BACKGROUND INFORMATION

JOINT OVERSIGHT HEARING

A NEW ERA IN STATE LEVEL CYBERSECURITY

FEBRUARY 28, 2018

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION

ED CHAU, CHAIR

ASSEMBLY SELECT COMMITTEE ON CYBERSECURITY

JACQUI IRWIN, CHAIR

This hearing is a follow up to previous Joint Hearings of the Privacy and Consumer Protection Committee and the Cybersecurity Select Committee held on April 6, 2015, entitled "Cybersecurity at the State-Level" and February 24, 2016, entitled "Assessing California's Cybersecurity Strategy: Is the State Prepared to Defend Itself Against 21st Century Attacks?" . During those hearings, the Committees uncovered systemic inadequacies at the leadership level and throughout California's information technology (IT) enterprise related to cybersecurity.

In the interceding three years, many efforts have been undertaken by both the Executive Branch and the Legislature to bolster the cybersecurity posture of the state. Listed below are a few of the more fundamental actions taken which will likely be expanded upon by hearing testimony.

Executive Actions

Governor Brown signed **Executive Order B-34-15** on August 31, 2015, creating the California Cybersecurity Integration Center (Cal-CSIC) within the Governor's Office of Emergency Services (Cal OES). The primary mission of the Integration Center 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." The order also outlined that the Cal-CSIC would be responsible for coordinating with federal and state partners to provide warnings of cyber attacks, develop a statewide cybersecurity strategy, and establish a Cyber Incident Response Team to serve as California's primary unit to lead cyber threat detection, reporting, and response.

The Governor also directed Cal OES and the California Department of Technology (CDT) to jointly establish the **California Cybersecurity Task Force**, "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's subcommittees on risk mitigation, information sharing, workforce development and education, economic development, emergency preparedness, legislation and funding, and high tech and digital forensics advise Senior Administration Officials.

Governor Brown has also appointed new key leaders including: **Amy Tong**, as Director of CDT and State Chief Information Officer; **Peter Liebert**, as State Chief Information Security Officer; and **Keith Tresh**, as Commander of the Cal-CSIC.

Legislative Actions

AB 670 (Irwin) *Chapter 518 of 2015* – required the Office of Information Security, in consultation with Cal OES, to require at least 35 assessments of state agencies and departments per year based upon a prioritized risk index. These assessments will ensure that California's resources are targeted to known risks, such as large stores of personal data, health and financial information, or records of non-compliance.

AB 1841 (Irwin) *Chapter 508 of 2016* – required the inclusion of cybersecurity strategy incident response standards in the Technology Recovery Plans (TRPs) for each state agency to secure its critical infrastructure controls and critical infrastructure information. CDT's update to the TRP standards is required by July 1, 2018, with department and agency compliance with updated TRPs by July 1, 2019.

AB 2623 (Irwin and Gordon) *Chapter 389 of 2016* – required state agencies and departments to annually report to CDT a summary of its actual and projected information security costs. Originally required to be submitted beginning January 1, 2018, AB 475 (Chau) *Chapter 193 of 2017* changed submission of those security cost reports to February 1 of every year to align with the deadline for agencies' IT and telecommunications cost annual reports.

AB 1022 (Irwin) *Chapter 790 of 2017* – required state agencies and departments, and authorized specified local entities, to report an inventory of their critical infrastructure controls to CDT. By reporting inventories to CDT, oversight of projects, budgets, and security will be increased and allow for efficient use of taxpayer funds. Departments and agency must submit inventories with their updated TRPs by July 1, 2019.

Glossary of Key Terms

Four-Core: The main four state entities with jurisdiction over cybersecurity are the California Department of Technology (CDT), the Governor's Office of Emergency Services (Cal OES), the California Military Department (CMD), and the California Highway Patrol (CHP).

Independent Security Assessments (ISAs, AB 670 Assessments): A technical analysis of identified controls designed to measure cybersecurity maturity. Areas within current ISAs include host vulnerability assessments, firewall analysis, host hardening analysis, phishing susceptibility, network penetration testing, and snap-shot analysis of network traffic for signs of threat actor compromise. ISAs in almost all instances are performed by the Cyber Network Defense Team of the CMD, as specified under AB 670.

Information Security Audits: A CDT program that evaluates compliance with state security and privacy policies by validating that security systems, procedures, and practices are in place and working as intended.

Technology Recovery Plans (TRPs): Each state entity must develop a TRP in support of the state entity's Continuity Plan and their business needs to protect critical information assets and to ensure their availability following an interruption or disaster. Each state entity must keep its TRP up-to-date and provide annual documentation for those updates to the Office of Information Security within CDT.

Statewide Administrative Manual: The State Administrative Manual, also referred to as the "SAM," is a reference resource for statewide policies, procedures, requirements and information developed and issued by authoring agencies which include the Department of Finance (DOF), Department of Human Resources, Department of General Services (DGS), CDT, and the Governor's Office. In order to provide a uniform approach to statewide management policy, the contents are published under the authority of the Directors of DOF and DGS.

Statewide Information Management Manual: The Statewide Information Management Manual, also known as the "SIMM," Sections 05 through 80 and Sections 5300 et seq. contain standards, instructions, forms and templates that state agencies must use to comply with IT policy.

California Cybersecurity Integration Center (Cal-CSIC): a central organization for the analysis and sharing of cyber threat information. The Cal-CSIC houses multiple state and federal government partners to address real-time threats and vulnerabilities to California's infrastructure.

CDT Security Operations Center (SOC): The CDT SOC assists in providing protection against, detection of, and response to malicious activity targeting the California Government Enterprise Network (CGEN – which is the Statewide Wide Area Network) as well as IT systems owned and/or managed by CDT. The CDT SOC is intended to be a 24/7, 365 day/year operation that is constantly monitoring for malicious activity and is staffed utilizing a unique model. The SOC is operated by a team of both State civil service staff, as well as State active duty staff from the CMD. As is widely known, acquiring and retaining IT security specialists is difficult due to the vast shortage of individuals with these skills and this innovative model allows for tapping multiple sources for those skills.

Some definitions are adapted from published reports by Executive Branch Departments.