



OEM: Weekly SITREP

November 02, 2021

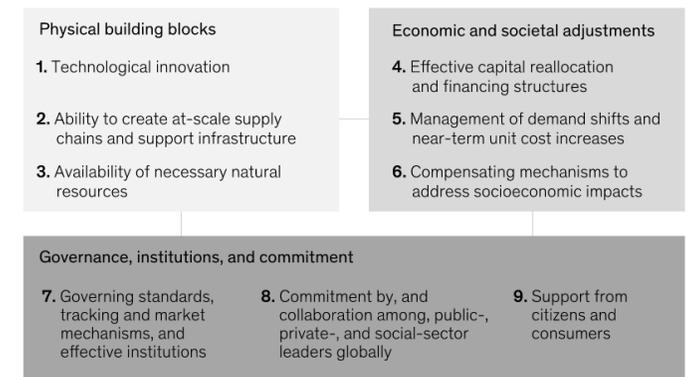
USA & WORLD

- NYC Vaccine Mandate: [Contingencies](#) in place as mass layoffs loom.
- Neurological [complications](#) after first dose of COVID-19 vaccines.
- [Fireproofing](#) America's forests.
- CDC: [\\$26M](#) for infectious disease forecasting.
- Antibiotic resistance at a [crisis point](#) – new drugs needed.
- [Timeline](#) for potential attacks by Islamic State against the West.
- 100 days until Winter Olympics: Beijing races to [control](#) Covid.
- [Racial reckoning](#) in the US: Expanding global transitional justice.
- Proposed new [Wealth Tax](#) explained.
- FBI: 4,071 more police officers [assaulted](#) in 2020 than 2019.
- China [lockdown](#): new Covid outbreak to worsen in coming days.
- In major shift, NIH [admits](#) funding risky virus research in Wuhan.
- How Public Health took part in its own [downfall](#).
- What's in the megabill? [Cheat sheet](#) on 12 big topics.
- China using '[wide variety](#)' of methods to steal trade secrets.
- Russia [targeting](#) technology supply chains.
- NSA awards [\\$500,000 cybersecurity grant](#) to University of Missouri.
- The [Facebook Papers](#): What to know about the insider documents.
- US troops have been [training](#) Taiwanese forces.
- UK military honing "[economic warfare](#)" skills to counter cyber-ops.



- The 26th UN Climate Change Conference of the Parties (COP26) summit will bring parties together to accelerate action towards the goals of the Paris Agreement and the UN Framework Convention on Climate Change.
- [74 countries](#) –accounting for more than 80 percent of global GDP and almost 70 percent of global CO2 emissions—have put net-zero commitments in place.

There are nine requirements for solving the net-zero equation and ensuring an orderly transition.



CALIFORNIA

- State [renews](#) \$1.7 billion contract with troubled COVID lab.
- [Partnership](#) aims to expedite port, infrastructure projects.
- [Testimony](#) about wildland firefighting workforce reforms.
- How trade unions and climate advocates can forge an [alliance](#).
- Recent storm caused rockslide – forces [Highway 1](#) closure.
- Key prosecutors are [leaving](#) SF DA's office to join the recall effort.
- UC Hastings [reckons](#) with the shame of native massacres.
- [Study](#): State facing massive [groundwater contamination](#).
- Newsom touts recovery, but employment [data](#) says otherwise.
- Carson declares [emergency](#) over a strong noxious smell.
- Gas [prices](#) continue to rise - most expensive in U.S.
- Lawrence Berkeley National Lab: Managing [water](#) resources.
- Did changes to [high-speed rail spending](#) break the law?
- Unemployment fraud reaches at least [\\$20 billion](#).
- Insurers [owe no coverage](#) for COVID-19 interruption losses.
- California is [2nd toughest place](#) in U.S. to find a job.
- The state's [four](#) main problems.
- Newsom visits [UC Merced](#), highlights equity efforts of med school.
- [Visualizing](#) California's stunning shipping gridlock.
- [\\$24 billion](#) in goods is floating outside California's biggest ports.

