GAVIN NEWSOM
GOVERNOR

NANCY WARD
DIRECTOR

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

August 7, 2025

The Honorable Jesse Gabriel
Chair, Assembly Committee on Budget
1021 O Street, Suite 8230
Sacramento, CA 95814

The Honorable Scott Wiener
Chair, Senate Committee on Budget
1020 NO Street, Room 8620
Sacramento, CA 95814

Gabriel Patek, Legislative Analyst
Legislative Analyst's Office
925 L Street, Suite 100
Sacramento, CA 95814

**Subject: Report to the California Legislature on the California Cybersecurity Integration Cetner Expenditures and Activities Required by Senate Bill 104, Provision 5**

Dear Assemblymember Gabriel, Senator Wiener, and Mr. Patek:

Please find the closed "Report to the California Legislature on the California Cybersecurity Integration Center Expenditures and Activities" pursuant to Budget Act of 2023, 0690-001-0001, Provision 5 (Senate Bill 104, Chapter 189, Statutes of 2023). This report is to be submitted to the chairpersons of both budget committees of both houses of the Legislature and the Legislative Analyst's Office.

If you have any questions, please contact the Office of Legislative and Governmental Affairs, Deputy Director Yvonne Dorantes at (916)364-4525 or Yvonne.Dorantes@CalOES.ca.gov.

Sincerely,

Nancy Ward

NANCY WARD
Director

Enclosure:
Report to the California Legislature on the California Cybersecurity Integration Center Expenditures and Activities Required by Senate Bill 104, Provision 5

EMERGENCY MANAGEMENT EMAP Accredited ACCREDITATION PROGRAM

3650 SCHRIEVER AVENUE, MATHER, CA 95655
(916) 845-8506 TELEPHONE (916) 845-8511 FAX
www.CalOES.ca.gov

# REPORT TO CALIFORNIA LEGISLATURE REGARDING THE BUDGET ACT OF 2023

# CALIFORNIA CYBERSECURITY INTEGRATION CENTER EXPENDITURES AND ACTIVITIES REQUIRED BY SENATE BILL 104, PROVISION 5

**February 1, 2025**

**TABLE OF CONTENTS**

## 1. EXECUTIVE SUMMARY

The California Cybersecurity Integration Center (Cal-CSIC) is a collaborative effort within the California Governor's Office of Emergency Services (Cal OES), that is inclusive of the California Department of Technology (CDT), the California Department of the Military (CMD), and the California Highway Patrol (CHP). Codified by Chapter 768, Statutes of 2018 (Assembly Bill 2813), the Cal-CSIC is intended to serve as the central organizing hub of state government's cybersecurity activities. Moreover, it is instrumental in coordinating information, sharing with key stakeholders, and ultimately reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and/or public and private sector computer networks.

Pursuant to Provision 5, Section 13 of Chapter 189 of 2023 (Senate Bill 104, Skinner, Budget Act of 2023), Cal OES in consultation with other Cal-CSIC partners, shall develop a report to the Legislature on the Cal-CSIC's use of additional resources to address specific internal capability gaps and goals. A copy of this report shall be submitted to the chairpersons of the budget committees of both houses of the Legislature, and to the Legislative Analyst's Office, by February 1, 2025. The report shall include:

- Clear progress towards remediation of capability gaps identified by Cal-CSIC in the 2023-24 Budge Change Proposal (BCP);
- Specific goals for each new Cal-CSIC activity and/or position funded in 2023-24, informed by Cal-Secure and other statewide information security activities, with quantifiable success measures for each activity and/or position, where possible;
- How required resource estimates have evolved from the analysis used in the 2023-24 BCP justification.

Information for this report spans a data date range of July 1, 2023, through June 30, 2024, unless otherwise noted.

During this period the Cal-CSIC made significant progress on all gaps. While there is work left to do and most gaps required a revised approach considering Cal-CSIC growth, progress continues with an upward trajectory.

## 2. 2023-2024 CAL-CSIC BUDGET REQUEST OVERVIEW

The Cal-CSIC proposal was a combined request from the Cal-CSIC "core four" partners, Cal OES, CDT, CMD, and CHP. The Cal-CSIC initially received three-year funding in 2020-21, which expired on June 30, 2023. The 2023-24 BCP served two critical functions; to sustain ongoing operations driven by mission requirements and to support the continued expansion, maturation, and development of capabilities aligning with Cal-CSIC mission requirements.

The Cal-CSIC is intended to foster collaboration and coordination by enhancing information sharing between state, local, and federal partners. The high-level goals of the 2023-24 Cal-CSIC proposal focused on strengthening the Cal-CSIC's capabilities to better safeguard California's cyber landscape. These objectives were multi-faceted and included expanding threat detection and response by enhancing the ability to detect, assess, and mitigate cyber threats. Additionally, the proposal sought to secure ongoing funding to support the established functions of the Cal-CSIC with 14 additional positions to support the agency's growing responsibilities. This proposal aimed to improve infrastructure protection, focusing on safeguarding critical networks in both the public and private sectors from cyber incidents and to continue the rollout of Cal-Secure in partnership with CDT. Finally, the proposal looked to bolster cybersecurity assessments and accountability through enhanced security assessments, audits, and risk evaluations across state entities.

Success for these goals is measured by key achievements. Those include:

- The hiring and effective deployment of cybersecurity experts in crucial areas, thereby expanding the Cal-CSIC's overall capacity;
- Improved incident response rates, especially in managing high-profile cyber (e.g., SolarWinds and Log4j), demonstrating the Cal-CSIC's enhanced readiness;
- The increased production and distribution of intelligence reports, coupled with stronger collaboration with partners such as the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS), showing improved information sharing and joint threat management efforts; and
- Enhanced real-time vulnerability detection and prevention of breaches in critical systems.

Further indicators of progress include advancements in specific initiatives, such as the Cybersecurity Maturity Assessment Program (CMAP) and Cyberspace Operational Protected Systems (COPS). Both initiatives aim to improve security across diverse sectors. Additionally, the development of technological solutions for threat detection, including the establishment of an OT lab, will be vital for defending critical infrastructure. Training on standard procedures, automated tools, and incident mobilization, as well as proactive risk analysis, will help prepare the Cal-CSIC to face evolving threats.

