DO YOU WANT TRAINING?

The Cal-CSIC Training and Exercise team provides training guidance and resources based on member needs. We can offer different training options, to include in-person and virtual, many at no cost. We also provide resources, planning and coordination for table-top exercises to test your incident response plans.

Contact the Cal-CSIC to request training or exercise information, or with any cybersecurity training questions!

WANT CYBER THREAT INTELLIGENCE?

SIGN UP FOR OUR SERVICES!

WANT HELP WITH YOUR CYBERSCURITY RISK MANAGEMENT STRATEGY?

CONTACT US:

1-833-REPORT-1 or **916-636-2997**

calcsic@calOES.ca.gov

https://www.caloes.ca.gov/cyber

OUTREACH

CALIFORNIA CYBER SECURITY INTEGRATION CENTER

10390 Peter A. McCuen Blvd
Building D
Mather, CA 95655

OUR MISSION

The California Cybersecurity Integration Center (Cal-CSIC) is a department of the California Office of Emergency Services, which is funded by the State, and our primary mission is to reduce the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public and private sector computer networks in our state.

HOW DO WE PRIORITIZE EFFORTS?

Cal-CSIC prioritizes our engagements based on incident severity and impact to California's economy, health, and safety. Requests of the same severity level are fulfilled in a first come, first serve basis. Engagements with lower severity levels may be put on hold when resources are needed for a higher severity incident at the Commanders' discretion.

WANT CYBERSECURITY INCIDENT RESPONSE?

Cal-CSIC offers incident assistance to public and private entities with key services like:

INCIDENT RESPONSE

Coordinate activities to respond to malicious cyber activities in your network

NETWORK PERIMETER ANALYSIS

Scan and assess your internet-facing devices for vulnerabilities and improvement opportunities

DIGITAL FORENSICS

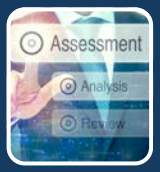
Gather and examine digital artifacts from memory, disk, network, malware, and email to help guide threat containment and eradication

HOST PROTECTION

Provide tools for (computer) endpoint detection and remediation (up to 30 days)

WANT PROACTIVE CYBERSECURITY SERVICES?

Cal-CSIC also offers proactive advisories and consultations such as:



CYBERSECURITY ASSESSMENT

Assess your internet-facing environment, and share ways to harden configurations and improve cybersecurity posture

THREAT BRIEFING

Produce virtual presentations on cyber threat topics and trends

THREAT INFORMATION EXCHANGE

Collect and share common threat actors' Tactics, Techniques, and Procedures (TTPs) as well as Indicators of Compromises (IOCs)

WHO CAN WE HELP?

Cal-CSIC is authorized to assist the following types of entities:

- California state government entities under executive, legislative, or judicial branch, including but not limited to any state agencies, boards, commissions, departments, offices, courts, as well as constitutional and independent entities
- Local government entities within California, including but not limited to counties and cities
- Public and private schools within California, including K-12, colleges, and universities
- Private sector entities, non-governmental organizations, and tribal or territorial entities who own Critical Infrastructure and Key Resources (CIKR)

WANT TO JOIN THE CALIFORNIA CYBERSECURITY TASK FORCE?

The California Cybersecurity Task Force (CCTF) is a statewide advisory body co-led by Cal OES and Cal-CSIC that unites government, academia, and industry to strengthen California's cybersecurity posture. It develops policy recommendations, fosters cross-sector collaboration, and supports initiatives to protect the state's critical infrastructure and information assets.

CONTACT US:

1-833-REPORT-1
916-636-2997
calcsic@caloes.ca.gov
https://www.caloes.ca.gov/cyber

TLP: CLEAR

CAL-CSIC SERVICES MENU
CYBERSECURITY SUPPORT FOR CALIFORNIA PARTNERS
FIFA World Cup 2026

WHO ARE WE?

Our mission is to reduce the likelihood and severity of cyber incidents affecting California's economy and critical infrastructure. Through integrated threat intelligence, premier advisory services, dynamic incident response, and industry training, we enable coordinated action and improve California's ability to anticipate, withstand, and recover from cyber threats.

MS-ISAC STATE-WIDE MEMBERSHIP

No-cost cybersecurity services and threat intelligence to state, local, tribal and territorial governments. Benefits provided with membership include threat intelligence and distribution, incident response and forensic services, 24x7x365 access to the Security Operations Center and membership collaboration.