California Climate Investments



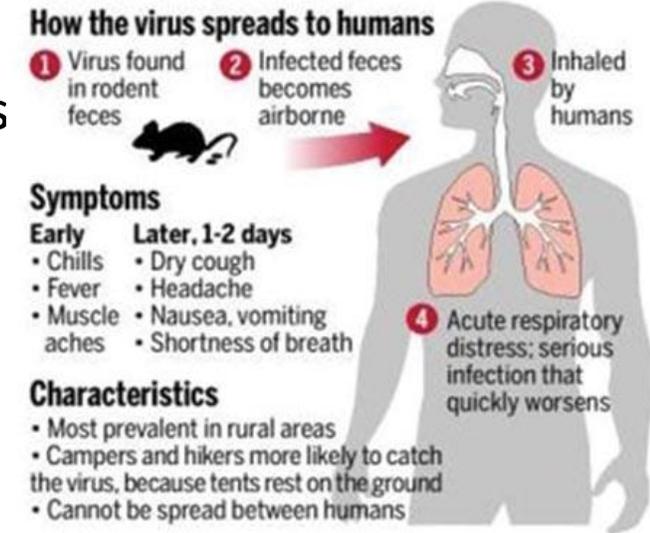
- **California Climate Investments Project shows [project level information](#) on California Climate Investments using Cap-and-Trade auction proceeds.**
- **These projects are a subset of a larger and coordinated effort to make climate and energy investments throughout California that further the State's climate goals.**
- **[Universities and research institutions](#) can apply for cap-and-trade funding for research and projects that reduce greenhouse gas emissions.**

REGION

- LA County Sheriff Alex Villanueva warns that the [county's vaccine mandate](#) will cause a "mass exodus" of police & poses a threat to public safety.
- How Riverside [lured](#) ISCA Technologies to uproot global agriculture.
- Why Los Angeles is suddenly [tripping](#) out.
- Lack of affordable housing plagues region, [drives homelessness crisis](#).
- El Super market chain fined [\\$1.1M](#) over alleged COVID sick leave violations
- San Marino man sentenced with [11 felonies](#) for disrupting demonstration.
- UCR tests protocols for [microplastics testing](#) in water.
- Hill International secures [\\$125M contract](#) with SoCal Edison.
- USGS [confirms](#) earthquake felt widely across SoCal.
- Atmospheric river-amped bomb cyclone [breaks records](#) across SoCal.
- Firm hired by RivCo simultaneously ran pro/anti vaccination [campaigns](#).
- Armed officers still patrol [SoCal schools](#), despite outcry.
- Changes affect area codes 562, 626, 949 and [951](#).
- Santa Ana becomes first Orange County city with [rent control](#).
- How [surfing](#) became the key to OC's political future.
- Rattlesnakes are part of life in SoCal – Here are six [myths](#) about them.

Hantavirus in brief

How the virus spreads to humans

- 1 Virus found in rodent feces
 - 2 Infected feces becomes airborne
 - 3 Inhaled by humans
- 

Symptoms

- | | |
|----------------|------------------------|
| Early | Later, 1-2 days |
| • Chills | • Dry cough |
| • Fever | • Headache |
| • Muscle aches | • Nausea, vomiting |
| | • Shortness of breath |

Characteristics

- Most prevalent in rural areas
- Campers and hikers more likely to catch the virus, because tents rest on the ground
- Cannot be spread between humans

First human case of [hantavirus](#) in RivCo. Infection generally occurs accidentally by inhalation of virus-containing aerosols from rodent excretions such as urine, feces and saliva. It is not transmitted from human to human.

[RivCo EOC](#) is currently activated to Level 3 (virtual) in support of the ongoing COVID-19 response.

COMMUNICATIONS

- **01 November:**
 - **UCR Employee COVID-19 Testing Communication (UCOP Vaccine Policy Mandate - Testing Compliance)**
- **29 October:**
 - **Chancellor's Update – October 2021**
- **28 October:**
 - **UCPD Crime Alert: Attempted Robbery Occurred on Campus**
 - **UCOP COVID-19 Digest**
 - **UCR 2021-2022 Winter Holiday Closure**
- **27 October:**
 - **New School of Medicine building begins construction**

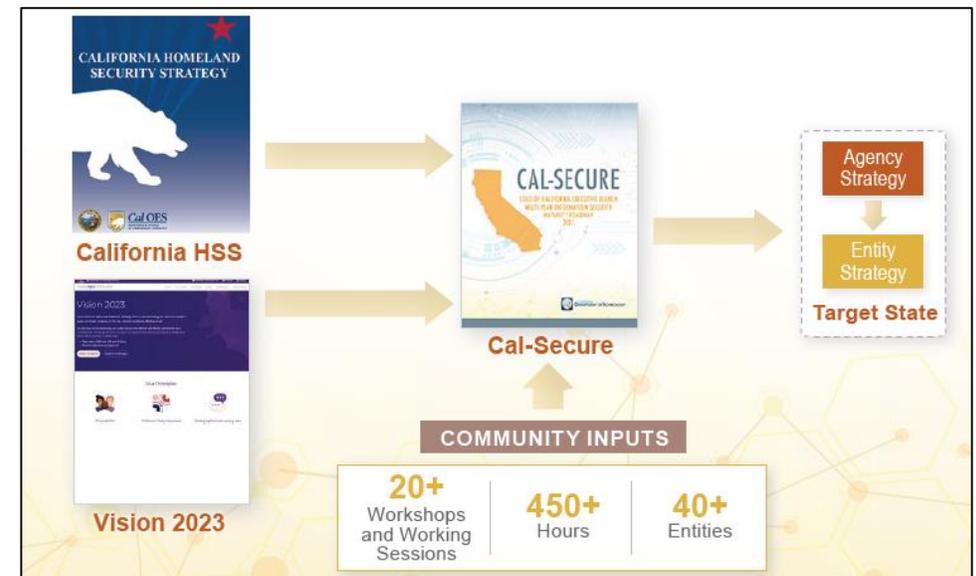
Please Reference Notes Section For More Information