These combined goals and measures of success are designed to protect the state from emerging cyber threats, ensure resilience in the face of potential attacks, and build a robust framework for future cybersecurity efforts. By conducting thorough risk assessments, providing outreach to state agencies, and facilitating the rapid deployment of skilled analysts and law enforcement personnel, the Cal-CSIC will be well-equipped to manage and mitigate cyber incidents effectively.

## 3. PROGESS ON REMEDIATION OF THE 10 GAPS IDENITIFIED IN THE 2023/24 PROPOSAL

### *Gap 1: Build and maintain an asset model for the state, often referred to as the "California cyber terrain."*

The Cal-CSIC's goal is to create a resilient and proactive cybersecurity environment across California's critical infrastructure. The goal is to reduce vulnerabilities and enable faster, more coordinated responses to emerging threats.

The Cal-CSIC's primary mission is to reduce the likelihood and severity of cyber incidents that threaten California's economy, public and private sector computer networks, and critical infrastructure. The Cal-CSIC determined a "cyber terrain" model that monitors the cyber threat landscape in California was necessary. This will detect emerging threats and early stages of major incidents, reduce dependence on outside parties and voluntary reporting, and shift from a reactive to a proactive posture.

The "cyber terrain" model supports Cal-Secure efforts such as the technical capability "asset management" and cybersecurity initiatives such as "creating tools for cybersecurity strategy development at state agencies and entities." Prior to the budget proposal, this was an idea still in development and only partially grasped California's cyber terrain, creating vulnerabilities. Further, this limited perspective forced a reliance on voluntary reporting from external parties. Consequently, this led to a reactive posture, which generally limited the ability of the Cal-CSIC to proactively mitigate attacks. This lack of information increased difficulties for the Cal-CSIC to estimate the scope and scale of incidents. Regardless, estimates indicated a high volume of significant cyber threat activity with increasing severity. As the Cal-CSIC's threat intelligence has improved, these early estimates remain valid.

**PROGRESS FOR GAP 1**

With additional resources, the Cal-CSIC is focused on expanding the "California cyber terrain" initiative by deepening engagement with critical infrastructure sectors and addressing the challenges of data sharing and collaboration. The Cal-CSIC scoped the problem set, revealing the scale and complexity of developing a comprehensive cyber asset model.

Progress toward building and maintaining a comprehensive asset model, or the "California cyber terrain," has advanced significantly using tools such as the Cal-CSIC attack surface management (ASM) software solution, and partnerships with entities like the Cal OES Critical Infrastructure Protection (CIP) unit within the State Threat Assessment Center (STAC). The Cal-CSIC is actively working to identify and monitor vulnerable assets across key sectors, such as energy, water, healthcare, and education, using data from ASM tools. Ongoing efforts to streamline asset tracking and improve monitoring accuracy is the current focus. By securing consent from organizations to maintain and update information about their assets within Cal-CSIC's systems, this initiative will help refine asset lists, ensure up-to-date monitoring, and provide clear insights into managing vulnerabilities.

Collaborations with CIP allow the Cal-CSIC to link to existing infrastructure assessments, gain insights into critical facilities and strengthen ties with other sectors such as water and energy. While challenges remain, particularly in establishing comprehensive information-sharing agreements and updating older data, these efforts have laid a solid foundation. By prioritizing sectors, improving tagging, and monitoring systems, the Cal-CSIC is building a clearer picture of California's cyber terrain. In turn, this enables more accurate threat analysis and enhances its ability to provide proactive alerts and support.

### UPDATED GOALS AND MEASURES OF SUCCESS FOR GAP 1

Each of the 16 federally designated critical infrastructure sectors in California have unique networks and technology. Consequently, many organizations face legal, regulatory, and technical hurdles in sharing cybersecurity information. In response, the Cal-CSIC aims to build stronger partnerships, foster trust, and explore incentives for voluntary reporting, such as priority support.

Success in building and maintaining California's cyber terrain will be demonstrated by the Cal-CSIC's enhanced ability to conduct sector-focused analysis across California's critical infrastructure. This will include close engagement with sector partners, facilitating information-sharing, and enabling real-time monitoring of emerging threats. Through the development and implementation of a tailored risk-informed approach, the Cal-CSIC aims to meet its primary mission. Additionally, the Cal-CSIC aims to empower sector-specific analysts with the information necessary to identify risks, prioritize assets, and drive rapid response efforts. In turn, this will enable a resilient cybersecurity posture for California's critical infrastructure. The Cal-CSIC will need to focus effort on prioritizing the top four highest-risk sectors and growing partnerships with subject matter experts within those sectors.

***Gap 2: Establish semi-automated processes to enhance efficiency.***

As the Cal-CSIC continues to grow and mature, the demand for automation is shifting from an internal need to an external need. Without adequate automation, this growing demand will be unmanageable. Consequently, the continued absence of automated solutions forces an inefficient use of valuable resources.

Given the Cal-CSIC's focus on rapid response and the high-risk nature of its operations, automation can significantly enhance incident response by streamlining routine security tasks, such as initial threat detection, analysis, and response workflows. Automated threat feed ingestion can enable deeper analysis leading to threat picture and insights previously unavailable to the Cal-CSIC. Many commercial solutions charge exorbitant fees for services that the Cal-CSIC could provide to partners directly.

**PROGRESS FOR GAP 2**

The Cal-CSIC has made consistent progress in developing semi-automated processes to enhance operational efficiency and strengthen cybersecurity collaboration across California. Key initiatives include integrating platforms to streamline various functions such as incident tracking, threat intelligence feeds, managing schedules and supporting grant related processes. Automation of these processes will facilitate smoother coordination between departments and partners and ultimately improve cybersecurity efforts statewide. This automation will allow cybersecurity professionals to focus more on core cybersecurity challenges and less on routine or administrative tasks. The Cal-CSIC is implementing a Cyber Incident Fusion Tracker Office 365 Power App that integrates California cyber incident data from various sources and records, including both proactive and reactive services. Insights derived from this data improve the Cal-CSIC's understanding of state entities, cybersecurity programs, and inform strategic planning. Moreover, the Cal-CSIC is actively sharing these insights and data with California fusion centers to enhance collaboration and facilitate a coordinated response to cyber incidents.

