the IT Modernization Roadmap

Integrate cybersecurity into the state's IT Modernization Roadmap as CGEN and data centers migrate to contemporary and flexible technologies that support digital services.

ANNEX C

DETAILED CYBERSECURITY GOVERNANCE STRUCTURE

California's Executive Branch cybersecurity governance structure is designed to disseminate the strategy and standards defined by statewide leadership, position AISOs to adapt these strategies to the needs and requirements of individual entities, and enable entities to implement these strategies to manage the cybersecurity risks to California's Executive Branch's mission.

STATE OPERATIONS AND OVERSIGHT

STATE CIO

State CISO

- Policy
- Audit and Independent Security Assessments
- Security Operations
- Statewide Strategy and Planning
- Privacy
- Statewide Security Culture
- Advisory Services

- Create, update, publish statewide cybersecurity policies and standards
- Coordinate AISO and ISO activities
- Integrate statewide security initiatives
- Formulate statewide cybersecurity strategies
- Promote and enhance risk management and priority programs
- Identify high-risk activities and entities
- Conduct cybersecurity audits and assessments
- Manage statewide cybersecurity operations

AGENCY CYBERSECURITY OVERSIGHT

AGENCY CIO (AIO)

AISO

- Entity Cybersecurity Risk Oversight
- Agency Cybersecurity Strategy
- Cybersecurity Compliance Oversight
- Statewide Policy Compliance
- Advisory Cybersecurity Policy

- Create, update, and publish Agency cybersecurity policies and standards
- Coordinate OIS requirements and initiatives with entity ISO
- Inform and advise Agency leadership on cybersecurity risks, threats, and incidents
- Assist with resource prioritization
- Reinforce statewide cybersecurity culture
- Coordinate cybersecurity workforce requirements and job opportunities
- Be informed of cybersecurity incidents and assist in remediation
- Develop and exercise Agency strategy to leverage capabilities and resources across the Agency
- Establish and maintain information security and privacy programs

ENTITY CYBERSECURITY MANAGEMENT

DEPARTMENT CIO

ISO

- Risk Identification Reporting and Mitigation
- Entity Cybersecurity Strategy
- Drive Cybersecurity Maturity
- Cybersecurity Capability Implementation
- Inform and Review Security Architecture
- Statewide and Agency Policy Compliance
- Entity Cybersecurity Policy and Standards
- Drive Security Culture and Awareness

- Inform entity of high-risk activities and remediation
- Create, manage, and publish security policies
- Drive security and privacy awareness and culture
- Oversee execution of cybersecurity capabilities
- Communicate with entity, business owners, and leaders on security requirements and operations
- Ensure confidentiality, integrity, and availability of entity data and services
- Establish and maintain information security and privacy programs

ANNEX D

CAL-SECURE AND CALIFORNIA HOMELAND SECURITY STRATEGY ALIGNMENT

CAL-SECURE

GOALS

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.

PEOPLE

- Develop pipeline for cybersecurity professionals
- Align cybersecurity roles with the National Initiative for Cybersecurity Education (NICE) framework
- Create a cybersecurity career path toolkit
- Expand tailored workshops for the state cybersecurity workforce

PROCESS

- Create tools for cybersecurity strategy development at state agencies and entities
- Formalize the cybersecurity governance structure
- Transform state information, privacy, and cybersecurity policies and standards
- Modernize cybersecurity procurement
- Create multi-tiered cybersecurity governance bodies
- Define cybersecurity technology requirements through community-led groups
- Integrate cybersecurity into the IT Modernization Roadmap

TECHNOLOGY

- Create a portfolio of cybersecurity as a service offerings
- Implement the Unified Integrated Risk Management platform
- Provide all state entities with security operations services
- Define cybersecurity technology requirements through community-led groups
- Integrate cybersecurity into the IT Modernization Roadmap

HOMELAND SECURITY STRATEGY

GOALS

Strengthen Security and Preparedness across Cyberspace

PLANNING AND ORGANIZATION

- Develop STAS-Cal-CSIC SOPs for cybersecurity information collection, analysis, and sharing among STAS
- Define standardized levels of cyber incident response capability (resource typing)
- Identify cyber incident response capability (resource typing) among SLTT partners
- Develop a statewide Cyber Incident Response Mutual Aid Criteria/Plan
- Identify gaps in funding for threat intelligence and cyber incident response
- Develop a succession plan for the state's information security workforce
- Develop a professional development plan for the state's information security workforce
- Publish a plan to promote and encourage cybersecurity training to recruit and retain the state's information security workforce

EXERCISES

- Conduct a cyber incident response exercise with SLTTP partners

ACKNOWLEDGMENTS

We would like to acknowledge the following California entities for their contribution to the California cybersecurity strategy.

Air Resources Board
Board of State and Community Corrections
Business, Consumer Services and Housing Agency
California Cybersecurity Integration Center
California Environmental Protection Agency
California Highway Patrol
California Lottery
California Military Department
California Prison Industry
Coastal Commission
Department of Aging
Department of Conservation
Department of Education
Department of Finance
Department of Fish and Wildlife
Department of Forestry and Fire Protection
Department of General Services
Department of Industrial Relations
Department of Insurance
Department of Motor Vehicles
Department of Parks and Recreation
Department of Pesticide Regulation
Department of Rehabilitation
Department of Resources Recycling and Recovery
Department of Toxic Substances Control
Department of Transportation
Department of Veterans Affairs
Employment Development Department
Financial Information System for California
Franchise Tax Board
Gambling Control Commission
Government Operations Agency
Governor's Office of Emergency Services
Health and Human Services Agency
Legislative Data Center
Natural Resources Agency
Office of Environmental Health Hazard Assessment
Office of Health Information Integrity
Office of Statewide Health Planning and Development
Office of the State Public Defender
Public Employees Retirement System
San Francisco Bay Conservation and Development Commission
Secretary of State
State Controller's Office
State Water Resources Control Board
Victim Compensation Board

707 3rd Street, Second Floor North • West Sacramento, CA 95605
Phone: (916) 319-9223