

Executive Department
State of California

EXECUTIVE ORDER B-34-15

WHEREAS information technology networks and critical infrastructure around the world are threatened by increasingly sophisticated cyber attacks; and

WHEREAS 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; and

WHEREAS state government agencies protect the state's computer networks and investigate criminal attacks on state computer networks and critical infrastructure systems under current state law; and

WHEREAS the California Cybersecurity Task Force was formed in 2013 to increase public and private sector coordination, communication, and information sharing on cybersecurity; and

WHEREAS the National Cybersecurity and Communications Integration Center was established through the National Cybersecurity Protection Act of 2014 to oversee federal government cybersecurity and critical infrastructure protection; and

WHEREAS the increasing number and complexity of cyber attacks demands heightened levels of coordination, information sharing, and emergency response between state government and federal agencies, local governments, tribal governments, private companies, academic institutions, and other entities in order to protect computer networks and critical infrastructure systems from damage or unauthorized access; and

WHEREAS the California Emergency Services Act 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, and further authorizes the Governor's Office of Emergency Services and its Director to take actions to coordinate emergency planning, preparedness, and response activities.

NOW, THEREFORE, I, EDMUND G. BROWN JR., Governor of the State of California, in accordance with the authority vested in me by the Constitution and statutes of the State of California, do hereby issue the following orders to become effective immediately:

IT IS HEREBY ORDERED THAT:

1. The California Governor's Office of Emergency Services shall establish and lead the California Cybersecurity Integration Center. The Integration Center's primary mission will be 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 Integration Center will serve as the central organizing hub of state government's cybersecurity activities and coordinate information sharing with local, state and federal agencies, tribal governments, utilities and other service providers, academic institutions, and non-governmental organizations. The California Cybersecurity Integration Center shall be comprised of representatives from the following organizations:

- California Governor's Office of Emergency Services (Cal OES)
- California Department of Technology, Chief Information Security Office
- California State Threat Assessment Center
- California Highway Patrol
- California Military Department
- California Office of the Attorney General
- California Health and Human Services Agency
- California Utilities Emergency Association
- California State University
- University of California
- California Community Colleges
- United States Department of Homeland Security
- United States Federal Bureau of Investigation
- United States Secret Service
- United States Coast Guard
- Other members as designated by the Director of Cal OES

2. The California Cybersecurity Integration Center shall operate in close coordination with the California State Threat Assessment System and the U.S Department of Homeland Security - National Cybersecurity and Communications Integration Center, including sharing cyber threat information that is received from utilities, academic institutions, private companies and other appropriate sources. The Integration Center will provide warnings of cyber attacks to government agencies and non-governmental partners, coordinate information sharing among these entities, assess risks to critical infrastructure and information technology networks, prioritize cyber threats and support public and private sector partners in protecting their vulnerable infrastructure and information technology networks, enable cross-sector coordination and sharing of recommended best practices and security measures, and support cybersecurity assessments, audits, and accountability programs that are required by state law to protect the information technology networks of California's agencies and departments.

3. The California Cybersecurity Integration Center shall develop a statewide cybersecurity strategy, informed by recommendations from the California Task Force on Cybersecurity and in accordance with state and federal requirements, standards, and best practices. The cybersecurity strategy will be developed to

improve how cyber threats are identified, understood, and shared in order to reduce threats to California government, businesses and consumers. The strategy is also intended to strengthen cyber emergency preparedness and response, standardize implementation of data protection measures, enhance digital forensics and cyber investigative capabilities, deepen expertise among California's workforce of cybersecurity professionals, and expand cybersecurity awareness and public education.

4. The California Cybersecurity Integration Center shall establish a Cyber Incident Response Team to serve as California's primary unit to lead cyber threat detection, reporting, and response in coordination with public and private entities across the state. This team will also provide assistance to law enforcement agencies with primary jurisdiction for cyber-related criminal investigations and to agencies responsible for advancing information security within state government. This team shall be comprised of personnel from agencies, departments, and organizations represented on the California Cybersecurity Integration Center.
5. Information sharing by the Integration Center shall be conducted in a manner that protects the privacy and civil liberties of individuals, safeguards sensitive information, preserves business confidentiality, and enables public officials to detect, investigate, respond to, and prevent to cyber attacks that threaten public health and safety, economic stability and national security.


I FURTHER DIRECT that all state departments and agencies ensure compliance with existing information security and privacy policies, promote awareness of information security standards with their workforce, and assist the California Governor's Office of Emergency Services and the California Cybersecurity Integration Center in executing this order.



IN WITNESS WHEREOF I have hereunto set my hand and caused the Great Seal of the State of California to be affixed this 31st day of August 2015.


EDMUND G. BROWN JR.
Governor of California

ATTEST:


ALEX PADILLA
Secretary of State