Another significant advancement is the collaborative platform that supports the California Cybersecurity Task Force (CCTF). This system has improved data collection and validation for programs like the State and Local Cybersecurity Grant Program (SLCGP). Broadly, this system allows the Cal-CSIC to better assess the cybersecurity maturity of various types of organizations statewide. Future enhancements aim to introduce more comprehensive features, including self-registration and streamlined communication, simplifying the management of an expanding network of stakeholders.

Simultaneously, the Cal-CSIC is enhancing automated processes for threat and vulnerability management. Recently acquired commercial tools provide initial alerts and streamline reporting, including automated exchange of threat

intelligence, which facilitates the sharing of crucial information across state agencies, local governments, and critical infrastructure operators. This two-way information flow ensures entities throughout California can bolster their defenses against cyber threats.

Efforts to automate routine processes are also underway. For instance, the Cal-CSIC is developing a case management platform which includes communication management, workflow and task automation, reminders, templates, metrics and reporting capabilities. The Cal-CSIC is also implementing a Security Orchestration Automation and Response (SOAR) platform to expand workflow automation capabilities via integrations with existing systems, intel feeds, and others to reduce dependence on manual processes.

Furthermore, the Cal-CSIC is integrating these automated reporting systems to streamline the analysis and presentation of data. Platforms supporting asset monitoring have been integrated to enhance asset visibility, with ongoing efforts to refine tracking and management processes. Such platforms include an industry-standard active attack surface management solution that enables rapid discovery, analysis, and response to unknown risks in state and local government internet-connected systems and exposed services. This continuous development reflects the Cal-CSIC's commitment to building a robust automation framework adaptable to the evolving cybersecurity landscape.

Overall, the focus on semi-automated processes is leading to improved efficiency and scalability across the Cal-CSIC's operations. By establishing a solid foundation and integrating versatile tools, the Cal-CSIC is set to enhance coordination, minimize manual tasks, and strengthen cybersecurity collaboration with partners across California. This strategic direction ensures the organization can respond swiftly to provide consistent and reliable support to all the entities it serves.

### UPDATED GOALS AND MEASURES OF SUCCESS FOR GAP 2

Establishing semi-automated processes at the Cal-CSIC means enhancing operational efficiency, streamlining tasks, and bolstering security across the organization. More specifically, primary automation goals should focus on improving operational efficiency by removing bottlenecks identified in process improvement programs and ensuring rapid incident response. Following principles of standard information technology (IT) management frameworks, it is critical to have well-established processes before implementing automation. While the Cal-CSIC is in the process of solidifying foundational workflows, the direction is clear and optimistic. By carefully defining these processes now, the Cal-CSIC is preparing to produce effective and seamless automation in the future. Once implemented, this strategic approach ensures that automation will drive consistent and reliable improvements across all areas. These efforts will ensure Cal-CSIC can move forward with a unified and scalable strategy.

Security orchestration, automation, and response (SOAR) tools have the potential to greatly enhance efficiency by reducing manual tasks and accelerating response times. The Cal-CSIC's planned transition to Infrastructure as Code (IaC) will enable quicker recovery in case of incidents and ensure scalability, adding resilience to its systems. While these initiatives are still in the preparatory phase, this groundwork is critical for successful integration.

### *Gap 3: Maintain a state-level cybersecurity scorecard that provides a comprehensive overview of cyber risks across California.*

The original intent of the cybersecurity scorecard initiative was to harvest, analyze, score, report, and maintain cyber risk data for the state. This would allow the Cal-CSIC to baseline the state's actual cyber risk using technical instrumentation to make the most accurate determinations of risk and provide "ground truth" ratings. At the time, other agencies were collecting incomplete metrics. By seeing and reporting what attackers see of your network, organizations can take a proactive lead to close those high-risk gaps increasing the barrier for entry to attackers. While ambitious, the cyber risk scorecard was meant to show California's overall attack surface and risks involved. The Cal-CSIC would work with higher-risk candidates to issue warnings and guidance and help close their gaps. The original scope included state and local government agencies along with critical infrastructure to some degree.

This goal was also intended to support the Cal-Secure cybersecurity initiative, "Implement Statewide Unified Integrated Risk Management Platform," for automation of information security programs and oversight.

Prior to the proposal, assessment capabilities and partnerships with stakeholders were not fully mature. This hindered the ability to establish a thorough statewide baseline of cyber risk.

#### **PROGRESS FOR GAP 3**

Significant strides have been made toward developing a state-level cybersecurity scorecard, despite the project's complexity. Early efforts to use independent security assessment (ISA) data and combine it with the ASM scores have not yet been fully realized, as the necessary strategic planning is still in progress. However, the development of frameworks such as the California Cybersecurity Maturity Metrics (CCMM, previously referred to as Cybersecurity Capability Maturity Model or C2M2) based on the National Institute of Standards and Technology (NIST) standards have laid the foundation for comprehensive cyber risk assessment.

While ISA data is not fully integrated yet, ISAs do measure whether Cal-Secure technical capabilities are adequately implemented throughout the assessed organization. In turn, this provides a more accurate reflection of the department's cybersecurity maturity than self-assessments. Entities that actively

engage with the ISA team benefit from knowledge transfer and validation of their overall cybersecurity posture.

Additionally, self-assessments can help fill gaps. Many state and local agencies participate in the Nationwide Cybersecurity Review (NCSR), which overlaps with the technical capabilities outlined in Cal-Secure. The NCSR is an annual, voluntary self-assessment for U.S. government agencies to evaluate cybersecurity practices. Developed by the Department of Homeland Security (DHS) and the Center for Internet Security (CIS), the NCSR assists state, local, tribal, and territorial entities in assessing cyber readiness by identifying strengths and gaps in their defenses. Both CDT and OES can monitor NCSR completion, while CDT has some visibility into state agency NCSR responses.

