California Department of Technology

CAL-SECURE 2.0

State of California Executive Branch
Multi-Year Information Security Maturity Roadmap

Table of Contents

Cal-Secure 2.0 is a living document, and subject to refinement and expansion by the CDT in the future.

The latest version of Cal-Secure 2.0 and the Cal-Secure 2.0 Toolkit can be downloaded at https://www.cdt.ca.gov/

Message From the State CIO and State CISO

As California advances its commitment to “California for All” and delivers on the promise of an inclusive digital experience for everyone, we acknowledge the ever-increasing responsibility to safeguard our residents and ensure the uninterrupted delivery of vital public services. The accelerated pace and complexity of cyber threats today is fueled by Artificial Intelligence, agentic attackers operating at machine speed, and a time-to-exploit window that has collapsed from months to hours. To match the velocity of these threats, there is an elevated demand for unwavering vigilance, proactive leadership, and innovation.

Guided by our core values of Transparency, Collaboration, and Innovation, **our mission for the next five years is to help every level of government become future-ready, remain responsive to emerging threats, and serve Californians today while anticipating tomorrow’s needs**. Cybersecurity is no longer an afterthought; it is foundational to the continuity of state services and the trust Californians place in their government. Every benefits payment, every public safety system, every health record, every transportation system depends on it. Cal-Secure 2.0 is our commitment that California will modernize boldly and securely, while adopting AI and other emerging technologies in a manner that enhances privacy, protects services, and keeps our residents safe. Cal-Secure 2.0 fulfils this mission by equipping state agencies and entities to proactively strengthen their resilience in the face of technological advancements and the increased pace and sophistication of cyber threats.

Cal-Secure 2.0 builds on the solid foundation of California’s original cybersecurity initiatives, evolving to adopt a risk-based approach to cybersecurity and addressing technological advancements such as Artificial Intelligence and Quantum Encryption. State entities are empowered to turn collective vision into action, forging a secure, adaptive, and inclusive cyber future for California. We accomplish this in alignment with the State Government Annual Technology Strategy: Envision 2026, by strengthening and connecting the three foundational components of People, Process, and Technology.

Cal-Secure 2.0 establishes flexible governance models that prioritize partnerships across all levels of government, fostering a unified approach to risk management and oversight. Our focus on measurable outcomes ensures that every initiative demonstrably strengthens our collective security, so California remains agile and accountable in the face of evolving threats.

Together, we remain committed to protecting essential services, empowering our government, and building the trust that is foundational to California’s success in the digital era.

Chris Given
Director and State Chief Information Officer

Vitaliy Panych
State Chief Information Security Officer

Executive Summary

State and local governments across the nation are facing an increasingly complex and diverse cyber threat landscape. Rapid technological advancements have led to new attack techniques powered by Artificial Intelligence, including AI-orchestrated intrusion campaigns, autonomous vulnerability discovery, and machine-speed exploitation of newly disclosed flaws. Recognizing this environment, the California Department of Technology (CDT) and its Office of Information Security (OIS) are pleased to release Cal-Secure 2.0: a forward-thinking approach designed to position California at the leading edge of cybersecurity excellence, enable the state to ensure the uninterrupted delivery of vital public services, and protect residents and their information.

Cal-Secure 2.0 empowers and guides California's agencies and boards, departments, and offices ("entities") to execute individual cybersecurity strategies and capabilities, instead of being a compliance document or one-time checklist. Developed in collaboration with the California Cybersecurity Integration Center (Cal-CSIC), the California Governor's Office of Emergency Services (CalOES), California Highway Patrol (CHP), California Military Department (CMD) and cybersecurity leaders from across the state, Cal-Secure 2.0 recognizes today's realities while anticipating tomorrow's opportunities.

Cal-Secure 2.0 Components

Aligned to the State Government Annual Technology Strategy: Envision 2026, Cal-Secure 2.0 is organized around the three strategic components of People, Process, and Technology. Within these components, ten key priorities and fifteen forward-looking initiatives provide structure, while toolkits offer mechanisms for entities to understand their cybersecurity maturity journey and implement new technical capabilities.

People

Build a ready, capable, and diverse public sector cybersecurity workforce and be known as a place to grow a mission-driven career.

Process

Strengthen collaboration, integration, and accountability to provide effective statewide oversight.

Technology

Invest in modern tools and services to protect California's data and systems from new and growing cyber threats.

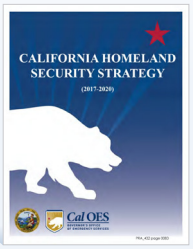
Building on the strong foundation established by the initial Cal-Secure in 2021, Cal-Secure 2.0 is an evolution of the state's cybersecurity approach in several important ways:

- It adopts a risk-based approach to cybersecurity tailored to the diverse profiles and missions of entities.
- It empowers cybersecurity leaders to clearly convey security value and outcomes to business and legislative stakeholders.
- It incorporates strategies for the secure adoption, operation, and continuous oversight of emerging technologies including generative AI and post-quantum cryptography, capturing the benefits of these technologies while minimizing new risks.
- It provides actionable resources to all entities across different stages of their cybersecurity journey, offering clarity and transparency in the direction of statewide progress.
- It unifies the state's cybersecurity approach as a call to action and adoption for all entities across varying maturity levels and reporting requirements.
- It recognizes that no single entity defends California alone, Cal-Secure 2.0 is delivered in partnership with private-sector cloud, telecom, and technology providers; federal partners; academia; local governments; and the broader cybersecurity community.