MS-ISAC® Membership

Fusion Center Liaison (LNO)

Where intelligence meets action

LNO PROGRAM: Embeds cyber professionals s in CA fusion centers; integrates Cal-CSIC services & CTI into all-hazards operations

BIDIRECTIONAL REPORTING: Rapid CTI/incident sharing: fusion centers ↔ state leadership ↔ pub/priv partners

CYBER SITUATIONAL AWARENESS: Fusion centers as force multipliers for statewide cyber risk reduction

FEDERAL/NATIONAL SYNC: Aligning with NFCA, CISA, FBI, InfraGard, STAS/STAC

FOCUS AREAS: Processes, authorities, data flows for timely/trusted threat & incident exchange

OPERATIONAL FRAMEWORKS: In development; enable consistent cyber services & actionable intel through fusion enterprise

CYBER OPERATIONS CENTER (CYOC)

Your central hub for cyber incident coordination

1. Central communication node for CYOC operations, synchronizing internal coordination and external stakeholder engagement.
2. Conduct and sustain outreach to affected entities, integrate Cal-CSIC services, and ensure timely, accurate information flow across all parties.
3. Maintain continuous situational awareness and act as the enduring point of contact throughout the incident lifecycle, ensuring unity of effort and operational transparency.

CONTACT INFORMATION: calcsic@caloes.ca.gov (916) 636-2997

CAL-CSIC SERVICES MENU

CYBERSECURITY SUPPORT FOR CALIFORNIA PARTNERS

FIFA World Cup 2026

Cal OES
GOVERNOR'S OFFICE OF EMERGENCY SERVICES

Subscription Intelligence Services

Continuous support to maintain your security posture

AUTOMATED INDICATOR EXCHANGE

Defensive network detections and real-time state-wide intelligence sharing.

Requirements: Reports regarding malicious behavior observed in your environment, including IOCs, MITRE attack techniques, and malware samples.

Deliverables: **No-cost** access to the Threat Intelligence Platform (TIP) and automated IOC integrations into defensive systems (e.g., Sentinel, Splunk).

CYBER THREAT INTELLIGENCE REPORTING

Proactive awareness of adversary behaviors and emerging cyber risks.

Requirements: Recipient name, organization title, and official email.

Deliverables: Weekly Cyber Threat Intelligence Reports and urgent Cyber Advisories (CVEs, Zero Day Exploits).

ATTACK SURFACE MONITORING

Continuous visibility into externally exposed assets to identify misconfigurations.

Requirements: External IP ranges and identification of asset types (on-premises or cloud).

Deliverables: Direct alerts and notifications of vulnerabilities affecting your environment.

Customized Intelligence Services

Tailored assessments based on specific organizational needs

DIGITAL THREAT MONITORING

Early insight into threat actor intent across digital channels and the dark web.

Requirements: Keywords (brands, executives), password policies, and authentication URLs.

Deliverables: **Time-sensitive** alerts, domain takedown notifications, and identification of compromised credentials).

EXTERNAL VULNERABILITY SCANNING

Identify exploitable weaknesses in internet-facing systems through automated assessments.

Requirements: **Formal written consent** and authorized IP ranges/domains.

Deliverables: External vulnerability assessments with severity-ranked findings and remediation guidance.

NETWORK TRAFFIC INTELLIGENCE (NETFLOW ANALYSIS)

Detect anomalies, suspicious behaviors, and lateral movement within network patterns.

Requirements: **Formal written consent** and specific CIDR ranges to be scanned.

Deliverables: Malicious traffic findings, enriched indicators, and mitigation recommendations.

PHISHING ANALYSIS INTELLIGENCE

Early insight into threat actor intent across digital channels and the dark web.

Requirements: Suspicious emails sent as **.msg** or **.eml** attachments to the official phishing analysis email address.

Deliverables: Analysis findings reports and targeted mitigation recommendations.

INCIDENT INTELLIGENCE SUPPORT

Analytical support during and after active security breaches to guide containment.

Requirements: Known indicators, access to logs, incident timelines, and identification of affected business units

Deliverables: Rapid threat actor identification, enriched IOCs, and a final Post-Incident Intelligence Report.

IMPORTANT: Meeting these requirements ensures lawful collection and analytic validity. Incomplete or restricted inputs may limit visibility and reduce the overall effectiveness of the service.

CAL-CSIC SERVICES MENU

CYBERSECURITY SUPPORT FOR CALIFORNIA PARTNERS

FIFA World Cup 2026

Cyber Advisory Team (CAT)

Sharpening your defenses before the fight begins

PROGRAM AND SECURITY ASSESSMENT

A strong defense starts with knowing your weaknesses. We evaluate your security program's maturity, identify critical gaps, and provide actionable insights to strengthen your overall posture.