Collaborative efforts, including surveys linked to grant applications and Cal-Secure reporting requirements, have yielded valuable insights, with hundreds of valid responses providing a clearer picture of California's cybersecurity posture. As the Cal-CSIC moves forward, integrating these processes and maturity data will create a proactive, data-driven platform that enhances risk assessment and resource allocation across the state.

### UPDATED GOALS AND MEASURES OF SUCCESS FOR GAP 3

The Cal-CSIC's updated goal is to fully implement and maintain a state-level cybersecurity scorecard that offers a comprehensive overview of cyber risks across California's critical sectors. Building on existing frameworks and survey data, the aim is to identify representative organizations across industries, engage them for continuous monitoring, and develop a standardized scoring mechanism that reflects their cybersecurity posture. This will involve significant coordination between the Cal-CSIC, CDT, and CMD and effective application of prioritization frameworks.

In coordination with its partners, the Cal-CSIC will need to establish a risk assessment framework for prioritizing entity enrollment, develop entity onboarding procedures, and define key metrics for executive reporting.

Success will be measured by the creation of a scorecard reflective of California's overall attack surface and risks with it. Additionally, empowerment of organizations to take ownership of their own cybersecurity posture will require a user-friendly platform where organizations can view their scores, enabling clear and actionable insights. By standardizing data collection through existing initiatives, such as ISAs and the ASM tools, and developing automated aggregation tools, the Cal-CSIC can transition from a reactive to a proactive approach in assessing statewide cyber risk. The ultimate goal is to enhance collaboration and transparency across sectors. This will ensure data-driven, priority-based resource allocation to address vulnerabilities more effectively.

***Gap 4: Scale incident response capacity to meet typical demand, surge scenarios, and projected threats.***

The Cal-CSIC mission includes a Cyber Incident Response Team serving as California's primary unit to lead cyber threat detection, reporting, and response in coordination with public and private entities across the state. This team is tasked with assisting law enforcement and other agencies responsible for advancing information security within state government.

This goal also supports the Cal-Secure technical capability of "incident response" and the cybersecurity initiative to "create multi-tiered governance bodies" to coordinate response efforts. Within Cal-Secure, CDT provides initial incident response management for entities on the California Government Enterprise Network (CGEN). Conversely, the Cal-CSIC provides "complex incident response" for CGEN and a range of incident response options for government and non-government entities statewide. Together, these response resources are critical as incidents continue to grow and impact the cybersecurity landscape.

**PROGRESS FOR GAP 4**

To support the increased number of incidents, the Cal-CSIC is scaling its incident response capacity to effectively handle typical demand, surge scenarios, and projected cyber threats, reinforcing California's cybersecurity resilience. Acknowledging the evolving landscape of cyber threats, the Cal-CSIC has ramped up staffing in digital forensics and incident response (DFIR) roles, with several new personnel. This growth includes the addition of an Information Technology Specialist II (ITS II) and two interagency agreement (IAA) positions to support the forensic lab, enhancing the Cal-CSIC's capacity to deliver timely and detailed insights during incidents.

Emphasizing the value of proactive cybersecurity, the Cal-CSIC is committed to providing tools and services for success. Proactive services now engage directly with organizations to harden their networks by guiding them through frameworks, offering walk-throughs on implementation, and practical demonstrations of locating useful resources. This approach reinforces good cyber hygiene, which is capable of preventing most attacks. Notably, Cal-CSIC's proactive services tracker captures this engagement's impact, while the incident tracker provides insights into response effectiveness.

In coordination with federal and state entities, the Cal-CSIC has continued to advance its multi-tiered governance framework, forging strong partnerships with the FBI, Cybersecurity and Infrastructure Security Agency (CISA), and other agencies. These partnerships facilitate collaborative initiatives including a recent project on streamlining and migrating ISA results into a digital platform, harnessing advanced capabilities to aggregate data for trend analysis, identifying vulnerabilities, and enhancing the effectiveness of incident analysis.

Recent investments have also enabled a hardware refresh including new highly specialized laptops, a digital evidence storage server, software licenses, and other essential supplies which improved the incident response team's readiness to respond to emerging threats.

The incident response team's effectiveness is further enhanced by new tools for OT incident response. The addition of personnel and resources has improved incident response times, strengthened forensic reporting on threat actor tactics and procedures, and boosted Cal- CSIC's participation in significant cyber defense campaigns addressing ransomware and state-sponsored attacks. Through these initiatives, the Cal-CSIC is securing its role as a leader in statewide and federal cybersecurity, delivering on its mission to protect California's cyber critical infrastructure.

**UPDATED GOALS AND MEASURES OF SUCCESS FOR GAP 4**

These updated goals focus on efficiency, enhancing proactive services, and improving coordination across various tiers of governance. Recognizing the increasing workload and the critical need for swift and effective responses, the Cal-CSIC aims to refine its team with dedicated personnel for digital forensics and DFIR roles. This will allow for better handling of typical demand and surge scenarios.

Continued streamlining of the mission resource tasking (MRT) process will provide additional capacity to surge resources in an incident. MRTs require resources drawn from outside Cal-CSIC, typically from the California Military Department (CMD) to include additional personnel not already assigned to Cal-CSIC. MRTs can be used when a cyber incident exceeds Cal-CSIC's capacity to respond.

Success will be measured by training new personnel and retention. Retaining and training personnel will increase the capacity to handle more frequent and more complex incidents. Additionally, strengthening proactive engagement through ad hoc consultations and system hardening will help entities mitigate risks before escalation. Key achievements will include participation in major cyber campaigns, response to emergence of significant vulnerabilities, and new capabilities for operational technology (OT) incident response, highlighting a more comprehensive and resilient incident management structure.

