AGENDA

Joint Oversight Hearing
Assembly Privacy and Consumer Protection Committee
Assembly Select Committee on Cybersecurity
Assembly Members Ed Chau and Jacqui Irwin, Chairs

WEDNESDAY, FEBRUARY 24, 2016 – 10:00AM
STATE CAPITOL ROOM 444

ASSESSING CALIFORNIA'S CYBERSECURITY STRATEGY: IS THE STATE PREPARED TO DEFEND ITSELF AGAINST 21ST CENTURY ATTACKS?

I. OPENING REMARKS

Assembly Member Jacqui Irwin, Chair
Assembly Member Ed Chau, Chair
Committee Members

II. STATE OFFICIALS

- **CALIFORNIA STATE AUDITOR'S OFFICE**
  ELAINE HOWLE, STATE AUDITOR

- **ATTORNEY GENERAL AND CALIFORNIA HIGHWAY PATROL**
  SPECIAL COUNSEL FOR LEGISLATION, ROBERT SUMNER;
  CHIEF SCOTT HOWLAND AND CAPTAIN RICH DESMOND

- **DEPARTMENT OF TECHNOLOGY**
  STATE CHIEF INFORMATION SECURITY OFFICER MICHELE ROBINSON

- **CALIFORNIA MILITARY DEPARTMENT**
  MAJOR GENERAL MATT BEEVERS, DEPUTY ADJUTANT GENERAL

- **GOVERNOR'S OFFICE OF EMERGENCY SERVICES**
  DIRECTOR MARK GHILARDUCCI

III. PUBLIC COMMENT

* * *

CALIFORNIA STATE CYBERSECURITY

BACKGROUND

California's Cybersecurity Challenge

In the past few years, retailers, financial institutions, and government agencies have increasingly fallen victim to cyberattacks. Most recently, in June 2015 the federal Office of Personnel Management announced that a cybersecurity intrusion had exposed the personal information of approximately 20 million current and former federal employees and other individuals.

Given the size of California's economy and the value of its information, the State presents a prime target for similar information security breaches. California's agencies and departments maintain an extensive range of confidential and sensitive data, including Social Security numbers, health records, and income tax information. If unauthorized parties were to gain access to this information, the costs both to the State and to the individuals involved could be enormous.

Moreover, California is home to a wide range of critical infrastructure – like power grids, telecommunications and transportation networks, and water systems – controlled by state and local entities as well as the private sector. And as it described in the California Bureau of State Audits "High Risk Update – Information Security" report of August 2015, the State already has a number of identified weaknesses in its assessment, mitigation and management of information security vulnerabilities and incident response plans.

Cybersecurity challenges are constantly evolving, and the methods that could be used to breach, disrupt, or damage our networks change quickly. Equally challenging is the diversity of sources that can produce these threats – from a kid in the basement to a sophisticated criminal network overseas, or even a foreign nation. From a state perspective, the range of threats is a function of what is important to us – protection of citizens' personal information held by state government, continuity of government services, and resiliency of critical infrastructure which is mostly privately-owned and operated.

As the eighth largest economy in the world, California produces the technology that drives the innovation economy and grows the food that sustains millions of Americans every day. Even without considering the significant number of military bases in the state, California is a critical asset for our nation. But underneath all this activity is the digital infrastructure that makes all this productivity possible. From the port of Los Angeles to the start-ups of Silicon Valley, from the farms of the Central Valley to the fishing fleets of the North Coast, digital systems networked to the Internet enable our economy to operate more efficiently.

However, this reliance on technology also makes us vulnerable to a variety of threats. From the danger of data breaches and identity theft, to "hacktivism" driven by domestic political considerations, criminals have many potential motivations to attack California networks. Furthermore, the targeting of industrial control systems for critical

infrastructure – for purposes not entirely clear – has been growing in sophistication and number. While we have not yet seen a loss of life in California caused directly by these threats, the activities of hostile nation states, terrorist groups, and criminal enterprises suggest that it is only a matter of time before the intent to cause harm is matched by the capability to do so.