ADVISORY BRIEFINGS & THREAT AWARENESS

The threat landscape never stops evolving. We deliver expert briefings tailored to your environment so your leadership and teams are always informed and prepared.

REMEDIATION ROADMAPS

Findings mean nothing without a plan. We translate scan results and assessment findings into a clear, prioritized roadmap so your team knows exactly what to fix and when.

ADVOCACY SUPPORT

Cybersecurity initiatives need a champion. We work alongside you to build the case for security investments and drive alignment across leadership and stakeholders.

EXTERNAL AND INTERNAL VULNERABILITY SCANS

Attackers are always looking for a way in. We systematically scan your internal and external environments to surface hidden vulnerabilities before they can be exploited. This includes **penetration testing**, where we simulate real-world attacks to validate findings and uncover weaknesses that automated scans alone may miss.

Digital Forensics & Incident Response (DFIR)

OES DFIR report of findings meets specific requirements designed to serve legal, financial, and claims-based purposes — not just technical remediation

INCIDENT RESPONSE

RANSOMWARE: A ransomware attack can cripple operations in minutes. Our team deploys rapidly to contain the threat, recover critical systems, and get you back online with minimal disruption.

INSIDER THREATS: Not every threat comes from outside. We investigate and neutralize malicious or negligent insider activity before it escalates into a larger crisis.

DATA BREACH / EXFILTRATION: Covers the unauthorized access and removal of sensitive data including PII, PHI, financial records, intellectual property, and credentials — whether conducted by external threat actors or malicious insiders.

NETWORK INTRUSION: When attackers breach your perimeter, speed is everything. We detect, contain, and analyze unauthorized access to stop data loss in its tracks.

CLOUD/SAAS INCIDENTS: Covers account compromise and takeover of cloud platforms and SaaS environments, including AWS, Azure, and GCP account compromise, as well as Office 365 and Google Workspace compromise.

DIGITAL FORENSICS

MALWARE ANALYSIS: Understanding your enemy is the first step to defeating it. We dissect malicious software to uncover its behavior, origin, and full scope of impact.

MULTI-PLATFORM FORENSICS: Threats don't discriminate by device. We conduct thorough forensic investigations across Windows, Unix, iOS, Android, and Mac environments to leave no stone unturned.

Join US

California Cybersecurity Task Force

Task Force Subcommittees

- Election Security
- Emerging Technology
- Critical Infrastructure
- Cyber Risk Management
- Workforce Development and Education
- High Tech and Digital Forensics
- Training and Exercise
- Economic Development

Volunteer-driven collaboration strengthening California's cybersecurity

Learn more about CCTF

Learn More

Register For CCTF

Sign Up

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CALIFORNIA CYBERSECURITY TASK FORCE

What is the California Cybersecurity Task Force?

The California Cybersecurity Task Force (CCTF) is a statewide advisory body that provides strategic guidance to California senior leadership on cybersecurity issues. The Task Force brings together experts from government, industry, academia, and law enforcement to help strengthen the state's cyber resilience.

Participation in the California Cybersecurity Task Force is voluntary and provides an opportunity for cybersecurity professionals to contribute their expertise in support of California's statewide cybersecurity efforts.

California Cybersecurity Task Force Subcommittees

The Task Force operates through specialized subcommittees that focus on priority cybersecurity areas.

- **Election Security**
- **Critical Infrastructure**
- **Workforce Development and Education**
- **Training and Exercise**
- **Emerging Technology**
- **Cyber Risk Management**
- **High Tech Digital Forensics**
- **Economic Development**

Register for the CCTF

Sign Up

Learn More about CCTF

Learn More

Cal OES
GOVERNOR'S OFFICE OF EMERGENCY SERVICES

Center for Internet Security®

MS-ISAC®

For more information
www.cisecurity.org/ms-isac
info@cisecurity.org

State-Sponsored MS-ISAC Membership

Your state has already secured MS-ISAC membership on your behalf, giving your organization access to powerful cybersecurity tools and dedicated support at no cost. Activate your membership today to begin taking full advantage of the benefits and resources available to you.

Activate Your MS-ISAC Membership Today

New to the MS-ISAC? Register at https://learn.cisecurity.org/ms-isac-registration to become a member.

Previous member of the MS-ISAC? Log in to the CIS Portal and follow the prompts to join.

For assistance with joining, contact info@cisecurity.org and our team will be glad to assist.

What Is the MS-ISAC?

The Multi-State Information Sharing and Analysis Center® (MS-ISAC®) is the nation's trusted cybersecurity resource for U.S. State, Local, Tribal, and Territorial (SLTT) government organizations. Backed by the U.S.-based 24x7x365 CIS Security Operations Center, the MS-ISAC provides threat intelligence, monitoring, and expert support to help public sector entities defend against ever-evolving cyber threats.