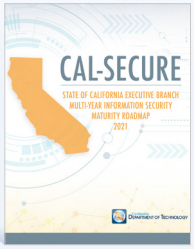
Cal-Secure 2021 Retrospective

The Cal-Secure Multi-Year Information Security Maturity Roadmap, published in 2021, set a clear five-year objective: ensure California's Executive branch had a world-class cybersecurity workforce, an empowered and right-sized federated cybersecurity oversight governance structure, and effective cybersecurity defenses across all technology, including critical infrastructure.

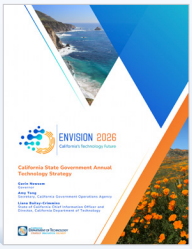
Since the introduction of Cal-Secure, thousands of dedicated cybersecurity professionals have made significant progress towards this goal by implementing technical capabilities and community-driven initiatives. These efforts have established a solid foundation for continued improvement and increased maturity across the state's cybersecurity landscape.



Vision 2023



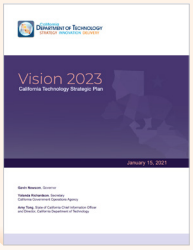
California Homeland Security Strategy



Cal-Secure 2.0

2017 — **California Homeland Security Strategy**

2020 — Vision 2023

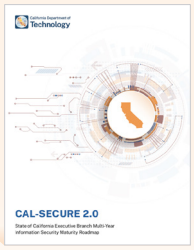


2021 — **Cal-Secure**

2021 — California Homeland Security Strategy

2024 — **Envision 2026**

2026 — Cal-Secure 2.0



From 2019-2020, California has invested over $1 billion to enhance cybersecurity across state government. As a result, Executive Branch Agencies and Departments have reached over 80% completion on all 4 Cal-Secure capability priorities , with progress trending positively despite increasingly sophisticated risks and threats.

Cal-Secure's comprehensiveness, ongoing audits, independent security assessments, and the state's agile response have positioned entities to better anticipate and address emerging threats.

To maintain the momentum of Cal-Secure, it is important to identify the resources and efficiencies that will accelerate progress statewide.

Cal-Secure anticipated the trajectory of the threat landscape over the past five years, but state government is threatened by attacks that have grown faster, larger in scale, and more sophisticated.

This drives the need for a refreshed cybersecurity approach that addresses today's risks and adapts as they evolve.

As new threats including ransomware-as-a-service, GenAI-enabled social engineering, prompt-injection attacks against AI agents, and state-sponsored threats to critical infrastructure continue to evolve, Cal-Secure and its ongoing implementation of technical capabilities and strategic initiatives will continue to play a pivotal role in enhancing California's defenses. Building on the success of Cal-Secure, sustained legislative backing and collaboration between CDT, Cal-CSIC, CalOES, CHP, and CMD remain vital to sustain progress and drive adoption of Cal-Secure 2.0.

Foundational Guidance – Purpose, Vision & Values

Mission

> Our mission for the next five years is to help every level of government become future-ready, remain responsive to emerging threats, and serve Californians today while anticipating tomorrow's needs.