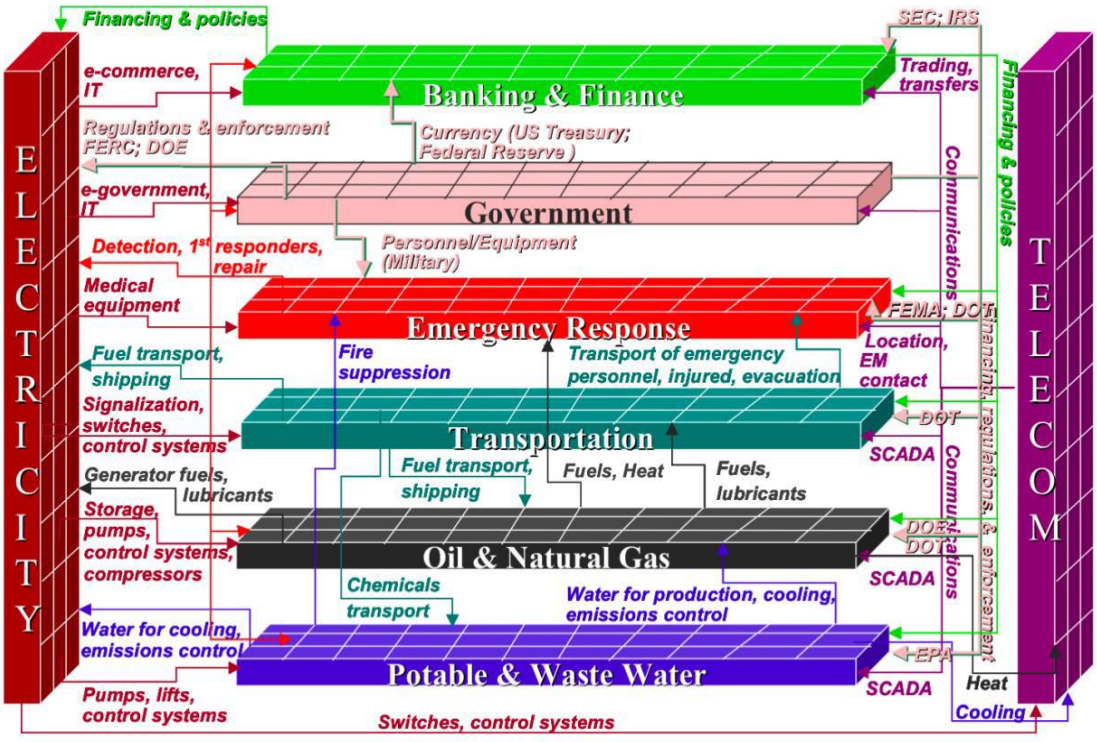
Protecting Critical Infrastructure Is Important…And Complicated.

In the context of cybersecurity, critical infrastructure is defined as 'means, systems and assets so vital to the state that the incapacity or destruction of those systems or assets would have a debilitating impact on security, economic security, public health and safety, or any combination of those matters.'

According to the Department of Homeland Security, critical infrastructure includes the following 16 sectors of the economy:

Chemical	Dams	Food & Agriculture	Military bases
Commercial Facilities	Emergency Services	Government	Nuclear facilities
Communications	Energy/ Electricity	Healthcare	Transportation
Critical Manufacturing	Financial Services	Information Tech.	Water

Adding to the challenge of protecting our critical infrastructure is the growing interdependence of these systems. That interdependence is demonstrated by the following graphic provided by the Governor's Office of Emergency Services, which demonstrates how an attack against even a single sector could have serious effects on other sectors, with the duty of coordinating a response falling on a dizzying array of government agencies:



Exacerbating this problem is the unique nature of the industrial control systems built into our critical infrastructure. Designed for reliability, often many years ago, these systems are highly trusting of their operator by design. In the physical world when you flip a switch to power up a medical device or produce drinking water, you want to be sure it operates properly. In the digital realm, we have learned to be less trustful, building in security and encryption to verify users and commands.

Moreover, because our critical infrastructure was built and maintained in collaboration between the public and private sectors, the protection of that infrastructure must be a community effort. Much of our state's critical infrastructure is owned or operated by the private sector, so without solutions that make business sense, the necessary investments in the security of these critical systems will not take place. Government also has a supporting role to play in driving public awareness around the need for better security and incentivizing best practices.

Improving Information Security by Sharing Best Practices.

Recognizing this need for collaboration, the Federal government has partnered with cybersecurity leaders in the private sector to develop a plan for holistically addressing cybersecurity risks across our digital and physical infrastructure. Aside from being an excellent collection of cybersecurity best practices, the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity creates a common lexicon for managing these risks that can be usefully applied by businesses from the pizza place around the corner to a global energy company. However, California has a lot of work to do in implementing these best practices in its own networks, as the 2015 BSA audit has demonstrated.

Another lesson to be learned from the Federal government is the importance of addressing cybersecurity from a risk management approach. That starts with identifying which assets are most critical to protect and making reasonable investments to protect them. This is a two-part process that starts with identifying where a cybersecurity incident could pose the greatest risks, then working with the owners and operators of those assets to determine the level of risk they are actually facing. This was the approach taken by the Obama Administration to produce an accurate measure of risk and prepare a targeted response.

Finally, California can prevent economic loss and harm to individuals by building in as much resiliency as possible into our networks. Standard industry best practices appear to rely on a combination of **awareness** (pre-attack self-assessment), **response/preparation** (tracking potential threats through information sharing and joint exercises), and **training** (both skills training for operators and 'security hygiene' training for general employees). The findings of the August 2015 Bureau of State Audits report showed substantial and widespread deficiencies in awareness and training, an unfortunate revelation that demonstrates the need for California to have a broad-ranging and long-term strategy to ensure its own cybersecurity.

