# Preparedness Summit Cybersecurity Panel

Presented by: Nora Wetzel

# NORA
# WETZEL

## Burke, Williams & Sorensen LLP

**Nora has been designated as a Certified Information Privacy Professional, United States (CIPP/US) by the International Association of Privacy Professionals (IAPP).**

Nora advises clients regarding their compliance with U.S. federal and state privacy laws, privacy and cyber security related contractual obligations, and breach response.

# CYBERSECURITY AND LAW

Lack of universally applicable cybersecurity specific laws
Why?

- Law is slow to evolve
- One size Fit all Approach does not work in this context

- Cybersecurity – constantly evolving.
  - new threats detected constantly
  - Technology advances rapidly and changes quickly

- Industry specific regulation more common (banking, healthcare, etc)

# PUBLIC RECORDS STORAGE

While mostly applicable to state agencies instead of local government, there are requirements for public records storage that applies to local government by contractual agreement.

**Section 12168.7 of the Government Code:**

(A) adopt uniform statewide standards for the purpose of storing and recording public records in electronic media or in a cloud computing storage service.

(b) In order to ensure that uniform statewide standards remain current and relevant, the Secretary of State, in consultation with the Department of Technology, **shall approve and adopt appropriate uniform statewide standards** by using standards that are accredited by the American National Standards Institute or other applicable industry-recognized standards making body, including the International Organization for Standardization TR 15801:2017 or successor standard**, for storing and recording public records in electronic media or in a cloud computing storage service**.

# PUBLIC RECORDS STORAGE

( (f)(1)A state agency, prior to establishing an information technology system interconnection or data exchange with a local government entity or otherwise partnering with a local government entity for the development, use, or maintenance of an information technology system, product, or service, **shall first enter into a written agreement with that local government entity for the purpose of establishing mutually agreeable terms that protect relevant public records**.


# PENDING LEGISLATION

## CA A.B. 581

(Section 11549.3 of the Government Code is amended)

Status: Pending

Requires all state agencies, as generally defined, to review and implement specified National Institute of Standards and Technology (NIST) guidelines for, among other things, **reporting, coordinating, publishing, and receiving information about a security vulnerability** relating to **information systems** and the resolution thereof, no later than July 1, 2022.


# PENDING LEGISLATION

**CA A.B. 581 (continued)**
Status: Pending

**The bill would authorize a state agency to satisfy their requirement to implement NIST guidelines by adopting those standards and procedures published in the State Administrative Manual and Statewide Information Management Manual**. The bill would require the office to provide assistance to any state agency that requests assistance in implementing the guidelines or the standards and procedures, and to provide operational and technical assistance to state agencies on reporting, coordinating, publishing, and receiving information about cybersecurity vulnerabilities of information systems, until that agency withdraws their request for assistance with implementation or cybersecurity."


# STATE ADMINISTRATIVE MANUAL

SAM currently requires state agencies to follow NIST 800-53

- 800-53 addresses, for example,
  - Usage restrictions
  - System monitoring
  - Denial of service protection
  - Transmission confidentiality and integrity
  - Cryptographic key establishment and management

# PENDING LEGISLATION

## CA A.B. 809

Status: Pending (Section 11549.3 of the Government Code)

**Requires state agencies not covered by** the policies and procedures issued by the Office of Information Security within the Department of Technology **to adopt and implement information security and privacy policies, standards, and procedures based upon standards issued by the National Institute of Standards and Technology and the Federal Information Processing Standards**.

# California Cybersecurity Integration Center “CSIC”

## Cal. Govt  Code § 8586.5

(a) “the California Cybersecurity Integration Center shall 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 nongovernmental organizations.”

# California Cybersecurity Integration Center “CSIC”

## Cal. Govt  Code § 8586.5 (continued)

(c) 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 shall 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 shall also 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.

Even though not mandated, **voluntary participation with CSIC may be helpful**

https://www.caloes.ca.gov/cal-oes-divisions/law-enforcement/california-cybersecurity-integration-center

“State, local, and tribal governments, non-governmental organizations and the private sector **can partner** with the Cal-CSIC by registering to receive Alerts and Advisories, sharing IOCs and cyber incident reports, and connecting to the California Automated Indicator Exchange.

# CSIC


# Bulk Electric Systems Subject to CIP

- Critical Infrastructure Protection (CIP)  Reliability Standards overseen by North American Reliability Council (NERC) and the Federal Energy Regulatory Commission (FERC).
- Includes Cybersecurity requirements:
  - Cyber System categorization
  - Security management controls
  - Personnel and training
  - Electronic security perimeters
  - System security management
  - Incident reporting and response planning
  - Recovery planning
  - Configuration change management
  - Information protection

# BES Subject to NERC Supply Chain Mgmt.

- NERC issued supply chain management requirements.
- (FERC) issued Order No. 829 directing the North American Electric Reliability Corporation (NERC) to develop a new or modified Reliability Standard that **addresses cyber security supply chain risk management for industrial control system hardware, software, and computing and networking services** associated with Bulk Electric System (BES) operations as follows:

https://www.nerc.com/pa/comp/guidance/DraftImplementationGuidanceDL/CIP-013-1-R1%20Implementation%20Guidance.pdf