Chris Given and Vitaliy Panych
State CIO and State CISO

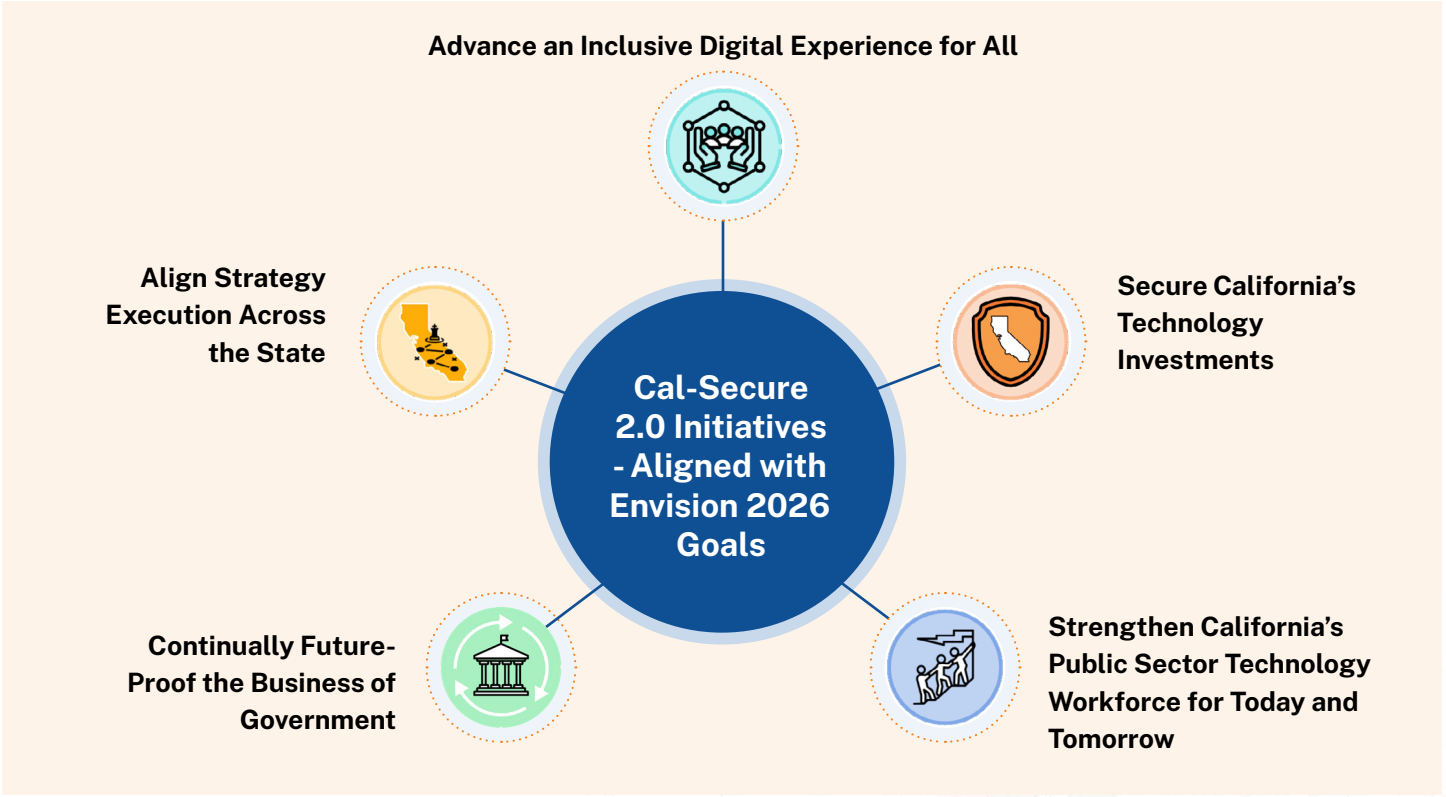
Purpose

The purpose of Cal-Secure 2.0 is to strengthen California's cybersecurity maturity and preparedness, overcoming adoption barriers, and enabling cybersecurity capabilities allowing state entities to continue delivering critical services to Californians and protect their information.

Values

Transparency **Collaboration** **Innovation**

Transparency, Collaboration, and Innovation are the guiding values of Cal-Secure 2.0, ensuring that as California adopts new defensive capabilities, it does so responsibly, with transparency to Californians about how emerging tools and techniques protect their services and data, collaboration across agencies, experts, and communities to identify and address unintended consequences, and innovation grounded in human oversight, continuous validation, and clear boundaries on autonomous action. Together, these values keep the state future-ready by building public trust, turning statewide alignment into consistent execution, and driving smarter investments that outpace evolving threats without outrunning accountability.



Cal-Secure 2.0 Overview

Cal-Secure 2.0 innovates on the ideas of privacy, safety, and resilience to provide clear, risk-centric direction to all state entities as they develop their own cybersecurity strategies. It recognizes that cybersecurity maturity is not a one-time goal but a continuous practice that must evolve alongside the threat landscape and new technologies that the state adopts.

Purpose and Intended Use	Developed to support state agencies and entities, Cal-Secure 2.0 provides a common framework for building entity-level cybersecurity strategies. It establishes statewide priorities and links them to tactical and operational steps needed to adopt the capabilities and initiatives defined in the Cal-Secure 2.0 components. This approach enables all entities to prioritize and improve cybersecurity maturity regardless of their current resources or maturity level, driving improvements in the services and operations that support Californians..
Organizing Construct: People, Process, and Technology	Similar to Cal-Secure 2021, the document continues to be organized into the components of **People, Process, and Technology.** These components must be equally addressed and balanced by entities to sustain progress. Each component includes goals and priorities to guide execution, along with actionable initiatives, which, when achieved, will make a measurable impact on the success of the priorities.
Starting Point	Entities should consider leveraging the **Cal-Secure 2.0 Toolkit** and the embedded **Capability Map**, which identifies the cybersecurity capabilities that OIS has prioritized for entities to adopt and implement over the next five years. The map aligns to the six functions of the NIST Cybersecurity Framework (CSF) 2.0: **Govern, Identify, Protect, Detect, Respond,** and **Recover** and to the capability tiers defined on the following page, so entities can distinguish foundational controls from advanced and emerging-technology capabilities (applicable as each entity's mission, risk, and maturity warrant).
Capability Prioritization and Maturity Measurement	The **Cal-Secure 2.0 Toolkit** includes **Organizational Profiles** rooted in NIST CSF 2.0 concepts, which help entities understand their current and target states, and prioritize capability adoption and implementation using a **risk-based approach rooted in NIST SP 800-37 Risk Management Framework** that factors their mission, risk appetite, criticality of systems, and the data they protect. The **Organizational Profile** accompanies the **Maturity Matrix** that expands on the capabilities in the **Capability Map** by defining distinct maturity levels for each, allowing entities to understand their current and target states. The Cal-Secure 2.0 Toolkit is a "living" document and may be updated by CDT at any time.
Support, Services, and Resources	The **Service Catalog and Resources** provides a catalog of centralized cybersecurity operations and advisory services offered by CDT and Cal-CSIC, along with procurement learning and additional resources to help entities adopt Cal-Secure 2.0 and improve their cybersecurity maturity.