ROLES AND RESPONSIBILITIES OF STATE ENTITIES

Governor's Office of Emergency Services

The California Governor's Office of Emergency Services' (OES) cybersecurity role goes beyond protection of state networks. OES works with operational partners, including public and private sectors, academia, and the overarching critical infrastructure sectors— to make sure they can mitigate the risk faced by the state collectively.

As the state's leader on emergency planning and homeland security, one of OES' many responsibilities is the protection of critical infrastructure. OES is engaged in risk and vulnerability assessments and works with the public and private sectors on contingency planning. The majority of critical infrastructure is owned and operated by the private sector, which makes this a particularly difficult challenge, but underscores why government's ability to share information in real time and engage with the private sector is critical. OES is also working with Federal, State and local agencies and other organizations toward a full and comprehensive cybersecurity strategy that includes the state's cyber emergency, governance, and integration plans.

The Governor, through Executive Order B-34-15, directed OES to establish and lead the California Cybersecurity Integration Center (Cal-CSIC), which will be responsible for improving inter-agency and cross-sector coordination to reduce the likelihood and severity of cyber-attacks. Cal-CSIC will work closely with the California State Threat Assessment Center and the U.S Department of Homeland Security to facilitate more integrated information sharing and communication with Federal, State and local agencies, tribal governments, utilities and other service providers, academic institutions and non-governmental organizations.

Specifically, Cal-CSIC is intended to:

- Cultivate a neutral and collaborative environment where resources can be leveraged and shared to support statewide incident management;
- Integrate intelligence resources from public and private sectors;
- Allow partners to share information and threat actors' Tactics, Techniques, and Procedures. Collaboration like this allows for cross-training and lessons learned; it enhances visibility of events, training opportunities, network infrastructure, and personnel;
- Enhance and encourage coordination between private industry security professionals, security alliances, and intelligence groups;
- Present California with significant opportunities for research and development in cybersecurity, communications, intelligence, and response methodologies, techniques, and technologies;
- Provide opportunities to promote professional development in State government over the long term; and
- Leverage specialized training resources from places like the Department of Justice Advanced Training Center, California Military Department and California Department of Technology to improve retention and attract new talent to State government.

OES currently operates the State Threat Assessment Center (STAC) which performs threat information sharing functions at the state level, filters information from regional centers (RTACs) and serves state agencies/leaders. The mission of STAC is to serve as California's information sharing clearinghouse for threat analysis and strategic situational awareness reporting to statewide leadership to prevent, prepare for, mitigate, and respond to cybersecurity incidents and hazards impacting California citizens and critical infrastructure. The STAC's primary mission is not cybersecurity *per se*, but rather detecting and disseminating information on cybersecurity crimes. Because of the growing volume and sophistication of cybersecurity issues, OES is developing the Cal-CISC to supplant the duties currently performed by the STAC.

California Department of Technology

The Department of Technology (Department) is responsible for 1) advising the Governor on the strategic management and direction of the state's information technology resources; 2) establishing and enforcing state information technology strategic plans, policies, standards, and enterprise architecture; and 3) providing technology direction to agency and department chief information officers to ensure the integration of statewide technology initiatives, compliance with information technology policies and standards, and the promotion of the alignment and effective management of information technology services. (Government Code Section 11545)

The Department also produces two annual reports, which it forwards to the Legislature. The first, the Department's Information Technology Strategic Plan, guides the acquisition, management, and use of information technology. The second, its annual IT Performance Metrics Report, assesses the state's progress toward acquiring and enhancing new and existing technology, reducing costs associated with the implementation of technology assets, and enhancing the security and reliability of information technology networks.

Office of Information Security

The Department's Office of Information Security (OIS) is responsible for the establishment and oversight of the statewide information security and privacy program applicable to executive branch agencies. California's statewide information security program is focused on four overarching program objectives:

1. Effective Policy and Oversight: OIS chairs Security and Privacy Governance meetings, working closely with other executive branch agencies and market players. OIS also directs state agencies through policy directives, standards and procedures, and it reviews and monitors agencies' compliance with security requirements.

2. Creating a Culture of Awareness: Through training and support programs, OIS subject matter experts' promote security and privacy awareness initiatives across the state.

3. Establishing a Robust Risk Management and Response Capability: OIS is responsible for security, education and training. A key element to establishing an effective risk management and response capability is developing and maintaining a strong and highly-skilled cybersecurity workforce. OIS sponsors an Annual

Cyber Security Awareness Symposium, and also directly provides recurring training.

Furthermore, OIS is a key partner in the Department's Project Approval Lifecycle process and Information Technology Procurement reform initiatives to integrate security risk management steps into the procurement process. It also requires state agencies to conduct ongoing risk analyses and a biennial comprehensive risk assessment, and to work with the Department of the Military's Computer Network Defense Team to promote the use of their risk assessment services. OIS also works with the Department's Office of Technology Services to provide a 24/7 Network Operations Center, and with the Department's Security Management Branch's Network Intrusion Prevention Systems to protect the state from cyber-attacks.