### *Gap 5: Scale intelligence analysis capacity to meet typical demand, surge scenarios and projected threats.*

The Cal-CSIC's mission includes,

- Providing warnings of cyberattacks to government agencies and nongovernmental partners;
- Coordinating information sharing among these entities;

- Assessing risks to critical infrastructure and information technology networks;
- Prioritizing cyber threats and support public and private sector partners in protecting their vulnerable infrastructure and information technology networks;
- Enabling cross-sector coordination and sharing of recommended best practices and security measures; and
- Supporting cybersecurity assessments, audits, and accountability programs that are required by state law to protect the information technology networks of California's agencies and departments.

All of these activities require a robust intelligence analysis and information sharing function within the Cal-CSIC that is dynamic and flexible in response to evolving threats.

This goal supports the Cal-Secure technical capability of "threat intelligence platform" and the cybersecurity initiatives to "expand tailored workshops for the Executive Branch's cybersecurity workforce" to enhance analytical skills and the understanding of cybersecurity risks to the state.

Demand for intelligence production for the Cal-CSIC Cyber Threat Intelligence Branch (CTIB) grew to 30 events/products during the reporting period and CTIB produced 111 advisories. The Cal-CSIC predicts this number will only trend upward.

**PROGRESS FOR GAP 5**

The Cal-CSIC has made significant progress in scaling its intelligence analysis capacity to meet current and projected demands. Over the past year, the team produced 111 cyber advisories, participated in strategic briefings, and responded to a range of requests for information (RFIs) across sectors. This comprehensive support, which included vulnerability monitoring, threat assessments, and participation in exercises, has allowed the Cal-CSIC to provide timely and accurate intelligence to various stakeholders, including state agencies, local governments, and private sector partners. Despite the growing workload, the team successfully met all requests, often working beyond standard hours to ensure comprehensive support.

The strategic intelligence team has actively engaged in regular briefings, including bi-weekly updates for state leaders and situational awareness sessions for key stakeholders. This initiative fosters collaboration across teams and enhances real-time threat assessment capabilities. While the demand for strategic assessments has increased, the team has managed to maintain a consistent output, highlighting its adaptability and commitment. The inclusion of new technologies and methodologies, like monitoring trends in artificial intelligence (AI), shows foresight in preparing for future challenges.

The vulnerability team has also been at the forefront, delivering essential services such as daily CVE monitoring, external vulnerability scans, and regular tabletop exercises (TTXs). Their efforts have included ad-hoc network traffic analysis and quarterly vulnerability assessments, with a substantial output of vulnerability notifications and advisory products. This consistent activity demonstrates their ability to maintain operational readiness and provide proactive insights into potential cyber threats across California's critical sectors.

In addition to existing capabilities, the Cal-CSIC has been involved in major cybersecurity exercises such as Cyber Dawn. This exercise gathered diverse stakeholders for hands-on cyber threat intelligence support and cyber incident response training. This participation not only enhances readiness but also solidifies the Cal-CSIC's role as a central hub for statewide cybersecurity coordination. As demand for these services grows, particularly with new goals for monitoring critical infrastructure and educational sectors, the Cal-CSIC is preparing to scale its efforts further, ensuring comprehensive coverage.

The Cal-CSIC continues to evaluate and adjust its resource allocation to meet the increasing need for intelligence analysis. Plans include expanded trend analysis, ongoing cyber advisories, and enhanced external vulnerability monitoring. The team is also exploring new training opportunities for analysts to handle more specialized tasks, such as detailed risk assessments.

By refining existing processes, leveraging new technologies, and fostering collaboration, the Cal-CSIC is poised to enhance its intelligence analysis capabilities, ensuring robust support for California's cybersecurity landscape. The groundwork laid today is setting up a more responsive and agile team ready to meet the challenges of tomorrow.

### UPDATED GOALS AND MEASURES OF SUCCESS FOR GAP 5

The Cal-CSIC's success will be measured by its ability to increase the production of cyber advisories beyond the 111 issued last year, while maintaining timely responses to information requests, ensuring consistent and comprehensive support across stakeholders. Existing requirements for analysis related to GenAI threats alone will demand an estimated 200 percent increase in production output. Additionally, success includes expanding participation in strategic briefings using criteria still under development, at least one cybersecurity exercise (such as Cyber Dawn), and improved interagency coordination with real-time threat assessment. Finally, the Cal-CSIC will prioritize adaptability and innovation by implementing new technologies or methodologies to enhance intelligence analysis with a focus on monitoring trends in AI applications and usage and detailed risk assessments which ensure readiness for emerging threats.

### *Gap 6: Achieve full multi-sector coverage to ensure robust cybersecurity across all critical infrastructure sectors.*

In coordination with the STAC, part of the Cal-CSIC's core mission includes assessing cybersecurity risks to critical infrastructure. This goal also supports the Cal-Secure cybersecurity initiative to "formalize the cybersecurity governance structure" and the technical capability of "operational technology security."

There are sixteen critical infrastructure sectors covering a vast depth of elements including sub-sectors, segments, sub-segments, and individual assets. Mapping and prioritizing these sectors require a sophisticated approach. Achieving multi-sector coverage to ensure robust cybersecurity initiatives across all 16 sectors will take time and prioritization.

#### PROGRESS FOR GAP 6

Progress has been made in several key areas, reflecting the Cal-CSIC's commitment to enhancing cybersecurity across sectors. The Cal-CSIC has successfully developed a plan for a risk-informed approach to two sectors prioritized by the Legislature. This approach is informed by standards like the NIST Cybersecurity Framework, while encouraging broader adoption through outreach programs, particularly in local government and education. Strong partnerships have been built with federal agencies, private companies, and critical infrastructure operators, although further strategic alignment is ongoing.

The Cal-CSIC hosts and participates in sector-specific workshops and working groups including a monthly meeting with public energy utilities facilitated by the California Public Utilities Commission. Partnership with one energy utility was instrumental in starting the Cal-CSIC OT lab. Developing relationships with sectors such as water and wastewater and food and agriculture remains a priority.