Cal-Secure 2.0 Strategy

People

Goal: Build a ready, capable, and diverse public sector cybersecurity workforce and be known as a place to grow a mission-driven career.

Across the nation and in California, the demand for skilled cybersecurity professionals far outpaces the available supply. State governments nationwide identify cybersecurity staffing and availability of professionals as a key challenge. The state is tackling this head-on by prioritizing learning and skills development, streamlining hiring, fostering cross-agency talent pools and shared expertise, and building an environment where employees can build lasting, meaningful careers in public service. Through statewide collaboration and a commitment to career growth, state entities will be equipped with a workforce prepared for today's and tomorrow's cybersecurity needs.

Priorities

- Effective organizational cybersecurity workforce planning strategies, inspiring statewide cybersecurity culture.
- Streamline hiring process and align recruitment, retention, and development activities with industry best practices.
- Learning, skills development, and career growth for Californians through training.

Initiatives

Tailored Cybersecurity Training Workshops and Learning Pathways

Expand well-targeted, role-based training workshops and create personalized learning pathways across technical, leadership, and cross-functional skillsets for California's public sector cybersecurity workforce.

Standardized Cybersecurity Career Pathways and Retention Toolkit

Develop and implement a statewide toolkit that aligns all cybersecurity roles to the NICE framework, outlines growth trajectories, and provides agencies with strategies and resources for talent retention.

Cybersecurity Communication Skills Development

Institute targeted communication and risk-translation training for cybersecurity professionals, focusing on how to convey technical risks and concepts to non-technical audiences and executives.

Streamlined Cybersecurity Hiring and Onboarding

Review and refine the end-to-end hiring and onboarding processes for public sector cybersecurity positions, drawing on current workforce best practices to reduce time-to-hire and improve retention of new recruits.

Vendor and Resource Sharing Education Program

Create a coordinated education program for agencies on effective resource sharing (talent, knowledge, and operational resources) and vendor engagement to leverage best available tools, training, and support.

Priorities

Effective organizational cybersecurity workforce planning strategies, inspiring statewide cybersecurity culture.

The state is adopting data-driven workforce planning to anticipate and address workforce needs, skills gaps, and organizational changes. Coordinated efforts across California fostered by recognition programs and leadership example will create a statewide cybersecurity culture that values continuous improvement, shared responsibility, and collaboration. These efforts will ultimately empower all employees to take part in safeguarding California's residents by protecting data and systems.

Workforce Data » **Anticipate Workforce Needs** » **Recognition Programs** » **Empowered Employees**

Streamline hiring process and align recruitment, retention, and development activities with industry best practices.

California is streamlining its hiring process and aligning recruitment, retention, and staff development activities with industry best practices. By simplifying application procedures, reducing time-to-hire, providing ongoing support, and offering professional development opportunities, California will attract top cybersecurity talent and create a workforce prepared to meet tomorrow's cybersecurity needs.

Recruitment **Retention** **Development**

Learning, skills development, and career growth for Californians through training.

California is prioritizing continuous learning and targeted development for staff at all levels through training programs that cover technical skills, leadership, problem-solving, communication, and the secure use of AI and agentic tools. Cybersecurity leaders will be trained in areas like procurement, finance, and executive communication to better convey cybersecurity needs to business and non-technical stakeholders. Personalized learning pathways and ongoing professional development will build a workforce equipped to address evolving challenges and motivated to pursue long-term careers in public service.

ALL STATE EMPLOYEES

Baseline Cybersecurity and Privacy Training

- Baseline Cybersecurity and Privacy Training
- Continuous phishing training
- Increased web-based training

AWARENESS

Security-minded culture

CYBERSECURITY PROFESSIONALS

Advanced Cybersecurity and Privacy Training

- Specialized Cybersecurity and Privacy Training
- External certifications
- Cybersecurity workshops

Cybersecurity Management Leadership Training

- Information Security Leadership Academy
- Cybersecurity leadership programs through partnerships

CAREER DEVELOPMENT

Trained, knowledgeable, agile cybersecurity professionals

Cal-Secure 2.0 Strategy

Process

Goal: Strengthen collaboration, integration, and accountability to provide effective statewide oversight.

California hopes to strengthen cybersecurity outcomes and improve oversight over all state entities by empowering them to address their unique needs while aligning to national and statewide standards. As AI-accelerated threats compress response windows, processes themselves must operate faster, and governance, procurement, patch deployment, and incident escalation will need to follow suit. Centralized services, shared toolkits, continuous assessment mechanisms, and standardized metrics will translate strategy into clear and effective processes –defined workflows that will guide actions and decisions across entities. Streamlined policies and modernized procurement will accelerate execution, drive consistency, and foster a culture of statewide collaboration and continuous improvement.