OIS also supports a robust response capability by tracking state breach incidents through a centralized incident reporting process, working closely with the California Highway Patrol Computer Crimes Investigations Unit to facilitate access to resources and support incident response.

OIS also works closely with the State's Threat Assessment System, comprised of six fusion centers encompassing all levels of government (the state, the Department of the Military, the Federal Bureau of Investigation, and local law enforcement) to monitor cyber threats, analyze thousands of vulnerability reports, and develop and disseminate hundreds of critical advisories with mitigation strategies each year.

4. Providing Resources that Support Success: OIS responds to numerous requests for assistance by state and local government agencies, and its subject matter experts serve on a number of nation-wide working groups that support the success of California's information security infrastructure.

Cybersecurity Task Force

The Department, through OIS, and OES co-chair the Task Force, which is charged with advising the Administration on cybersecurity matters and developing a strategy for critical infrastructure protection to ultimately improve California's overall cybersecurity posture.

The Task Force is a statewide partnership comprised of key stakeholders, subject matter experts, and cybersecurity professionals from California's public sector, private industry, academia, and law enforcement. By fostering a culture of cybersecurity through education, information sharing, workforce development and economic growth, the Task Force hopes to advance the State's cybersecurity and position California as a national leader and preferred location for cyber business, education, and research.

The Task Force is comprised on seven subcommittees: risk mitigation; information sharing; workforce development and education; economic development; emergency preparedness; legislation and funding; and high tech and digital forensics.

California Military Department

The California Military Department (CMD), as part of the California National Guard, provides unique military capabilities to the interagency team working to tackle cyber threats that face the State. The CMD's position as a member of the Department of Defense (DOD), and as a state agency under direction of the Governor, gives it unique access to national security information, training, and best practices in the cyber domain. The National Guard is the only military service that is authorized by federal law to use military resources to protect and defend state government networks and other state critical infrastructure.

The CMD approaches cybersecurity on three fronts:

1. Maintaining Awareness - CMD leverages substantial federal training and resources to know what threats, tools, and techniques are being used to help prevent and counter cybersecurity threats.

2. Computer Network Defense Team (CNDT) - The CNDT is an eight-person cyber protection team that assists state agencies in improving their network security.

3. Incident Response- In addition to the CNDT, the Military Department, under orders from OES, can use other National Guard cyber units to respond to an or attack on the state government network, or help with forensics, analysis, remediation, and appropriate reporting.

Department of Justice/ Attorney General's Office

Attorney General Kamala D. Harris established an eCrime Unit in 2011. The eCrime Unit is tasked with investigating and prosecuting large-scale identity theft and technology crimes with actual losses in excess of $50,000. The primary mission of the eCrime Unit is to investigate and prosecute multi-jurisdictional criminal organizations, networks, and groups that perpetrate identity theft crimes, use an electronic device or network to facilitate a crime, or commit a crime targeting an electronic device, network or intellectual property.

In addition, the eCrime Unit provides investigative and prosecutorial support to the five California regional high-tech task forces funded through the High Technology Theft Apprehension and Prosecution (HTTAP) Program Trust Fund. HTTAP provides investigative, legal, and prosecutorial support for technology crime investigations to those rural counties that are not represented by an HTTAP-funded task force; provides coordination for out-of-state technology-crime investigation requests; provides support for technology crime investigations that are initiated by other state agencies; provides legal support for state-operated digital forensic laboratories; and develops and delivers training for judges, prosecutors, law enforcement officers and the public on the importance of strong information-security practices and evolving technology-related crime issues.

Also, the Office of Digital Investigations (ODI) was recently created by the California Department of Justice (DOJ) in the California Justice Information Services Division (CJIS) as a response to the exponential usage of new and cutting edge technology in cyber-crime and data breaches. The ODI's primary focus within the California Cyber

Crimes Center (C4) is on evidential discovery during digital investigations on the latest computing devices and technology appliances. The ODI staff, with backgrounds in data center enterprise information systems and networks with highly specialized training in digital forensics, works with California and US law enforcement investigators and prosecutors. ODI is part of the response and restitution quadrants of the cyber security incident cycle, working with the DOJ eCrime Unit and the California Highway Patrol (CHP) to respond to, investigate and prosecute cyber-crime and criminal network and system breaches.

Currently, ODI specializes in the forensic analysis of servers and network-based environments along with reconstruction of computing environments, including web services. Forensic analysis of servers and networks involves acquisition, verification and analysis of large datasets from varying sources. Reconstruction involves taking static digital evidence and restoring it to allow investigators and prosecutors to see the environment as it existed just prior to seizure.

ODI's secondary focus is conducting research and development of cutting edge technologies and how they are used in criminal activities. With the drive to connect everything to the Internet for ease of use, remote monitoring and more, the increasingly connected digital economy provides unprecedented opportunities for criminals. ODI is currently working to be able to find potential evidence on such devices and appliances and the networks they utilize. Internet connected game consoles are an example of how the "Internet of Things" (IoT) can be used by criminals to aid in wrong doing by allowing criminals to skirt court-sanctioned communications monitoring via encrypted private channels. ODI's work involves proactively being able to recognize these types of activities in advance of their potential criminal use.