The Cal-CSIC has advanced its capabilities by investing in platforms such as a threat intelligence platform (TIP) and ASM tools, allowing for integrated multi-sector monitoring. The incident response team has been strengthened with the addition of OT specialists, enabling a coordinated response to incidents across sectors, while participation in exercises like Cyber Dawn, Cyber Storm, and Cyber Shield ensures preparedness.

#### UPDATED GOALS AND MEASURES OF SUCCESS FOR GAP 6

The Cal-CSIC aims to strengthen cybersecurity across critical infrastructure sectors by developing tailored frameworks that address unique risks and compliance requirements. Building on existing standards like NIST Cybersecurity Framework (CSF) and Center for Internet Security's Critical Security Controls (CIS Controls), seeks to promote widespread adoption of best practices, particularly within local government. The Cal-CSIC will continue to foster robust public-private partnerships, enhance threat intelligence capabilities, and expand sector- specific response teams to ensure coordinated efforts in managing and mitigating cyber threats.

Success will be measured by the development and adoption of sector-specific cybersecurity frameworks, improved engagement with public and private partners, the deployment of integrated Threat Intelligence Platforms (TIP), and ASM tools. The Cal-CSIC will need to maintain a full statewide multi-sector threat and cybersecurity maturity status. Enhanced incident response capabilities, including the ability to handle multiple critical infrastructure sector incidents simultaneously, will be a key indicator, as will the frequency and effectiveness of participation in cross-sector exercises such as Cyber Dawn and Cyber Storm. Additionally, the Cal-CSIC will need to be able to respond to incidents involving sector-specific OT and leverage the resources necessary to address the unique challenges in those environments as well as it does in IT environments. This will include bridging the gap between IT and OT where they are not well-integrated in an organization. Ongoing training, proactive outreach, and the promotion of resilience frameworks will further ensure that the Cal-CSIC can effectively protect and recover from cyber threats across all sectors.

***Gap 7: Fully leverage the Cybersecurity Task Force to enhance statewide cybersecurity efforts.***

In its mission to develop a statewide cybersecurity strategy, the Cal-CSIC is expected to solicit recommendations from the California Task Force on Cybersecurity (otherwise known as the California Cybersecurity Task Force or CCTF). To address the growing cyber threat to networks, personal privacy, and critical infrastructure, Governor Brown directed Cal OES, in coordination with the CDT to establish the CCTF in 2013. The CCTF is a statewide partnership comprised of key stakeholders, subject matter experts, and cybersecurity professionals from California's public sector, private industry, academia, and law enforcement. The task force serves as an advisory body to the State of California's senior administration officials in cybersecurity matters. The task force hopes to advance the state's cybersecurity by fostering a culture of education, information sharing, workforce development, and economic growth. Furthermore, the CCTF hopes to position California as a national leader and preferred location for cyber business, education, and research.

After its establishment, the Cal-CSIC assumed responsibility for management and administration of the CCTF. The CCTF was designed to have several subcommittees aligned to priority focus areas, such as critical infrastructure, information sharing, and workforce development. Each subcommittee would be a group of cybersecurity professionals with a commitment to assisting the state with cybersecurity planning.

Following the publication of Cal-Secure, the goal of maintaining and growing the CCTF was also intended to support the Cal-Secure cybersecurity initiatives. Specially, those of "create multi-tiered governance bodies" and "develop pipelines for cybersecurity professionals."

## PROGRESS FOR GAP 7

The CCTF has made significant strides in enhancing statewide cybersecurity efforts. The Cal-CSIC increased staff focused on CCTF management, allowing for greater progress in reinvigorating the CCTF.

Key accomplishments include the formation of the Cybersecurity Investment Planning Committee, which developed the required Cybersecurity Plan for the State and Local Cybersecurity Grant Program. In turn, this laid the groundwork to distribute over $22 million in subawards. Additionally, the Critical Infrastructure Subcommittee was revitalized, focusing on risk analysis for generative artificial intelligence (GenAI) and sector-specific outreach. Similar efforts have involved tapping private sector expertise for assessments and insights on developments in artificial intelligence (AI), specifically GenAI and its potential as a cyber threat enabler or use in cybersecurity tools. CCTF membership has grown from 450 to over 1,400 members, reflecting enhanced engagement and collaboration.

To improve efficiency, the Cal-CSIC invested in an enterprise platform to streamline member management and communication. This is set to launch soon.

## UPDATED GOALS AND MEASURES OF SUCCESS FOR GAP 7

The updated goals for the CCTF focus on expanding engagement, enhancing collaboration, and building a stronger governance structure across statewide cybersecurity initiatives. Increased staffing for the Cyber Policy and Strategy Planning Team (CPSPT) within the Cal-CSIC will improve the administration and management of CCTF activities. Additional goals include revitalizing other existing subcommittees and ramping up new working groups to address evolving risks and foster sector- specific expertise. Existing investments in technology platforms will further streamline communication and member.

The establishment and active participation of subcommittees, particularly in emerging areas like AI and critical infrastructure, will demonstrate effective governance and strategic focus. Key achievements will include the development of proposals and whitepapers informed by CCTF members and development of the statewide Cybersecurity Strategy, the successful organization of regular meetings, and training events including exercises supporting a pipeline for cybersecurity professionals. The launch of an enterprise platform for task force communication by mid-2025 will enhance operational efficiency which will allow the generation of activity metrics such as membership counts, event attendance, and surveys completed. The surveys themselves will produce a rich data source that can complement threat intelligence and other information describing the state's cyber terrain and cybersecurity posture.

***Gap 8: Ensure the full application of operational technology (OT) and forensics labs to meet cybersecurity needs.***

In partnership with public utilities, the Cal-CSIC began developing an Industrial Control Systems Analytics Program (ISAP). This program was designed to protect the OT environments of California's critical infrastructure.