Priorities

- Collaborate and integrate cybersecurity strategy across CDT, agencies, and entities for collective cybersecurity maturity
- Adopt a risk-based approach to execute cybersecurity strategies and achieve cybersecurity maturity.
- Refine cybersecurity requirements and track statewide progress.
- Cross-functional collaboration for coordinated cybersecurity strategy execution.

Initiatives

Standardize and Automate Cybersecurity Metrics & Reporting

Set statewide cybersecurity metric standards and deploy tools to automate entity maturity reporting and evaluation. Update risk models, KPIs, and reporting cadences to reflect AI-accelerated exploit timelines, machine-speed attack complexity, and resilience-focused. Conduct regular security audits, self-assessments, peer reviews, and continuous-control validation, and targeted risk mitigation across entities.

Formalize and Evolve Multi-Tiered Cybersecurity Governance

Support structured, multi-level governance with clear roles, escalation procedures, and collaborative forums to align statewide and entity cybersecurity oversight with business objectives. The CalOES Cyber Task Force will work to facilitate this governance, exercising statewide escalation procedures, cross-entity coordination, and pre-authorized decision rights periodically so the state can mount a Cal-CSIC coordinated response rather than a dispersed one when critical cybersecurity events occur.

Develop and Deploy Cybersecurity Strategy & Planning Toolkits

Develop and distribute standardized toolkits and guidance to help entities design, implement, and sustain customized cybersecurity strategies aligned with Cal-Secure 2.0 and industry best practices.

Continuous Security Audit, Assessment and Improvement Program

Offer core cybersecurity advisory services, including consultations, pre and post audit workshops, and other resources as shared solutions accessible to all entities.

Initiatives

Enhance Cybersecurity Procurement Processes

Streamline procurement processes and considerations to enable entities to efficiently access, acquire, and deploy vetted cybersecurity solutions. Establish a fast-track pathway for AI-enabled defensive technologies and agentic-security controls, so statewide adoption of proven new capabilities is not bottlenecked by approval cycles that predate the current threat environment.

Strengthen Public-Private and Cross-Government Collaboration

Formalize collaboration with the private sector, federal partners , academic institutions, local government, and information-sharing organizations. Strive towards joint tabletop exercises, bi-directional threat-intelligence sharing, and shared playbooks for sector-spanning incidents to bring together the combined strength of California to defend critical services.

Priorities

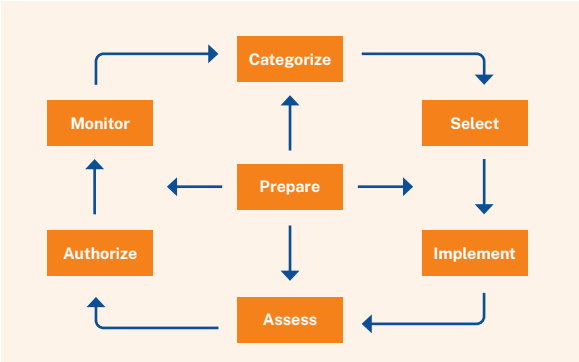
Collaborate and integrate cybersecurity strategy across CDT, agencies, and entities for collective cybersecurity maturity.

The state will encourage a continuous feedback loop, where statewide direction is translated into agency plans, executed by entities, and improved through measured outcomes and lessons learned. CDT OIS will publish and maintain statewide cybersecurity goals and priorities, common definitions of capability and maturity levels and measurement. Agencies will be empowered to provide specific guidance and coordinate consistent implementation within the agency. Entities can select, prioritize, and implement capabilities based on their mission and risk profile, while reporting feedback and lessons learned to the state to collectively increase California's cybersecurity maturity.

Adopt a risk-based approach to execute cybersecurity strategies and achieve cybersecurity maturity.

Acknowledging that entities have different missions, threat profiles, regulatory obligations, and that many protect critical infrastructure and residents' information, a risk-based approach rooted in NIST SP 800-37 Risk Management Framework (RMF) allows entities to select and prioritize the specific Cal-Secure

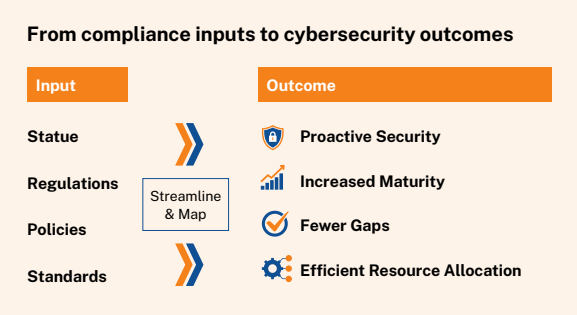
2.0 capabilities and initiatives that align with their needs, while maintaining a consistent statewide approach to improving and measuring cybersecurity maturity.



Priorities

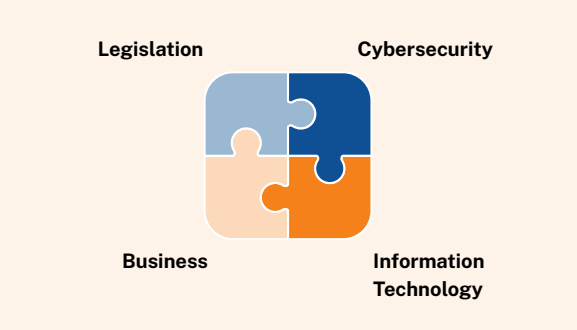
Refine cybersecurity requirements and track statewide progress.