Additionally, as part of the C4, DOJ has created the Cyber Accelerator which is a collaborative effort between ODI, and the Division of Law Enforcement's Bureau of Forensic Services (BFS) and Bureau of Investigation (BI). These organizations will use their expertise in forensic analysis, investigation and information technology to find better and faster ways of solving cyber-crime. The Cyber Accelerator will explore new and advanced forensic tools, collaborate with other talents in the technology field and develop technical talent for law enforcement.

California Highway Patrol

The California Highway Patrol (CHP) has a growing role in cybersecurity, particularly as a first responder. The CHP's cybersecurity role is two-fold:

- **The State's First Responder for Cyber.** The CHP is the primary investigating agency for cybercrimes occurring on or against state property. State agencies are required by law to report cybercrimes to the CHP. To satisfy this duty, the CHP has a specialized computer crimes investigations unit. Based upon this jurisdiction, the CHP develops partnerships with other federal and local law enforcement entities. (Government Code Section 14613-14615)

- **Participant in California's Fusion Centers.** California has five regional threat assessment centers (RTAC) and the CHP has personnel in 4 out of the 5 RTACs where multiple agencies are represented, including the FBI and the Secret

Service. The CHP works closely with Federal, State, and local stakeholders in this area, particularly on information sharing – on real-time awareness of threats, on preventative/ defensive measures, and on maximization of shared resources.

There are eight field divisions within CHP, and some of their investigators have special training in cyber issues. CHP's role in the fusion centers is strengthened by their unique statewide presence, and by their capability and collaboration with their other statewide partners.

As a law enforcement entity with sensitive data regarding ongoing investigations and prosecutions, the CHP ensures its own systems are up to date, secure, and protected from intrusion. CHP emphasizes the importance of preventative, defensive measures because usually by the time they get the call, an incident has already occurred – and often times they find that the incident was easily preventable. CHP also emphasizes the importance of speed and information sharing in response, which can reduce the overall amount of data loss. Also, rapidly sharing that information with partners may help prevent a similar cybercrime at another department or agency. CHP also assists in administrative investigations regarding state employees misusing information. CHP has digital forensics abilities through federal resources of FBI and associated training, and works closely with the DOJ's e-Crimes personnel.

Responsibility for Cybersecurity is Distributed Among State Agencies.
State agencies play a variety of roles in both the pre-incident preventative processes and the post-incident planning and response process. Some of these roles are dictated by statute, while others are a product of interagency agreements and other informal arrangements. Throughout, there are uncertainties regarding how certain functions would be funded, capacity constraints in some circumstances, and jurisdictional gaps and overlaps with federal and local operators. Some functions established by the Governor's Executive Order are still in the planning stages and are not yet operational. Roles and responsibilities are regularly shifting and the Administration is working on clarifying pre- and post-incident operations and providing that information to the Legislature. This lack of operational clarity raises a concern that the state response to a major attack might not be well-coordinated, with potentially serious negative consequences.

Pre-Incident Preparation

- OES coordinates overall state agency response preparation, mitigation and consequence management, as well as collaboration with federal and local resources. OES coordinates six state fusion centers that play a key role in intelligence and info sharing, as well as cybercrime and terrorist threat assessment. As the State's Homeland Security counterpart, OES has responsibility for critical infrastructure protection and conducting exercises to strengthen reliability. When the Cal-CSIC becomes operational, OES will have increased ability to integrate cybersecurity into its existing emergency management functions.

- The Department of Technology houses the chief information security officer, protects the ca.gov domain, oversees security assessments for state networks, and facilitates California's cybersecurity response (although Emergency Function

18 has not been completed). The Department is responsible for establishing minimum IT security standards and updating security policies through the State Administrative Manual and the Statewide Information Management Manual. The Department is responsible for auditing and validating compliance with these security standards.

- The California Military Department conducts security assessments and penetration tests as directed, helps protect the ca.gov domain, and supports compliance with state security controls when directed.

- The California DOJ consults with private sector entities, particularly small businesses, on security best practices informed by their data breach reporting. The DOJ also has authority to enforce a "reasonable" standard of security pursuant to CA Civil Code Section 1798.81.5. While this authority has yet to be exercised, the Federal Trade Commission has addressed negligent security practices under a similar law. DOJ could expand its influence in pre-incident preparation by more actively enforcing security standards among private sector networks.

- CHP participates in the state threat assessment system, high tech crime task forces, and fusion centers in using data to inform preventative activities. CHP operates the 24/7 Emergency Notification and Tactical Alert Center (ENTAC), which receives notification about security incidents and notifies OIS and their own Computer Crimes Unit.

