Date of Hearing: April 20, 2016

ASSEMBLY COMMITTEE ON GOVERNMENTAL ORGANIZATION
Adam Gray, Chair
AB 1841 (Irwin) – As Amended April 14, 2016

SUBJECT: Cybersecurity incident response plan and standards

SUMMARY: Requires the state Office of Emergency Services (CalOES) in conjunction with the Department of Technology (CDT) to develop, by July 1, 2017, a statewide emergency services response plan for cybersecurity attacks against critical infrastructure, and further requires CalOES and CDT to develop a comprehensive cybersecurity strategy by January 1, 2018, with which all state agencies must report compliance by January 1, 2019. Specifically, **this bill**:

1) Requires, on or before July 1, 2017, CalOES and CDT to transmit to the Legislature the Cyber Security Annex to the State Emergency Plan (SEP), also known as Emergency Function 18 (or EF 18) that includes, but is not limited to, all of the following:

    a) Methods for providing emergency services;

    b) Command structure for state-wide coordinated emergency services;

    c) Emergency service roles of appropriate state agencies;

    d) Identification of resources to be mobilized;

    e) Public information plans; and,

    f) Continuity of government services.

2) Requires, on or before January 1, 2018, CalOES and CDT to develop a comprehensive state cybersecurity incident standards for state agencies to prepare for cybersecurity interference with, or compromise or incapacitation of, critical infrastructure and the development of critical infrastructure information, and to transmit critical infrastructure information to CalOES.

3) Requires the standards developed by CalOES to consider all of the following factors:

    a) Costs to implement the standards;

    b) Security of critical infrastructure information;

    c) Centralized management of risk; and,

    d) National private industry best practices.

4) Requires each state agency to report to CalOES on its compliance with the CalOES cybersecurity standards, no later than January 1, 2019.

5) Requires CalOES and CDT to provide suggestions for a state agency to improve its compliance with the CalOES cybersecurity standards, if any, to specified public officials.

6) Declares that a cybersecurity compliance report, and any related communication records, are confidential and may not be disclosed pursuant to the California Public Records Act.

7) Defines the terms "critical infrastructure," "critical infrastructure information," "secretary" and "state agency."

8) Makes findings relative to the importance of cybersecurity of state networks, and declares the intent of the Legislature to develop a comprehensive cybersecurity strategy under the coordination of CalOES.

9) Makes findings and declarations relative to the need to limit the public's right to access to the documents referenced by this bill because of the need to promote public safety by prohibiting access to those who would use that information to thwart the cybersecurity of critical infrastructure systems within the state.

EXISTING LAW:

1) Establishes CalOES by the Governor's Reorganization Plan No.2, operative July 1, 2013.

2) Requires CalOES to perform a variety of duties with respect to specified emergency preparedness, mitigation, and response activities in the state, including emergency medical services.

3) Specifies that the State Emergency Plan (SEP) shall be in effect in each political subdivision of the state, and the governing body of each political subdivision shall take such action as may be necessary to carry out the provisions thereof.

4) Requires the Governor to coordinate SEP and those programs necessary to mitigate the effects of an emergency.

5) Requires the Governor to coordinate the preparation of plans and programs for the mitigation of the effects of an emergency by the political subdivisions of the State of California, such plans and programs to be integrated into and coordinated with the SEP and the plans and programs of the federal government and of other states to the fullest possible extent.

6) Establishes, within the California Department of Technology (CDT), the Office of Information Security (OIS) to ensure the confidentiality, integrity, and availability of state systems and applications, and to promote and protect privacy as part of the development and operations of state systems and applications to ensure the trust of the residents of this state.

FISCAL EFFECT: Unknown

COMMENTS:

Purpose of the bill: According to the author, "Cybersecurity threats are on the rise and California is a priority target because of the size of our economy and the value of our networks and other assets. The state bears a responsibility in actively defending the critical networks that

Californians rely on for services.

"A denial of service, theft or manipulation of data, disruption or damage to critical infrastructure through a cyber-based attack could have significant impacts on national security, the economy, and the livelihood and safety of individual citizens. In the first half of 2015 alone, the Department of Homeland Security responded to 108 cyber incidents impacting US critical infrastructure: electricity, water, health care, communications, financial, and manufacturing systems, among others…

"This issue has prompted state and federal leaders to warn operators of critical infrastructure of the need to bolster cyber defenses to protect against debilitating attacks. In 2015, Governor Brown declared in an executive order on cybersecurity that 'cyber- attacks aimed at breaching and damaging computer networks and infrastructure in California represent a major security risk and increase the state's vulnerability to economic disruption, critical infrastructure damage, privacy violations, and identity theft.

"AB 1841 will ensure sufficient preparations are taken to protect these critical infrastructure systems [, which] is a role of state government. A comprehensive cybersecurity strategy, undertaken in a coordinated effort between federal and state governments and private entities, will help prepare for cyberattacks on these critical infrastructure systems, and reduce the potential consequences from those attacks."

Background: In 2009, the California Legislature merged the powers, purposes, and responsibilities of the former OES with those of the Office of Homeland Security (OHS) into the newly- created California Emergency Management Agency (CalEMA).On July 1, 2013, Governor Edmund G. Brown Jr.'s Reorganization Plan #2 eliminated CalEMA and restored it to the Governor's Office, renaming it the California Governor's Office of Emergency Services (CalOES), and merging it with the Office of Public Safety Communications. Today, CalOES is responsible for overseeing and coordinating emergency preparedness, response, recovery and homeland security activities within the state.

