CAL-SECURE

State California
California Cybersecurity Integration Center

Cross-Boundary Collaboration and Partnerships

Project Completion: October 2021

Vitaliy Panych, California State Information Security Officer
Mark Ghilarducci, Director, California Office of Emergency Services

California Department of Technology

Cal OES Governor's Office

CHP

California Military Department

EXECUTIVE SUMMARY

Cal-Secure is the state's first universal cybersecurity initiative and marks the first time a large and diverse collection of contributing stakeholders—federal, state, local, education and private sector providers—collaborated to produce a security plan that outlines an overarching road map to prioritize initiatives and guide organizations at any level of maturity.

The success of Cal-Secure depends upon the input, information-sharing and adoption of guidelines by agencies and departments as well as federal, local, education, and private sector partners as part of a "one team, one fight" approach across government to manage cyber risks.

2020 introduced the world to the COVID-19 pandemic and with it came a 'cyber pandemic'.
As many employers turned to remote work, thousands of government institutions became low-hanging fruit for cybercriminals. In fact, 70% of all ransomware attacks in the United States continue to target state and local governments.

Between March and April 2020, approximately 75% or 190,000 California state government employees began teleworking. The logistics that such a remote workforce required could easily have created system and network vulnerabilities. California government leaders understood that a single security breach had the potential to disrupt the state's digital services supply chain. In response, California's united cybersecurity community came together to create a roadmap for government entities to bring their organizations up to a solid security standard and mitigate any existing gaps.

The outcome of this collaborative process was the State of California Executive Branch Multi-Year Information Security Maturity Roadmap—or Cal-Secure. Launched in 2021, the Cal-Secure roadmap is a world-class cybersecurity defense system that benefits the residents of California today and beyond. The plan focuses on three pillars to develop security capabilities: a diverse and innovative security workforce; an agile and flexible model; and an investment in technology and services to develop effective defenses to sustain the state's collective protection measures.

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

PROJECT NARRATIVE

Security incidents that compromise the integrity, confidentiality, and availability of information have affected numerous governments in recent years, especially during the COVID-19 pandemic. Some of these breaches resulted in the disclosure of confidential information or the shutdown of information systems and critical infrastructures. California has been no exception. In June 2020, a ransomware attack encrypted the data on a number of servers at the University of California, San Francisco (UCSF) School of Medicine. To recover the data, UCSF paid approximately $1.1 million to the individuals behind the attack. In March 2021, an employee at the State Controller's Office clicked an email link that appeared to come from a trusted outside entity and unknowingly provided a hacker with access to reports that may have included individuals' full names, addresses, Social Security numbers, and birth dates. The hacker then sent malicious emails to the employee's contacts. These types of incidents affect the state as a whole and put residents' sensitive data and other government information assets in jeopardy.

In response to the increasing number of cyberattacks, Governor Gavin Newsom's administration released Cal-Secure, the State of California's first multi-year cybersecurity roadmap. Built on industry-leading best practices and frameworks, Cal-Secure addresses critical gaps in the state's information and cybersecurity programs while enabling the state to manage existing and future threats more effectively. The roadmap defines a path for government entities to strengthen their security measures and prioritize resources to manage the most significant cyber risks while safeguarding services for Californians. This initiative is universal to all digital information providers and aligns with NASCIO's No. 1 State CIO Top Ten Policy and Technology Priorities for 2022: Cybersecurity and Risk Management.

IDEA

Does this look infected to you?

"Hackers steal our time, money, and peace of mind. Protecting our data is among the most important things we can do to prevent disruption to our daily lives and our economy. We have to do more to safeguard the state's critical infrastructure, intellectual property, and our status as one of the world's leading economies."

~ Governor Gavin Newsom

California's united cybersecurity community participated in the creation of Cal-Secure, which sets a new standard designed for all levels of California's government. Cal-Secure creates a world-class cybersecurity defense system that benefits the residents of California today and beyond. The plan focuses on building up technical capabilities, a security workforce and governance practices to help sustain the state's collective protection measures.

Cal-Secure is the state's first universal cybersecurity initiative and marks the first time such a large and diverse collection of contributing stakeholders—federal, state, local, education and private sector providers—collaborated to produce a security plan that outlines an overarching road map to prioritize initiatives and guide organizations at any level of maturity. The cybersecurity roadmap, calibrated with California's digital transformation initiatives, improves the delivery of services. The California Department of Technology (CDT) worked closely on critical operations with federal partners from the Department of Homeland Security, the California Cybersecurity Integration Center (Cal-CSIC), more than 40 California state departments, a consortium of education administrators and a variety of private-sector leaders.

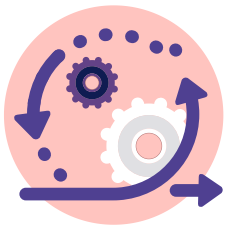
Cal-Secure's unified approach and centralized funding model outlines actionable steps and provides measurable success criteria to ensure adoption. Transparency with the provider community results in healthier and more efficient supply chain management. Collaboration across the private, public and academic sectors increases candidate pools and reinforces the security workforce pipeline to recruit and retain the next-generation security workforce. It is an adaptable support framework to guide organizations through a continually evolving security landscape.

IMPLEMENTATION

The three pillars and their initiatives that support Cal-Secure align with the principles of Vision 2023, California's statewide technology strategic plan. Collaborative working groups comprised of government, education and commercial participants were tasked to develop each pillar.