Through statewide sponsorship, your organization receives MS-ISAC membership at no cost, giving you access to powerful cybersecurity tools and services designed specifically for SLTT needs. An MS-ISAC membership gives your organization enterprise-grade cybersecurity capabilities, ensuring every local organization can benefit from shared defense, real-time insights, and expert guidance.

Benefits Provided with MS-ISAC Membership

An MS-ISAC membership delivers a comprehensive suite of cybersecurity support tailored for organizations like yours.

Threat Intelligence and Distribution

- SLTT Specific Threat Intelligence Analysis Products and Reporting
- MS-ISAC Threat Intelligence Platform STIX/TAXII and MISP Access
- Virtual Threat Intelligence Briefings (SLTT threat brief)

Member Collaboration and Engagement

- Exclusive access to a collaborative peer community
- 1:1 service consultations with CIS cybersecurity experts
- MS-ISAC Annual Membership Meeting
- Monthly membership calls
- Best practice webinars led by experienced peers and top experts
- SLTT mentorship program

Incident Response and Forensic Services

- MS-ISAC Incident Response & Forensic Services (as resources allow)

Security Operations Center (SOC)

- 24x7x365 SOC access, based in the U.S., operated by dedicated, full-time CIS experts
- SOC alerts, advisories, weekly malicious IP/domain List
- Cyber Early Warning Service — dark web monitoring and notification
  - Targeted vulnerability notifications
  - Initial Access Broker (IAB) monitoring
  - Breached credential monitoring
  - IP and domain monitoring

Services and Programs

- Malicious Domain Blocking and Reporting (MDBR) — highly-effective web security that prevents your users from connecting to known or suspected malicious sites online
- Annual cybersecurity self-assessment — *Coming Soon!*

Optional, Cost-Effective Add-On Services

- Albert Network Monitoring and Management
- Malicious Domain Blocking and Reporting Plus (MDBR+)
- CIS Managed Detection and Response™ (CIS MDR™)
- Managed Security Services (MSS)
- Red Team Services
- Malicious Code Analysis Platform (MCAP) Access
- Virtual or In-Person Delivery of Customized Tabletop Exercise (TTX) — *Coming Soon!*
- Virtual Threat Intelligence Briefings (Customized for Member) — *Coming Soon!*

CAL-CSIC FLYER

CYBER DAWN 2026

California's First Operations-Based Cyber Exercise

SEPTEMBER 14-18, 2026

WHAT IS CYBER DAWN?

Cyber Dawn is California's first large-scale, operations-based cybersecurity exercise program designed to test and strengthen the state's ability to respond to major cyber incidents. This integrated exercise initiative serves dual purposes:

(1) evaluating Cal-CSIC's incident command and coordination capabilities under California Emergency Support Function 18 Cybersecurity Annex to the State Emergency Plan; and **(2)** providing hands-on technical training for state and local government incident responders.

WHY NOW?

Cyber Dawn will test current capabilities, expose process gaps, and inform refinements to California's state-level cyber incident response framework. Findings will directly shape future training, exercises, and operational procedures.

PROGRAM STRUCTURE

TRACK 1 | INCIDENT COMMAND EXERCISE

Testing Cal-CSIC's coordination with ESF 18 partners, victim entities, and supporting agencies through a compressed 30-day scenario affecting critical state services.

TRACK 2 | TECHNICAL RESPONSE TRAINING

Providing focused incident response training using a cyber range with isolated technical challenges.

KEY EVALUATION FOCUS

Cyber Dawn prioritizes process discovery over performance rating. Evaluators will assess:

- Incident identification, escalation, and decision-making effectiveness
- Inter-agency coordination and communication clarity
- Documentation quality and information management
- Critical decision points and use of decision matrices
- Integration between technical responders and incident command

WHAT YOU WILL WALK AWAY WITH

- Real skills. Real readiness. Real impact on California
- Practical ESF 18 updates and incident response process improvement
- Actionable feedback to State, Local, and Private Sector IT workforce participants

BOTTOM LINE

Cyber Dawn tests California's state-level cyber incident command under operational conditions. By measuring where we are today, this exercise will generate the actionable insights needed to strengthen California's cybersecurity preparedness and protect critical state services.

Contact Us

Lead Planner, Matthew Ivler
Matthew.Ivler@CalOES.ca.gov

Cyber Exercise Coordinator, Akil Dangerfield
akil.dangerfield@caloes.ca.gov

Scan the QR Code

To register your interest today!