State Emergency Plan (SEP): The SEP addresses the state's response to extraordinary emergency situations associated with natural disasters or human-caused emergencies. In accordance with the California Emergency Services Act, the plan describes the methods for carrying out emergency operations, the process for rendering mutual aid, the emergency services of governmental agencies, how resources are mobilized, how the public will be informed and the process to ensure continuity of government during and emergency or disaster.

The plan is a management document intended to be read and understood before an emergency occurs. It is designed to outline the activities of all California jurisdictions within a statewide emergency management system and it embraces the capabilities and resources in the broader emergency management community that includes individuals, businesses, non-governmental organizations, tribal governments, other states, federal government and international assistance.

The SEP, amongst other things, establishes the California Emergency Functions (CA-EFs), which consist of 18 primary activities deemed essential to addressing the emergency management needs of communities in all phases of emergency management.

Standardized Emergency Management System (SEMS): SEMS is the system used for coordinating state and local emergency response in California. SEMS provides a multiple level emergency response organization that facilitates the flow of emergency information and resources. SEMS consists of the Incident Command System (ICS), mutual aid, the operational area concept and multi-interagency coordination. SEMS is designed to be flexible and adaptable to the varied emergencies that can occur in California, and to meet the emergency management needs of all responders. Government Code 8607(a), requires CalOES, in coordination with other state agencies and interested local emergency management agencies, to establish SEMS by regulation.

Operational Area (OA): Encompasses the county and all political subdivisions within the county. The OA serves as a focal point for all local emergency management information and the provision of mutual aid. It manages information, resources, and priorities among local governments within the OA. The OA also serves as the coordination and communication link between the local government level and the regional level. SEMS regulations authorize each County Board of Supervisors to designate an OA lead agency.

California Emergency Functions (CA-EFs): The CA-EFs were designed to bring together discipline-specific stakeholders at all levels of government to collaborate and function within the four phases of emergency management. At the state level, the CA-EFs consist of an alliance of state agencies, departments and other stakeholders with similar functional responsibilities. This grouping will allow each CA-EF to collaboratively mitigate, prepare for, cohesively respond to and effectively recover from an emergency.

A single state agency is assigned to lead each CA-EF based on its authorities, resources and capabilities. Each CA-EF member agency is responsible to assist in coordinating the state's response to emergencies, including provision of mutual aid and the allocation of essential supplies and resources.

Local governments and OAs are not required to implement the CA-EF concept unless they choose to do so. Instead, CalOES recommends they organize consistent with local resources and established SEMS regulations and guidelines.

The last CA-EF in the SEP is the Cyber Security Annex, also known as Emergency Function 18 (or EF 18).

CalOES and the incomplete EF 18. Current law authorizes the Governor to take actions to prepare for, respond to, and prevent natural or human-caused emergencies that endanger life, property, and the state's resources. It further authorizes CalOES and its Director to take actions to coordinate emergency planning, preparedness, and response activities.

CalOES, in its role as the state's lead agency on emergency preparedness, response, and damage mitigation, has responsibility to develop, implement, and manage a comprehensive strategy to protect the critical infrastructure systems of federal and state governments, and private entities. CalOES meets that responsibility in part by preparing SEP.

The most recent SEP provided by CalOES is from 2009 and outlines a state-level strategy to support local government efforts during a large-scale emergency. As required by CESA, the plan describes methods for carrying out emergency operations; the process for rendering

mutual aid; emergency services of governmental agencies; how resources are mobilized; emergency public information; and continuity of government. As stated above, the 2009 SEP also establishes the CA-EFs, which consist of 18 disciplines deemed essential to the emergency management community in California.

According to the CalOES website, only EF 18 remains incomplete, and is noted as being "in development." CDT, under the Government Operations Agency, is listed as the responsible entity, with the point of contact being the State Chief Information Security Officer.

According to a briefing document from CDT provided by the author, CDT has completed two of five steps in the development of EF 18: identifying and engaging stakeholders, and forming a working group. The three remaining steps: clarify authorities, roles and responsibilities; develop functional annex; and develop concept of operations; are listed as "work in progress." EF 18 has been pending completion since 2011.

Double Referral: This bill was first heard in Assembly Committee on Privacy and Consumer Protection and passed on an 11-0 vote.

Related/Prior legislation: SB 949 (Jackson) of 2015/2016 Session. Would authorize the Governor to require owners and operators of critical infrastructure to submit critical infrastructure information to OES or any other designee for the purposes of gathering, analyzing, communicating, or disclosing critical infrastructure information. (Pending hearing in Senate Governmental Organizations Committee).

AB 2595 (Linder) of 2015/2016 Session. Would establish in statute the California Cybersecurity Integration Center (Cal-CSIC) within the Office of Emergency Services to develop a cybersecurity strategy for California in coordination with the Cybersecurity Task Force. (Pending hearing in Assembly Privacy and Consumer Protection Committee)

AB 1346 (Gray) of 2015/2016 Session. Would require CalOES to update the State Emergency Plan on or before January 1, 2018, and every 5 years thereafter, and would require the plan to be consistent with specified state climate adaptation strategies. (Pending hearing in Senate Governmental Organizations Committee)

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

None on file

Analysis Prepared by: Kenton Stanhope / G.O. / (916) 319-2531