California Cyber Security Integration Center

"A Unified Approach to Secure California's Cyber Infrastructure and Activities"

INTRODUCTION AND BACKGROUND

On 31 August 2015, the Governor of California signed an executive order creating the California Cyber Security Integration Center (Cal-CSIC).

Executive order B-34-15 was the culmination of work between the Governor's Office, the Office of Emergency Services and others to establish an organization that would be responsible for:

1. Strengthening the state's cybersecurity strategy;
2. Improving inter-agency and cross-sector information coordination; and,
3. Reducing the likelihood and severity of cyber-attacks.

To achieve these goals, the Cal-CSIC immediately established "core partnerships" with the California Department of Technology, the California Military Department, and the California Highway Patrol. Each of these organizations was already deeply involved in multiple cybersecurity efforts across the state, and contained recognized experts within their respective fields.

Additionally, the Cal-CSIC is co-located with the California State Threat Assessment Center (STAC), the State's primary fusion center. This co-location is the physical manifestation of the realization that cybersecurity now encompasses all aspects of life in California, including the longstanding threats that have faced the state.

PROPOSED SOLUTION

With its core partners, the Cal-CSIC moved rapidly to establish four critical enabling capabilities to accomplish its mission.

Cyber Threat Intelligence Analysis will help those served by the Cal-CSIC to understand the motivations, tactics, techniques, and procedures of threat actors. This understanding can drive organizational policies and further solutions to protect California's systems and networks.

The Cal-CSIC's Cyber Incident Response Coordination activities will consist of multi-disciplined cyber incident handlers, assessors, and analysts who support the cyber incident management lifecycle by providing expertise, support, oversight, and coordination for cyber incidents of statewide significance.

A statewide Cyber Incident Reporting Process will employ the Standardized Emergency Management System—Incident Command System taxonomy to achieve greater interoperability, resulting in relevant and timely cyber threat and trend information distribution.

Finally, a system for Cyber Threat Information Sharing will enable the Cal-CSIC to serve as a conduit for cybersecurity information between Federal, State, Local, and Tribal government entities, California utilities and other critical infrastructure providers, the private sector, and academic institutions.

CURRENT STATUS

Today, recognizing the universal nature of cyber threats, the Cal-CSIC is focused on developing the cyberseucrity information links that will cross level attack information across all state agencies and organizations through human and machine reporting processes.

Additionally, the Cal-CSIC stood up its cyber threat analysis function and is actively producing intelligence notes and advisories covering such topics as recent ransomware attacks and vulnerabilities associated with newly released zero day hacks.

Contact Information: calcsic@caloes.ca.gov