California's cybersecurity governance, risk, and compliance landscape is shaped by a broad set of statutes, regulations, policies, and standards. Giving entities consistency and collaboration within these governing requirements enables them to devote resources efficiently to consistent and proactive security measures. These measures support cybersecurity maturity measurement, identify persistent gaps, and ensure requirements genuinely support improved security outcomes, including the emerging security outcomes required for safe AI adoption and the resilience outcomes required in a machine-speed threat environment.



Cross-functional collaboration for coordinated cybersecurity strategy execution.

Cybersecurity strategy execution requires coordination across legislative, cybersecurity, information technology, and business leadership within entities. Entities will break down silos and develop their own strategies that are closely tied to operational goals and business objectives. Joint decision-making will balance risk management with mission delivery, identify resource needs, and respond cohesively to incidents.



Process – Closing Thoughts

Plan proactively for vendor-ecosystem consolidation. As AI-native defensive capabilities become table-stakes, a meaningful share of legacy security vendors may not successfully transition. Multi-year procurement roadmaps, contract renewal cycles, and architectural decisions should anticipate vendor churn and adopt open standards, interoperable APIs, data portability, and avoiding deep lock-in to any single point in a security stack that may be acquired, deprecated, or superseded within the roadmap horizon.

Cal-Secure 2.0 Strategy

Technology

Goal: Invest in modern tools and services to protect California's data and systems from new and growing cyber threats.

We are committed to continuous technology modernization and proactive defense as legacy systems fall further behind, and threat actor technology improves at an increasing rate. While rapid advances in emerging technologies amplify both risks and opportunities, California will prioritize investments in foundational technical capabilities, real-time and runtime, and adaptive countermeasures that match the speed and scale of modern threats. Collaboration with industry and academia partners, along with improved access and availability for cybersecurity technology and infrastructure, empowers entities to not only safeguard critical data and systems, but also lead adoption of new solutions that strengthen the state's cybersecurity posture for the future.

Priorities

- Collaborate with industry and academia to adapt to evolving threats and technological advancements, including AI and GenAI.
- Safeguard California's data and technology assets from malicious attacks through proactive monitoring and risk analysis.
- Make cybersecurity technology and infrastructure accessible and highly available for entities of all sizes.

Initiatives

Enhance Security Operations with Artificial Intelligence and Automation

Incorporate AI-driven analytics and automation into cybersecurity operations to match attacker speed and scale. Uses include automated triage and enrichment, continuous exposure management, automated penetration testing and adversary emulation, AI-assisted detection engineering, and response playbooks. Coordinate detection capabilities with the statewide detection and runtime security program, which together supply the behavioral signals on which automated responses act.

Provide Statewide Security Services through Shared Cyber Portfolio

Offer core cybersecurity services, including threat monitoring, incident response, vulnerability management, and secure hosting, as shared solutions accessible to all agencies and entities.

Statewide Cybersecurity Innovation Lab

In partnership with the Cal-CSIC, reinvigorate and expand the existing cyber range to serve as a shared platform for jointly developing, testing, and validating emerging technologies and defense strategies before production deployment. By evolving the range, the state establishes a collaborative sandbox for safely evaluating third-party tools and emerging capabilities prior to statewide adoption without placing the full resource burden on any single entity.

Initiatives

Strengthen Critical Infrastructure, Operational Technology, and Cyber Recovery Capabilities

Continuously develop, validate, and enhance protection mechanisms for critical infrastructure and operational technology (OT) systems across all levels of government, including transportation, water, energy, and public-safety systems. Treat cyber recovery as distinct from traditional disaster recovery and invest in backup, recovery, and protective technologies. Test recovery under realistic ransomware and supply-chain scenarios to ensure critical systems can be restored to a trusted state within defined windows.

Enhance Statewide Threat Intelligence Fusion Programs with Cal-CSIC

Strengthen statewide cyber threat intelligence by formalizing partnerships, investing in automated platforms, and sharing actionable intelligence across all government levels.

Prepare for Post-Quantum Cryptography

Prepare the state's cryptographic infrastructure for the post-quantum era. Inventory cryptographic use across state systems (protocols, libraries, key lengths, certificate authorities, embedded devices). Establish crypto-agility to enable the ability to change algorithms without re-architecting applications. Track and adopt NIST-standardized post-quantum algorithms as they are published and validated.