Post-Incident Response

- OES is the lead agency for overall response to a cybersecurity incident, coordination with private stakeholders, and collaboration with federal and local resources. OES is tasked with monitoring the remediation efforts of a state entity if they are the victim to an incident, including the appropriate reporting, and providing a final analysis. As proposed in the Governor's Executive Order, and in line with their duty as the lead agency in response, OES would direct the multi-agency Cyber Incident Response Team (CIRT) in support of cyber threat detection, reporting, and response in both the public and private sectors.

- The Office of Information Security within the Department of Technology is designated as the federal government liaison (Gov. Code Section 11549.2). The Department is tasked with facilitating California's cybersecurity response through Emergency Function 18. The Department is responsible for approving and distributing breach notifications for state government entities.

- The California Military Department under orders from OES, can use National Guard cyber units to respond to an attack on the state government network; helping with forensics, analysis, remediation, and appropriate reporting. In January 2017, the California National Guard will have a federally-awarded 39-member Cyber Protection Team available for this purpose.

- The California DOJ assists criminal investigations and prosecutions by performing digital forensics and operates the e-crimes unit. Pursuant to state law, DOJ is notified of any breach affecting more than 500 residents, administer other breach requirements and report on data breaches annually.

- CHP provides first response capabilities, including digital forensics, and partnerships with other law enforcement entities such as the FBI. The CHP participates in the state threat assessment system, high tech crime task forces, and fusion centers in a collective investigation and prosecution effort.

RECENT DEVELOPMENTS IN CALIFORNIA'S CYBERSECURITY

State Auditor's High Risk Report on Information Security.
The Bureau of State Audits August 2015 report on the California Department of Technology's oversight of the State's information security preparedness highlighted the following:

"The California Department of Technology is responsible for ensuring that reporting entities that are under the direct authority of the Governor (Note: this does not include Constitutional offices e.g. Controller, Dept. of Insurance, Attorney General, etc.) maintain the confidentiality, integrity, and availability of their information systems and protect the privacy of the State's information. As part of its efforts to protect the State's information assets, the technology department requires reporting entities to comply with the information security and privacy policies, standards, and procedures it prescribes in Chapter 5300 of the *State Administrative Manual* (security standards)."

"However, the audit showed that the Department had not ensured that reporting entities complied with the State's information security standards. Many reporting entities did not have sufficient information security controls in place, nor does the State have an understood definition for a sufficient level of security. Each of the audit's five reporting entities had deficiencies, and most entities indicated they were not in full compliance with the SAM's security standards. The Department was unaware that they had not complied with these standards. Further, 37 of the 41 reporting entities that self-certified that they were in compliance with the security standards in 2014, indicated via survey they had not actually achieved full compliance.

"In all, 73 of 77 reporting entities responding to the audit survey indicated that they had yet to achieve full compliance with the SAM security standards. These reporting entities noted deficiencies in their controls over information asset and risk management, information security program management, information security incident management, and technology recovery. These weaknesses could compromise the information systems the reporting entities use to perform their day-to-day operations.

"Despite the seriousness of these issues, the Department has failed to take sufficient action to ensure that reporting entities address these deficiencies. In fact, until the audit, it was not aware that many reporting entities had not complied with its requirements. The Department relies on an annual self-certification form to determine compliance.

"Because of the nature of its self-certification process, the Department was unaware of vulnerabilities in information security controls throughout state government; thus, it did nothing to help remediate those deficiencies. Although the Department recently developed a pilot information security compliance audit program to validate the implementation of security controls, at its current rate of four auditors completing eight audits every year and a half, it would take roughly 20 years to audit all reporting entities. By implementing more frequent, targeted information security assessments in addition to periodic comprehensive audits, the technology department could acquire a more timely understanding of the level of security that reporting entities have established for their high-risk areas.

"Further, when noncompliance was known or reported, the Department failed to provide effective oversight of their information security and privacy controls. Although more than 40% of entities reported a lack of full compliance, the Department had not established a process for performing follow-up activities. In addition, more than half of reporting entities indicated that the Department did not provide sufficient guidance to assist them in complying with all of the security standards. More than one-third of reporting entities indicated that they did not understand all of the requirements in the security standards.

"Finally, a significant number of entities—such as constitutional offices and those in the judicial branch—are not currently subject to the Department's security standards or oversight. As a result of the outstanding weaknesses in reporting entities' information system controls and the Department's failure to provide effective oversight and assist noncompliant entities in meeting the security standards, the audit concluded that some of the State's information, and its critical information systems, are potentially vulnerable and continue to pose an area of significant risk to the State."

Assembly Bill 670 (Irwin)

In 2015, Assemblymember Jacqui Irwin authored Assembly Bill 670, which was signed into law and is now being implemented. The bill requires the State to perform a minimum of 35 network security assessments per year on state agencies, departments, and offices. The assessments are to be performed based upon a defined risk index that prioritizes the amount of valuable personal information, financial information, or health records held by that entity.

Although it was drafted before the State Auditor's report was released, AB 670 addressed one of the audit's key recommendations by requiring more frequent and targeted information security assessments.