Vision 2023 Principles

Put people first



Create continuous and timely improvements

Working together beats working alone

Likewise, Cal-Secure is broken into three pillars, or roadmap categories: People, Process and Technology.

PEOPLE
World-Class Cybersecurity Workforce

PROCESS
Federated Cybersecurity Oversight

TECHNOLOGY
Effective Cybersecurity Defenses

PEOPLE: 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. As a result, California's Homeland Security Strategy (HSS) has statewide objectives to make cybersecurity workforce development and training a priority. To help address this challenge, California's executive branch takes a proactive approach to increase training opportunities for existing staff, as well as increase the executive branch will focus on throughout the next five years to improve its cybersecurity maturity and identify and manage risks to the state.

ROADMAP PRIORITIES

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

PROCESS: 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 the Office of Information Security. 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**

TECHNOLOGY: Invest in technology and services to enhance cybersecurity capabilities at all state entities.

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 baseline set of technical cybersecurity capabilities required for all state entities, along with a roadmap for prioritizing their implementation. Second, the strategy aligns with the state's IT modernization effort that aims to modernize legacy business processes and systems throughout the state. Finally, Cal-Secure calls for the collaboration of the California

ROADMAP PRIORITIES

- **Define baseline cybersecurity capabilities for state entities**
- **Foster cybersecurity by design through IT modernization**
- **Collaboratively tackle cybersecurity threats**

Department of Technology Security Operations Center Cal-CSIC, and all state entities to tackle threats across the state. The 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.

The Collaborative Process

California conducted more than 20 workshops and working sessions with 40 diversified entities, culminating in over 450 hours of community input into Cal-Secure. With this feedback, the state evolved its cybersecurity governance model into a multi-tiered structure that encourages communication and coordination through community partnerships, fosters agile cybersecurity strategy development among state leadership and the private sector, and ensures baseline technical cybersecurity capabilities required for the California's Executive Branch. While the baseline capabilities are already required by state policy, the roadmap removes any ambiguity by establishing specific, prioritized milestones that clearly define roles and responsibilities.

Cal-Secure's specific, prioritized roadmap depicts a 5-year horizon.Success is measured on a yearly basis according to CDT's Office of Information Security Foundational Framework (SIMM 5330-B), the California Cybersecurity Maturity Metric (SIMM 5300-C) and the California HSS. Collaboration and planning are a cornerstone of California's HSS to ensure the security, reliability, integrity, and continuity of critical cyber information and services. Implementation and realization of the Cal-Secure roadmap will require resources and leadership from the entire security community, including the vendor community. To ensure compliance, each goal is prioritized and sequenced for maximum impact ensuring ample time for planning, establishing resources and implementation. Entities are given implementation guidance and deadlines and mandated to report incidents. Dedicated resources to achieve initiatives come from the state's $38.8 million annual IT security budget.

IMPACT

Prior to Cal-Secure, California's state government relied on entities self-assuring that their security measures were up to date and met the baseline as defined in policy. However, that wasn't always the case. Some departments lagged in patching critical software updates, security audits and filling essential gaps that could leave them exposed. Cal-Secure defines a clear path for all entities to

Measuring progress is a key component of the security roadmap. All initiatives and priorities in Cal-Secure align with the Office of Information Security's Foundational Framework, the California Cybersecurity Maturity Metric and the California HSS, as previously stated. The table lists key aspirational metrics as targets for improvement.

follow and has received national recognition in the National Security Telecommunications Advisory Committee report to the President.

Measuring Success
Patterns of Adoption

CDT has been seeing adoption of the Cal-Secure framework by state and local government entities. Evidence of this adoption is found in state projects submitted to CDT's Technology Modernization Fund—a $25 million fund that works proactively to invest in projects to modernize digital services for residents and state employees—that align security priorities with the plan's guiding framework. Many Budget Change Proposals (BCPs) for state technology initiatives are also showing alignment with Cal-Secure.

Government organizations aren't alone in adopting the roadmap, so too are many of California's commercial providers that are mapping their own products' technologies and security capabilities to Cal-Secure. Cal-Secure standardizes practices through collaboration and transparency with the provider community, meaning healthier and more efficient supply chain management, services that are more optimized and cost effective, better at integrating information, and individuals that are risk-minded at every facet of an organization.

Cal-Secure demonstrates the need to leverage partnerships and best practices to expand core capabilities, especially the partnership with the California Cybersecurity Integration Center (Cal-CSIC), the central organizing hub of state government's cybersecurity activities that serves as a conduit for cybersecurity threat information between federal, state, local and tribal government entities. Sharing core capabilities and leveraging partnerships dramatically increases California's ability to detect, protect and respond to cybersecurity threats. By the end of 2023, all state entities, regardless of size or business, will be part of this ecosystem.

Cal-Secure's tiered effort to consolidate and centralize security tactics enables government to operate at a faster pace and scale up to meet the threats of an ever-changing landscape. Its centralized auditing program identifies gaps and provides agencies the support to address deficiencies using consolidated and reusable capabilities and services within the state. As of May 2022, compliance is in the ninetieth percentile. Furthermore, Cal-Secure provides supports to entities that do not have the staffing or capability to monitor and protect their internal networks: nearly 30 entities have been onboarded to the Security Operations Center for enhanced monitoring. Cal-Secure ensures that as we head into a world where crime is increasingly conducted using cyber-enabled tactics, California will be prepared for the next generation of security risks.