Accelerate Vulnerability and Patch Management

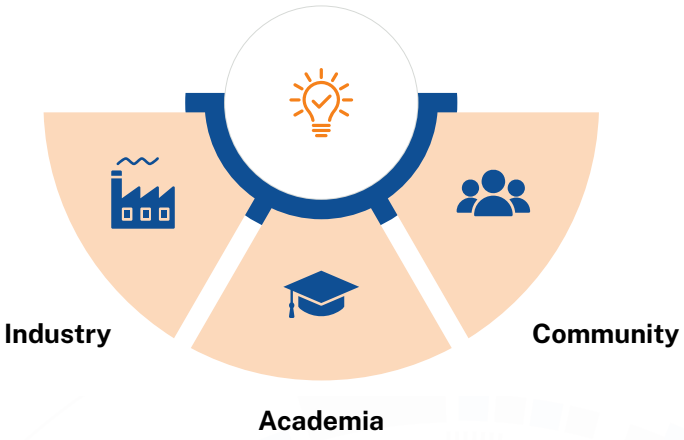
Build a Vulnerability Operations capability that treats vulnerability discovery, triage, and remediation with the same rigor and automation as DevOps. Use AI agents to discover vulnerabilities in state-owned code and third-party software before adversaries do; automate triage, severity classification, and patch testing; and, where mature, automated remediation. Update statewide patching cadences to align with the actual speed of exploitation.

Priorities

Collaborate with industry and academia to adapt to evolving threats and technological advancements, including AI and GenAI.

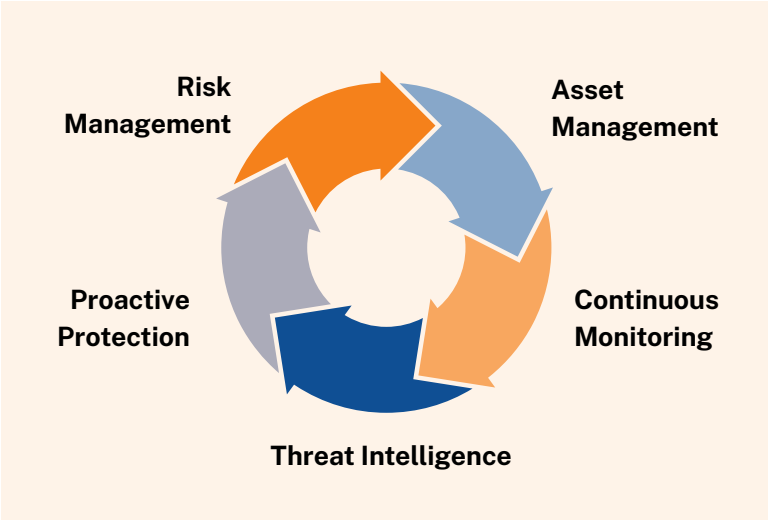
The state will foster collaboration between the state, industry, academia, and the broader cybersecurity community to access cutting-edge research, intelligence, and emerging technologies that drive cybersecurity maturity. These partnerships will bring fresh perspectives and innovative approaches to complex security problems, allowing entities to stay ahead of increasingly sophisticated threats.

Ongoing information sharing through the Cal-CSIC and co-development of solutions with partners will ensure adaptive defenses and agile cybersecurity strategies..



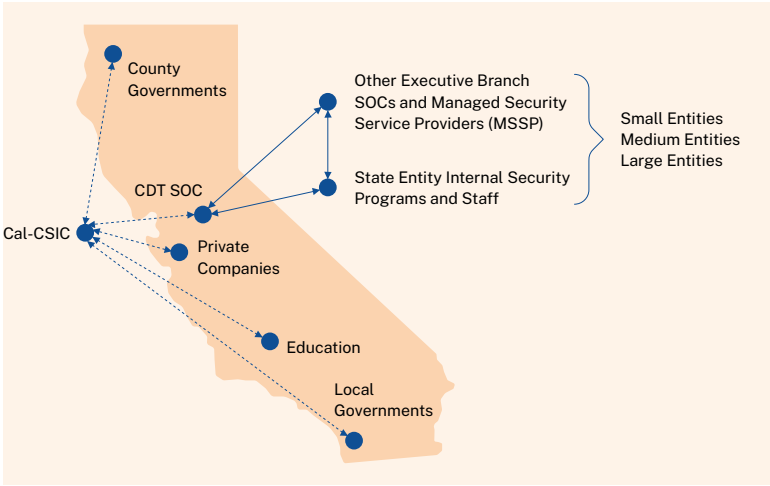
Priorities

Safeguard California's data and technology assets from malicious attacks through proactive monitoring and risk analysis.



California is transitioning from reactive defense to a proactive, intelligence-driven approach to protect residents' sensitive data and safeguard critical infrastructure. The shift in mindset rethinks data as not just bits of information but as an asset core to the State's mission. Continuous system, network, and runtime monitoring including for AI systems and agent behavior will enable early detection of threat activity before it escalates into damage. Static posture analysis alone cannot keep pace with machine-speed attacks; runtime telemetry provides the behavioral analysis required to detect adversaries by what they do, not just by what a configuration scan suggests they might be able to do. Where prevention is not possible (for example, against zero-day vulnerabilities not yet disclosed), deception and behavioral analytics identify adversaries by their actions rather than by known signatures.

Make cybersecurity technology and infrastructure accessible and highly available for agencies and entities of all sizes.



For cybersecurity technology and services to be effective in defense against evolving threats, they must be both accessible and highly available for all state entities. CDT and Cal-CSIC will work to support shared services, scalable solutions, and centralized resources to entities regardless of their maturity. Shared services for these entities include managed detection and response, managed deception, managed runtime security, managed vulnerability and patch management.