AB 670 was designed to bolster state cybersecurity three ways:

1. To increase the number of assessments performed on state entities in order to more quickly identify and correct network vulnerabilities and reduce the risk of a breach;
2. To provide the Governor and the Legislature with a real-time understanding of the level of vulnerability in certain areas of state government, and to better inform the allocation of resources and risk management in the budget process;

3. To better utilize cybersecurity resources available to the State such as the Department's authority to mandate security assessments and remediation, and employ the cybersecurity capabilities of the National Guard.

Governor's Executive Order on Cybersecurity
Governor Brown signed Executive Order B-34-15 on August 31, 2015 to bolster California's preparedness and response to cyber-attacks.

The order directs OES to establish the California Cybersecurity Integration Center (Cal-CSIC), which will be responsible for strengthening the state's cybersecurity strategy and improving inter-agency, cross-sector coordination to reduce the likelihood and severity of cyber-attacks. Cal-CSIC will work closely with the California State Threat Assessment System and the U.S Department of Homeland Security, and is intended to facilitate more integrated information sharing and communication with Federal, state and local agencies, tribal governments, utilities and other service providers, academic institutions and non-governmental organizations.

Under the order, Cal-CSIC will also establish a multi-agency Cyber Incident Response Team to serve as the state's primary unit to lead cyber threat detection, reporting, and response in coordination with public and private entities across the state.

The Cal-CSIC and the functions of the Executive Order will be funded through the redirection of existing Homeland Security Grant Program resources.

New Budget Requests for Cybersecurity Funding.
Released in January 2016, the Governor's 2016-17 Budget proposes increased funding for two of the departments with primary cybersecurity roles.

To address the recommendations of the State Auditor's Report, the Department of Technology submitted a budget change proposal (BCP) for $1.5 million to fund 11 full-time positions to expand their pilot audit team, suggesting that this funding would support 23 audits per year.

Also, the Military Department requested expansion of their reimbursement authority to $1.3M in performing security assessments pursuant to AB 670.

Additionally, in an effort to address identified cybersecurity weaknesses, various state departments submitted BCPs requesting funding to enhance IT security. Funding requests included plans to replace older, less secure systems or to hire staff qualified to implement security controls, such as those in the NIST Framework. In addition to the departments with primary cybersecurity responsibility, staff identified seven other approved BCPs for cybersecurity funding. These include the Department of Aging ($423K), Alcohol and Beverage Control ($117K), CalEPA ($1.1M – 4PYs), CalFIRE ($3M – 14PYs), Department of Human Resources ($154K – 1PY), Judicial Branch ($3.1M, $1.95M ongoing), and the State Controller ($1.7M, 13PYs).

Recent Executive Actions by President Obama.
President Obama has prioritized cybersecurity during his administration, issuing more executive orders on this issue (six) than any other modern president. Examples

include executive orders addressing each of the following issues: critical infrastructure protection, private sector information sharing, sanctions for international cyber-criminals, establishing a commission to guide policy and partnerships, and establishing a privacy council.

Most recently, the President declared a budget initiative to finalize his work on cybersecurity, which includes $3.1 billion for a cybersecurity modernization fund and an increase to an overall $19 billion in federal spending to improve government cybersecurity practices, staffing, and capabilities.

STAFF COMMENTS/QUESTIONS

Cybersecurity Policy Issues

There are five general policy areas that should be prioritized in order to improve the security posture of the state. Some are more long-term than others, but each involves identifiable problems with proven examples of improvement shown in either the federal government or the private sector.

1. Governance Structure/ Budgeting

California has implemented the new NIST Framework guidelines by adding them to the State Administrative Manual's policies. These guidelines provide recommended security controls and risk mitigations that focus more on procedure and management than product-based solutions. However, fully implementing these guidelines will be both technically complex and require significant manpower. Further complicating the effort is a lack of clear and measurable metrics, which could lead to wide variations in implementation across different agencies.

This is particularly concerning for a state government that has 151 separate state entities subject to the Department of Technology's policies. Also, without a sufficient means of enforcing the implementation of these security controls, the outcomes could be very poor, as shown by the State Auditor's 2015 report.

Many state agencies may also lack the budget to appropriately address their cybersecurity needs or respond to proper direction. New tools and additional manpower may be needed to identify their current compliance status and solve management control issues. However, a budget process that relies on individual BCPs to address what may be a systemic problem may represent a fragmented approach to the issue. Rather than identifying risk and targeting resources accordingly, individual entities are identifying their own priorities whether or not they are in line with existing requirements or a broader strategy guided by a comparative amount of risk.

There may be a need for more centralized leadership on this issue. Unlike the federal government, California does not have a single executive with full-time responsibility for cybersecurity. Because the issue is spread amongst various agencies, there is a lack of full accountability for both pre-incident and post-incident activities. The State should consider establishing a Director of Cybersecurity, a 'cyber-czar', that works in an interagency capacity to drive policy outcomes.