The Cal-CSIC's incident response is required to assist law enforcement agencies with primary jurisdiction for cyber-related criminal investigations and agencies responsible for advancing information security within state government. Effective support in such investigations necessitates deep precision analysis of compromised devices, robust chain of custody of devices, data considered evidence, and isolation from other networks to avoid malware. The Cal-CSIC built a forensics lab that provided this environment but needed additional resources to become fully operational and able to handle the anticipated workload of the Operations Branch.

Moreover, this goal also supports the Cal-Secure technical capabilities of "operational technology security" and "application security."

While support for the OT lab and initial Cal-CSIC investment was significant, it is clear the resources necessary to handle OT and forensics will be outpaced by projected demand. That gap risks an inability to effectively analyze cybersecurity threats to critical infrastructure OT and adequately perform forensic analysis of compromised systems.

**PROGRESS FOR GAP 8**

The OT and forensics labs have made significant strides in establishing a foundation to support Cal-Secure's technical objectives for "operational technology security" and "application security." The OT lab is partially operational, with key integrations across Supervisory Control and Data Acquisition (SCADA) systems, networking, and security tools, including substation and control center networks. Despite some challenges, such as the need to virtualize servers due to outdated hardware, the current setup provides a solid start in developing the Cal-CSIC's capabilities to secure critical infrastructure OT. The forensics lab became fully operational during the reporting period and has directly supported ongoing federal law enforcement investigations through collecting evidence of indicators of compromise (IOCs). The forensics lab and incident response teams follow chain of custody requirements consistent with federal investigations. Prompt identification of IOCs is a critical first step in any cybersecurity incident analysis. Both are vital elements of cybercrime investigations and cyber threat intelligence. Aggregating this intelligence and supporting law enforcement investigations leads to broad community benefits.

**UPDATED GOALS AND MEASURES OF SUCCESS FOR GAP 8**

The updated goals for Cal-Secure's OT and forensics labs aim to strengthen their ability to manage cybersecurity threats and respond quickly. One key goal is to ensure that all necessary security tools and systems are set up according to a sustainable baseline and consistently working well across the labs, enabling effective monitoring and response when needed.

Another goal focuses on developing a threat-detection system that helps identify risks specific to critical infrastructure, such as energy or water systems.

The measures of success in reaching these goals are clear and practical. Success will be shown by the labs' ability to provide real-time monitoring of essential systems and quickly record important events, proving that the setup is ready to handle threats as they arise. Additional testing through security exercises with state and utility partners will confirm that the system can effectively spot and respond to potential issues. This progress highlights a strong commitment to building a responsive and resilient cyber incident response capability.

### *Gap 9: Develop an operational technology lab that fully represents all sectors.*

As mentioned above, the OT lab supports the Cal-CSIC's incident response mission by providing a realistic training and testing environment for critical infrastructure commonly used in California. As noted in the state Homeland Security Strategy, "California has a high number of virtually connected industrial control systems, which operate and regulate critical infrastructure including oil facilities, electricity, and internet backbone lines. The connectivity of critical infrastructure systems, and the potential for exploitation puts California's security, economy, and public safety at risk." There are16 critical infrastructure sectors, all of which have cybersecurity components. While the Cal-CSIC, in coordination with the STAC CIP team and federal partners, is constantly striving to prioritize these sectors; covering even a small portion of them represents substantial workload.

This goal also supports the Cal-Secure Technical Capability "operational technology security" and the cybersecurity initiative "define cybersecurity technology requirements through community-led groups."

Prior to this proposal, the OT lab was still in its initial implementation phase, which means it did not yet provide comprehensive coverage across all sectors. This limitation would hinder the lab's ability to address sector-specific cybersecurity challenges effectively. While some OT is common across sectors, some is very specific to certain sectors (or sub-sector, segment, etc.).

## PROGRESS FOR GAP 9

The foundational setup of the OT lab is now complete, with a focus on supporting cybersecurity needs in the energy sector. The lab has established a scalable environment that addresses initial goals, setting up core infrastructure and virtual environments to work around hardware limitations. This adaptable structure allows the lab to expand as needed, preparing it to meet evolving demands in energy and beyond.

A secure access model is also in place, enabling lab users to connect safely and with strict authorization protocols. This ensures that all interactions with the lab's systems are protected, giving the team confidence as they prepare to expand into additional critical infrastructure sectors, like water and communications.

Ideally, the lab would represent all or a prioritized subset of the 16 critical infrastructure sectors beyond just energy. Additionally, for each sector represented, including energy, there would be a larger inventory of representative equipment. The current lab is limited to a certain set of older equipment donated by a single energy utility. However, the current lab setup has established a solid framework to build on, bringing the Cal-CSIC closer to the vision of a lab that fully represents all of California's critical infrastructure sectors.

## UPDATED GOALS AND MEASURES OF SUCCESS FOR GAP 9

The updated goals for the OT lab include establishing sector-specific coverage, starting with energy, and progressively expanding to cover critical infrastructure areas such as water/wastewater and communications. By emulating the unique environments and operational dynamics of each sector, the lab aims to enhance its ability to address cybersecurity challenges across multiple sectors effectively. A core measure of success in achieving this goal will be the lab's capacity to simulate sector-specific operations and cyber threats, thereby strengthening preparedness across California's critical infrastructure sectors.

In addition to sector-specific coverage, the lab's updated goals focus on the advanced integration of OT security tools and technologies. This includes achieving full compatibility with monitoring tools, security information and event management (SIEM) systems, and endpoint detection and response (EDR) capabilities that can support real-time data integration and cross-sector analysis. Success will be measured by the lab's ability to simulate different types of OT environments flexibly and to accommodate real-time data flows, enabling realistic training.

### *Gap 10: Establish a robust Cal-CSIC hosted cybersecurity exercise program that facilitates joint operations and strengthens statewide and national cyber resilience.*

Exercises are inherent to the Cal-CSIC's role as the central organizing hub of state government's cybersecurity activities and its mission to reduce the likelihood and severity of cyber incidents. Objectives of the state Homeland Security Strategy include the Cal-CSIC developing training and exercise programs to include the State Emergency Plan Cybersecurity Annex (Emergency Support Function 18).