This will provide statewide enterprise-level protection, rapid adaptation to new threats, and a unified approach to safeguarding critical data and services.

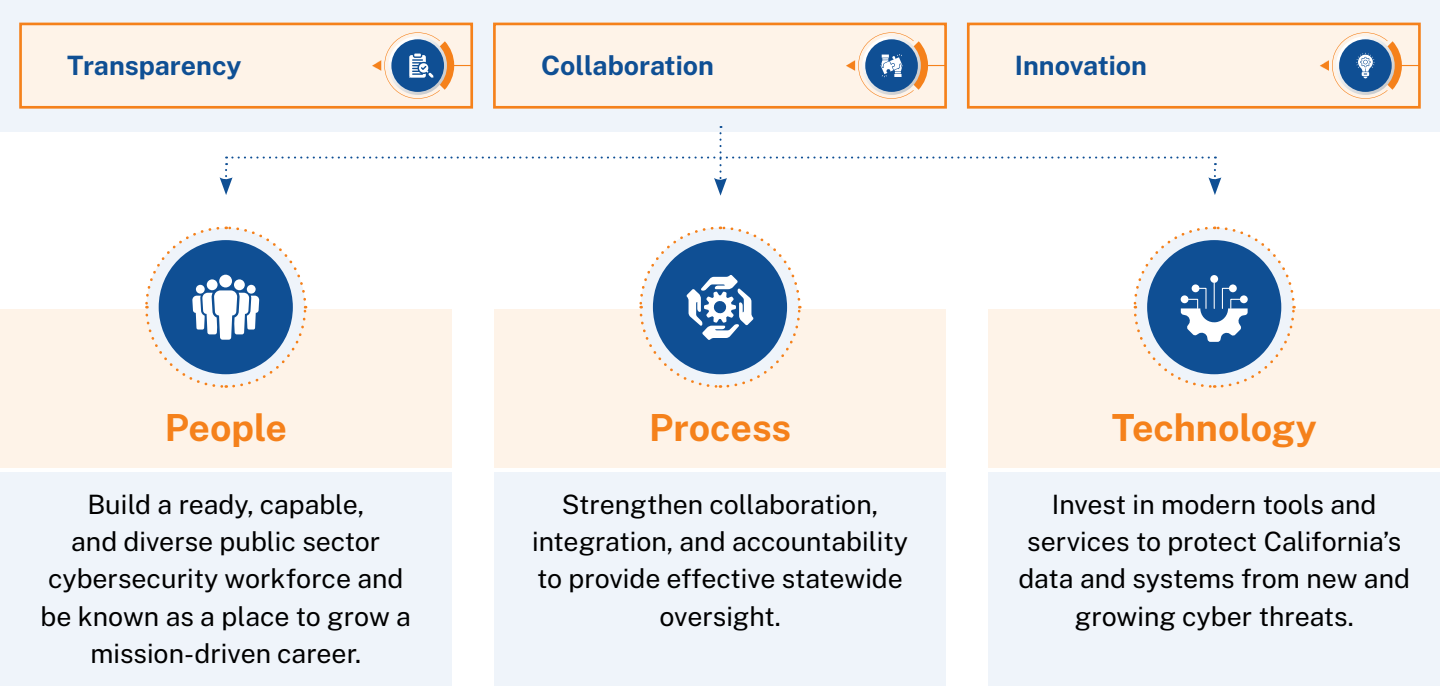
A Statewide Approach to Cybersecurity Maturity

The priorities and initiatives laid out across the Cal-Secure 2.0 components of People, Process, and Technology map out a path for the state to deliver on its mission to help every level of government become future-ready, remain responsive to emerging threats, and serve Californians today while anticipating tomorrow's needs. To sustain progress and deliver on this goal, each priority and initiative deserves equal focus while keeping top of mind Cal-Secure 2.0's values of transparency, collaboration, and innovation.

Transparency creates shared expectations and clear visibility into progress, ensuring everyone is working from common definitions, priorities, and measurements. The measures laid out in Cal-Secure 2.0 enable OIS to understand statewide cybersecurity maturity and act quickly based on what the data shows. Transparency to California residents about the measures taken to keep them and their data safe builds trust and confidence.

Collaboration is what makes Cal-Secure 2.0 truly statewide, aligning CDT, agencies, and partner entities around shared outcomes. Within each organization, cross-functional coordination among business, information technology, and cybersecurity turns that alignment into consistent execution.

Innovation keeps California future-ready by advancing skills, operating models, and risk-based individual cybersecurity strategies, supporting smarter investments and faster adoption of emerging technology safely and responsibly so California can embrace AI and other powerful tools in a manner that enhances privacy, protects services, and keeps our residents safe.



Cal-Secure 2.0 is a living roadmap. As threats, technologies, and public services evolve, CDT will maintain and refine it in partnership with state agencies, federal and local government, private-sector providers, academia, and the broader cybersecurity community, because keeping California safe is a shared commitment. To put the roadmap into practice, cybersecurity leaders and staff should reference the **Cal-Secure 2.0 Toolkit** to assess their current maturity, set target states, and chart a progression across People, Process, and Technology based on the capabilities OIS has prioritized for the next five years.

California Department of
Technology