NOTABLE

- [Bill to provide additional financial support for public servants affected by directed energy attacks](#)
- [Is internet addiction a growing problem?](#)
- [Meet Ray Epps: The Fed-protected provocateur who may have led the attack on the U.S. Capitol](#)
- [The STOP THE BLEED® Podcast](#)
- [Afghanistan facing desperate food crisis, UN warns](#)
- [Syria executes 24 people charged with lighting wildfires](#)
- [Walmart has quietly begun hosting Bitcoin ATMs](#)
- [What is the metaverse? Meaning explained](#)
- [DOJ: Kansas Man Pleads Guilty to Water Facility Tampering](#)
- [Securing your digital life: The basics](#)
- [Higher Ed, We've Got a Morale Problem — And a Free T-Shirt Won't Fix It](#)
- [Thousands of workers are opting to get fired, rather than take the vaccine](#)
- [This is How They Tell Me the World Ends: The Cyberweapons Arms Race](#)
- [Is the Pandemic Rewiring Kids' Brains?](#)
- [Webcast: TikTok – The Latest School Safety Challenge](#)

5 Year InfoSec Maturity Roadmap 2021

- Cal-Secure is 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) & critical partners:
 - Governor's Office of Emergency Services (Cal OES)
 - Highway Patrol (CHP)
 - Department of Technology (CDT)
 - Military Department (CMD)
 - State government security community
- The California Homeland Security Strategy (HSS) has established the goal of Strengthen Security & Preparedness across Cyberspace.
- Cal-Secure is broken into three roadmap categories – people, process, and technology.
- Cal-Secure identifies nine key priorities (three per roadmap category) and 15 forward-leaning initiatives.



5 Year InfoSec Maturity Roadmap 2021

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

5 Year InfoSec Maturity Roadmap 2021

- 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 and support strengthening cybersecurity and preparedness across the state.



5 Year InfoSec Maturity Roadmap 2021



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.

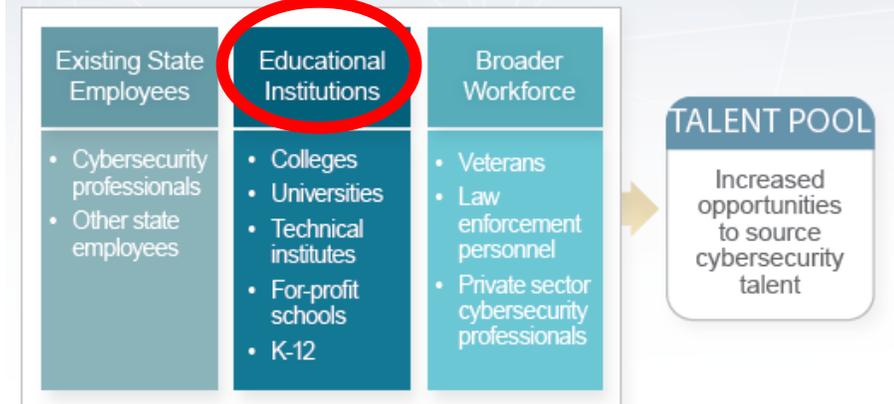
ROADMAP PRIORITIES

- 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

SOURCES OF TALENT



5 Year InfoSec Maturity Roadmap 2021



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

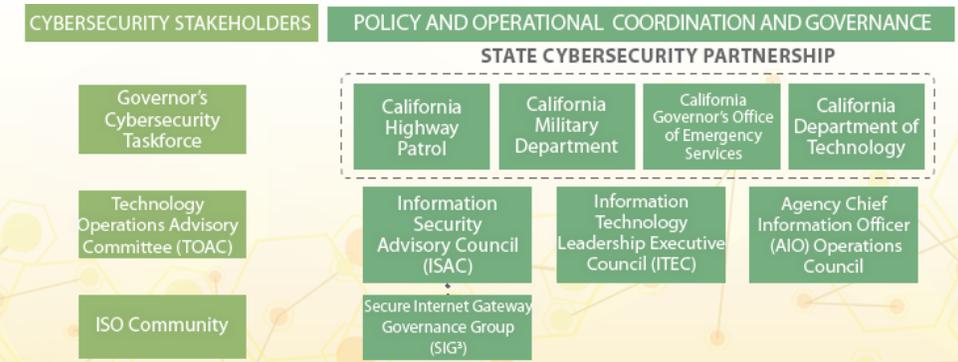
Provide effective information, privacy, and cybersecurity oversight of the Executive Branch