2. Risk Management

Cyberattacks on businesses can be costly; they can hamper operations, slow the supply chain, impact reputation, and compromise sensitive customer data and intellectual property. According to a 2013 Cost of Cyber Crime Study by the Ponemon Institute, the average annualized cost of cybercrime for organizations is $11.6 million per year, with a range of $1.3 million to $58 million. Accordingly, the private sector has developed ways to put a price on risk – how much is acceptable given a business's core function, and how much it may cost to reduce it through a proven process.

Identifying critical assets and associated impacts from cyber threats is essential to understanding risk exposure–whether financial, operational, reputational, or regulatory. Risk assessment results are essential for identifying and prioritizing specific protective measures, allocating resources, informing long-term investments and budget priorities, and developing policies and strategies to manage cyber risks.

The State does not have a clear mechanism for aggregating information that details the location or severity of risk that is being tolerated at a given time. The State should incorporate consideration of cyber risk into existing risk management and governance processes, and ensure that the executives responsible for managing that risk are held accountable.

3. Information Sharing

Access to high-quality cyber threat information is vital for the protection of critical infrastructure and other networks. The ability to quickly and reliably share information that identifies the source, methods, and effective countermeasures to cyber threats is essential to an effective defense and response.

The current threat information sharing system consists of various facilitators, the largest of which are governmental and quasi-governmental organizations sharing information from government to government or to private industry, as well as private nonprofits and exclusive groups administered by and for large corporations. The Cal-CSIC aspires to join this list of facilitators.

Adding value or proprietary resources in this area must start with an understanding of what is already offered in this area. To be effective, the Cal-CSIC must be a well-resourced and professional operation that identifies weaknesses in the existing information sharing community and targets the gaps that serve California's priorities. Recently enacted federal law provides legal protection for sharing information for preventative purposes. The State must actively encourage public and private sector partners to engage in information sharing. Similar to a neighborhood watch program, the outcomes of this practice will only be as good as its inputs, and government has a role in advocating for, and incentivizing contributions to community security.

Finally, the Legislature does not currently have a reliable mechanism to gain access to sensitive information about the severity or location of risks among state agencies – information necessary to measure performance and to match budget resources with the highest levels of risk. Without that information, the Legislature will be unable to engage in meaningful oversight of the process, which would be a lost opportunity both for

accountability and for genuine partnership between the branches to resource cybersecurity adequately.

4. Incident Response Coordination and Strategy

The State must develop and test cyber incident response plans. Each state entity should expect to experience a cyber incident at some point, and when that happens executives should be prepared to confidently respond, knowing which resources are available, what legal options are available, and what their channel of communication should be. Each state entity, and the state collectively, should exercise these incident response plans regularly.

The State performs similar emergency response functions for earthquakes, fires, etc. and the same should be expected for cybersecurity given the economic and public safety threat it presents. The State must integrate cyber incident response policies and procedures with existing disaster recovery and business continuity plans. Such exercises are performed by the Department of Homeland Security and the FBI with private partners, particularly in the critical infrastructure sectors. The State must identify leadership in coordinating cyber incident response planning. Early response actions can limit or even prevent possible damage.

5. Training and Workforce Development

Cybersecurity as a profession is critically important to California's economy: not only is the work itself important to our economic security, but the jobs are well-paid, in high demand, and less susceptible to outsourcing overseas. Unfortunately, there are simply not enough qualified candidates to do the work, and there is an urgent and growing need for more cybersecurity professionals. The 2014 job market for cybersecurity positions grew twice as fast as the overall IT job market in 2013. One industry member of the Governor's Cybersecurity Task Force remarked that it was difficult to find qualified people for the thousands of open jobs: “The number one challenge that I hear from employers now is…that it can take months or years to take somebody who even has engineering and science education and help them build the specific skills needed to practice cybersecurity.”

In fact, while the private sector is experiencing a shortage of cybersecurity professionals, the problem is even worse for the public sector – state law enforcement entities in our largest cities are struggling with shocking shortages of qualified personnel, a situation that puts all Californians at risk. California law enforcement needs new training resources to keep up with increasingly well-funded, sophisticated, and evolving criminal methods.

The State can take action in two primary areas: standardizing and funding educational pipelines for high-demand cybersecurity positions, and building out our digital forensics training capabilities. While there are nearly 100 postsecondary academic institutions in California offering some form of cybersecurity course, there is a concerning lack of standardization, especially when the industry relies heavily on a system of credentials that qualify specific skillsets.

Following the model of the National Initiative for Cybersecurity Education (NICE), the State should work with the public and private sector to address shortages with

measurable outcomes, building educational pipelines with employers from the job back to the academic institution. Lastly, the State should fund the development of digital forensics training and solicit funding from the Federal government and private interests for that purpose. As all aspects of criminal activity take on a digital element, law enforcement must equip themselves with the skills and tools to effectively detect and deter advanced cybercrime.

*** * ***