Date of Hearing: April 27, 2017

ASSEMBLY COMMITTEE ON GOVERNMENTAL ORGANIZATION
Adam Gray, Chair
AB 1022 (Irwin) – As Amended April 17, 2017

SUBJECT: Information technology: Technology Recovery Plans: inventory

SUMMARY: Requires state agencies to include within their Technology Recovery Plan (TRP) an inventory of all critical infrastructure controls and associated assets. Specifically, **this bill**:

1) Requires state agencies, as part of their TRP, to provide the California Department of Technology (CDT) with an inventory of all critical infrastructure controls and associated assets in their possession.

2) Authorizes any state or local governmental entity that is not required to report their updated TRP to CDT to voluntarily submit an inventory of all critical infrastructure controls, and their associated assets, in the possession of the entity, to CDT.

3) Declares the reports required or authorized by this bill to be confidential, and shall not be disclosed pursuant to any state law, including the California Public Records Act.

4) Makes findings and declarations that this bill strikes the appropriate balance between the public's right to access information about the conduct of their governmental agencies and the need to protect the cybersecurity of critical infrastructure controls within the state.

5) Makes other technical or non-substantive amendments.

EXISTING LAW:

1) Establishes the Office of Emergency Services (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) requires the Department of Technology, in consultation with the Office of Emergency Services and in compliance with the information security program required to be established by the chief of the Office of Information Security, to update the Technology Recovery Plan element of the State Administrative Manual to ensure the inclusion of cybersecurity strategy incident response standards for each state agency to secure its critical infrastructure controls and critical infrastructure information.

4) Establishes CDT within the Government Operations Agency, under the supervision of the Director of Technology, also known as the State Chief Information Officer.

5) Requires state entities to implement the information security and privacy policies, standards and procedures issued by the Office of Information Security (OIS).

6) Requires CDT, on or before July 1, 2018, to update the TRP element of the State Administrative Manual to ensure the inclusion of cybersecurity strategy incident response standards for each state agency to secure its critical infrastructure controls and critical infrastructure information.

7) Requires state agencies to report on their compliance with the updated Technology Recovery Plan standards to CDT in the manner and at the time directed by CDT no later than July 1, 2019.

8) Defines "critical infrastructure controls" as networks and systems controlling assets so vital to the state that the incapacity or destruction of those networks, systems, or assets would have a debilitating impact on public health, safety, economic security, or any combination thereof.

FISCAL EFFECT: Unknown

COMMENTS:

Purpose of the bill: According to the author, "cybersecurity is an ever growing threat to both the private and public sectors. For state government these threats put at risk the ability for agencies and departments to provide critical services to Californians. While California's state agencies and departments continue to mature their information security programs, additional strategic capabilities within the Office of Information Security will help ensure the state is protected against cyber threats. By reporting critical infrastructure control inventories to the Department of Technology, project and budgetary oversight will be more informed and allow for efficient use of taxpayer funds."

CalOES: The California Disaster Act was enacted by the State Legislature in 1945. The Act combined responsibility for planning and preparing for emergencies, whether natural, technological and human-caused into a single state agency. The California Emergency Services Act was enacted in 1970 to supersede the California Disaster Act. The new Act established the Governor's Office Emergency Services with a Director reporting to the Governor. The office was given responsibility to coordinate statewide emergency preparedness, post emergency recovery and mitigation efforts, and the development, review, approval, and integration of emergency plans.

In 2009, the California Legislature merged the powers, purposes, and responsibilities of the former Cal 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 Cal EMA 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.

Current law requires the CDT, in consultation with CalOES to update the TRP element of the State Administrative Manual to ensure the inclusion of cybersecurity strategy incident response standards for each state agency to secure its critical infrastructure controls and critical infrastructure information.

Technology Recovery Plans: According to the Committee on Privacy and Consumer Protection, the state's TRP program is a sub-set of the state entity's Business Continuity Plan, which is premised on identifying all business functions within a state entity, and then assigning a level of importance to each business function. An agency's TRP is activated immediately after a disaster strikes and focuses on getting critical systems back online. Every state entity is required by the State Administrative Manual (section 5325.1) to develop a TRP in support of the Continuity Plan and the business need to protect critical information assets to ensure their availability following an interruption or disaster.

Every state entity must keep its TRP up-to-date and provide annual documentation for those updates to the Chief Information Security Officer. The TRP must outline a planned approach to managing risks to the state entity's mission, including risk and potential impact to critical information technology assets. The TRP is currently required to cover: state entity administrative information, critical business functions/applications, recovery strategy, backup and offsite storage procedures, technology recovery procedures, data center services, resource requirements, assignments of responsibility, contact information and testing. (State Information Management Manual (SIMM) Section 5325-A)

The SIMM 5325-A instructions do currently require description of critical business functions and their supporting applications (SIMM 5325-A(2.1)), and a comprehensive list of the equipment, space, telecommunication needs, data, software, hard-copy references (forms and procedures), and personnel necessary for recovery (SIMM 5325-A(7.1)).

AB 1022 would explicitly direct all state agencies to provide an inventory of all critical infrastructure controls and associated assets to CDT (specifically, the CISO), as part of the agency's TRP. The bill would also authorize any other state or local governmental agency to voluntarily submit a similar inventory to CDT as well.

The author contends that this inventory is necessary so that the CISO has a better strategic view of the state's critical infrastructure assets and controls, making "the inventory no longer an optional appendix, but a key component of the report that can be accessed by the CDT for planning, budgeting, and security purposes."

Prior/Related Legislation: AB 531 (Irwin) of 2017/2018 of the Legislative Session. Would require the state OIS to review information security technologies currently in place in state agencies to determine if there are sufficient policies, standards, and procedures in place to protect critical government information and prevent the compromise or unauthorized disclosure of sensitive digital content, and develop a plan for state agencies to implement any information security technology OIS determines to be necessary to protect critical government information and prevent the compromise or unauthorized disclosure of sensitive digital content of a state agency. (Pending in Assembly Privacy and Consumer Protection Committee)

AB 1306 (Obernolte) of 2017/2018 Legislative Session. Would establish in statute the California Cybersecurity Integration Center (Cal-CSIC) within the Office of Emergency Services (OES) to develop a cybersecurity strategy for California, which currently operates under the authority of Executive Order B-34-15 (August 31, 2015). (Pending in the Assembly Governmental Organization Committee).

AB 1841 (Irwin), Chapter 508, Statutes of 2016. Requires CDT, in conjunction with OES, to update by July 1, 2018, the TRP element of the State Administrative Manual to ensure the inclusion of cybersecurity strategy incident response standards for each state agency.

AB 1881 (Chang) of 2015/2016 of the Legislative Session. Would have required the Director of CDT to develop and update mandatory baseline security controls for state networks based on industry and national standards, and annually measure the state's progress towards compliance. (Held on Suspense in the Assembly Appropriations Committee).

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

None on file

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