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



5 Year InfoSec Maturity Roadmap 2021



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

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

WHAT THE STATE PROVIDES

CALIFORNIA GOVERNMENT ENTERPRISE NETWORK (CGEN)*	STATEWIDE DATA CENTER MANAGED SERVICES	CALIFORNIA CYBERSECURITY INTEGRATION CENTER (CAL-CSIC)
<ul style="list-style-type: none"> • CGEN Edge Detection • CGEN Edge Protection • Distributed Denial-of-Service (DDoS) Protection • Initial Incident Response Management • Network Forensics • Access control services • Software Defined Network 	<ul style="list-style-type: none"> • 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) 	<ul style="list-style-type: none"> • 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.

5 Year InfoSec Maturity Roadmap 2021

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



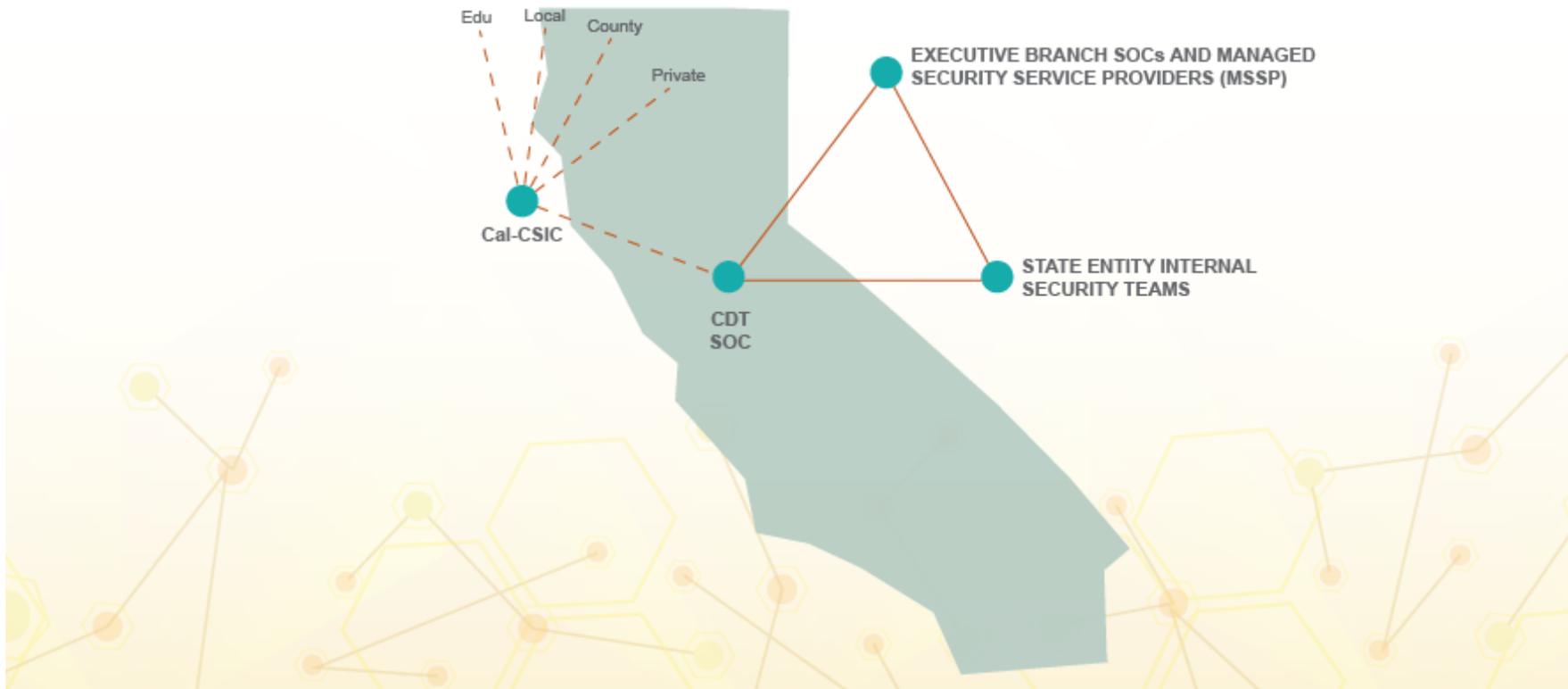
We will invest in technology and services to enhance the cybersecurity capabilities of the Executive Branch.

- ▶ 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

5 Year InfoSec Maturity Roadmap 2021

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.



5 Year InfoSec Maturity Roadmap 2021