This goal also supports the Cal-Secure cybersecurity initiative to "promote innovative programs for cybersecurity skill and leadership development" and the technical capability of "security and privacy awareness training."

Demand for participation in these exercises continues to grow along with requests for the Cal-CSIC to host them. The Cal-CSIC must plan and prioritize these events to ensure that these exercises continue and evolve as the cyber threat landscape continues to evolve.

#### PROGRESS FOR GAP 10

Progress toward developing a robust Cal-CSIC-hosted cybersecurity exercise program has gained momentum after a slow start in FY 2023-24. During this time, no exercises were conducted but six months of planning and vendor coordination occurred. The first exercise was held in August 2024. Facilitated by a top-tier cybersecurity vendor, the program now provides monthly in-person, three-day courses for up to 20 participants. These sessions, supported by industry leader cyber threat intelligence vendors and Cal-CSIC cyber coordinators, focus on real-world scenarios involving threat hunting and incident response. However, the training is conducted on a CTIB vendor's range using only vendor-provided tools. Ultimately, this limits flexibility as participants cannot use other industry standard tools, such as Security Information and Event Management (SIEM) systems that are commonly deployed on networks. This approach, though labeled as a "cyber range," requires additional scoping and development to fully meet Cal- CSIC's needs.

Despite these limitations, the Cal-CSIC has made significant strides in participating in larger-scale exercises. For example, in April 2024, the Cal-CSIC took part in Cyber Storm, a global exercise that involved over 30 participants from multiple organizations, simulating a multi-state and international cyber incident. Additionally, in June 2024, Cyber Dawn brought together over 200 participants, focusing on a mass-catastrophic cyberattack scenario in California, with a strong emphasis on collaboration between military and civilian components. These efforts highlight ongoing progress and a commitment to enhancing statewide cybersecurity readiness.

**UPDATED GOALS AND MEASURES OF SUCCESS FOR GAP 10**

An improved cyber range would have the ability to train IT Professionals and executive staff. The platform would need to scale from a small TTX to full scope exercise. It would include a learning management feature for pre- or post-exercise.

The Cal-CSIC's measures of success for establishing a robust cybersecurity exercise program include consistently hosting monthly, in-person, three-day training sessions for up to 20 participants, with a focus on real-world threat hunting and incident response scenarios. Success will also be measured by expanding the program's flexibility to incorporate a variety of tools beyond those currently provided by cyber threat intelligence vendors, aligning the program more closely with Cal-Secure requirements. Additionally, the Cal-CSIC aims to strengthen its role in larger-scale exercises, as demonstrated by its participation in events like Cyber Storm and Cyber Dawn. This engaged over 230 participants, respectively, and emphasized collaboration between state, national, and international stakeholders.

## 4. GOALS FOR NEW ACTIVITIES AND POSITIONS

Since the development of the 2023-24 BCP, the Cal-CSIC has been focused on implementation and execution of the cybersecurity mission. While there have been challenges, the Cal-CSIC has been working across programs and agencies to increase capabilities. Some of the lessons learned are discussed here:

- The cybersecurity program needs have outpaced the existing state classifications in IT. The state is exploring options to address this challenge statewide.
- There is increased need for cyber threat intelligence analysis, need to tailor that intelligence to highest risk consumers in most critical sectors of California, and effort to integrate the operations and intelligence branches even more than before.
- As awareness of cybersecurity threats in the state increases, more entities are reaching out for assistance.
- To best use its resources to scale effectively, the Cal-CSIC is improving its processes, leveraging technology, and working more closely with partners, to address the highest priority risks most effectively.

California state agencies face challenges in hiring qualified cybersecurity professionals due to a combination of factors. The cybersecurity industry has evolved rapidly, and we are exploring how to update the state classification system to address this. This is a national challenge, not unique to California. For example, a March 2023 joint publication by the National Governor’s Association

(NGA) and National Association of Chief Information Officers (NASCIO) highlighted the specific challenge faced by state governments. As of 2022, the state and local job opening rate was the highest in 20 years. In a survey, 54 percent of respondents said their wage compensation was not competitive. Most of the state and territory CISOs described excessive hiring timelines resulting in losing top candidates. This NGA-NASCIO specifically recommended increased alignment with the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) Framework.

Due to the initial vacant position and state operations reductions assumed in the 2024-25 Budget Act, the Cal-CSIC paused its hiring efforts in the summer of 2024 to allow for budget decisions. Ultimately, all of the Cal-CSIC positions were preserved, and recruitments and hiring have resumed.

Of the 26 positions included in the 2023-24 BCP, only two are still under recruitment and the Cal-CSIC is prioritizing filling these positions. The 26 positions contribute the cybersecurity mission in the following areas:

- Operations Management
- Intelligence Analysis
- Incident Response
- Defense Analysis
- Forensic Analysis
- Information Security Development
- Policy and Strategy Analysis and Planning
- Project Management
- Partner Integration

## 5. THE EVOLUTION OF RESOURCES ESTIMATES

The resources included in the 2023-24 Budget Act, help to build the foundation for the Cal-CSIC cybersecurity program. Since that time, the Cal-CSIC has been developing more automated data gathering solutions to assist in developing strategies to prioritize workload. The data and metrics should prove useful in determining future resource needs. Cal-CSIC also recognizes that the state's cybersecurity network is stronger through partnerships and the elimination of work silos. To that end, the Cal-CSIC invests in its partnerships with key state agencies such as the CDT, CMD, and CHP. Continued coordination with local agencies is also important to strengthen the state's cybersecurity posture.

## 6. CONCLUSION

The Cal-CSIC has made major progress in addressing the gaps identified in that budget proposal. This progress has included increased awareness of California's cyber terrain, partial automation of key processes, work with our partners to

establish cybersecurity maturity baselines, more robust incident response and intelligence analysis capabilities, a law-enforcement-standard forensics lab, a nascent operational technology lab, and a growing exercise program. While much work remains and progress should be considered in the context of an ever-increasing threat environment, the Cal-CSIC remains committed to strengthening cybersecurity in California.