# Critical Pipeline Operators

- TSA Pipeline Security Guidelines
  - Apply to natural gas and hazardous liquid transmission pipelines, natural gas distribution pipeline systems, and liquefied natural gas facility operators.
  - Establish risk-based corporate security program

- DHS's Security Directive requires **reporting confirmed and potential cybersecurity incidents to the DHS** Cybersecurity and Infrastructure Security Agency (CISA), **designating a Cybersecurity Coordinator,** to be available 24 hours a day, seven days a week, and **review of current practices as well as to identify any gaps and related remediation measures to address cyber-related risks** and report the results to TSA and CISA within 30 days.

# America's Water Infrastructure Act

- Applies to community drinking water systems serving more than 3,300 people
- Required to develop or update risk assessments and emergency response plans
- Includes assessing risks to electronic, computer, or other automated systems INCLUDING THE SECURITY of such systems.
- Resource: AWWA  Guidance and Assessment Tool to align to NIST Cybersecurity Framework and AWIA

# EPA Cybersecurity Best Practices for the Water Sector

- **Cyber Resilience resources**
  - Water Sector Cybersecurity Brief
  - Incident Action Checklist.
  - Training and Response Exercises
  - Technical Assistance Provider Program
    - Great for state and regional water systems

# DATA BREACH

Even if not required by law to implement specific cybersecurity practices, following cybersecurity best practices is advised anyway to reduce risk of data breaches.  Public entities ARE required to comply with California's  data breach statute Civil Code section 1798.29

# DATA BREACH

a) **Any agency** that owns or licenses computerized data that includes personal information **shall disclose** any **breach of the security of the system** following discovery or notification of the breach in the security of the data to any resident of California … The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.


# DATA BREACH

Reacting to data breaches can be complicated and expensive.

An agency must investigate what happened—using an outside forensic investigator is recommended.

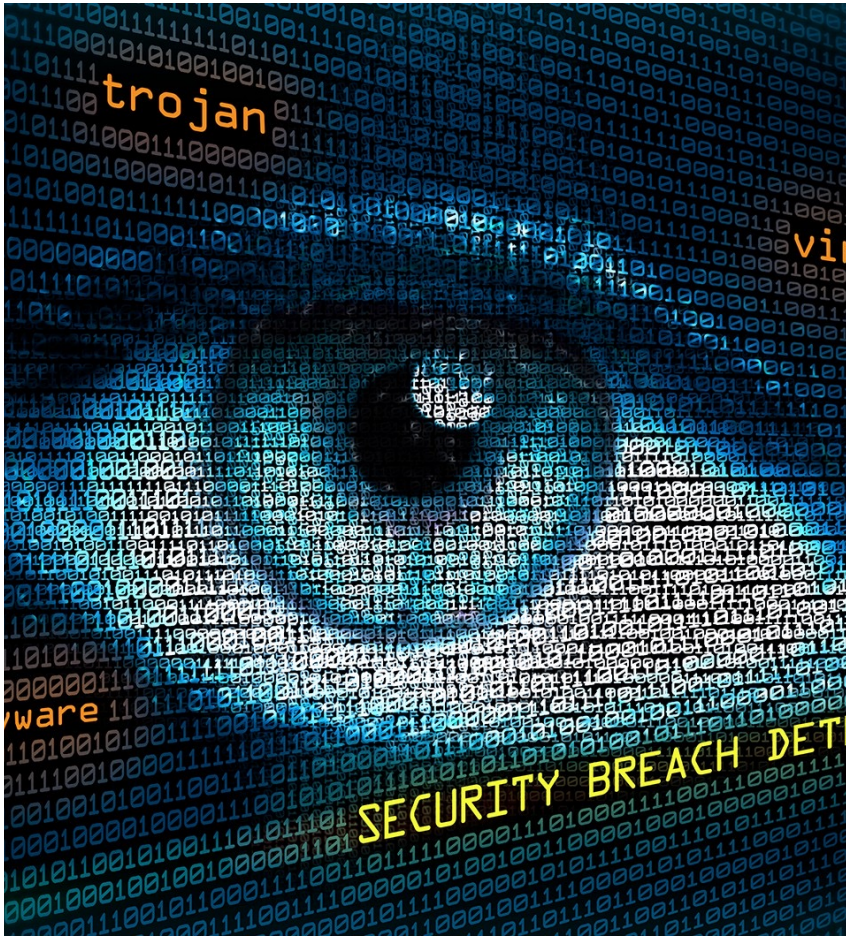
Depending on how many individual's personal information was affected, there could be a large number of persons entitled to be notified, warranting use of an outside vendor to handle the mailing and setting up a call center to handle calls from affected individuals inquiring as to the breach.

# RECOMMENDATIONS

Breaches are common:

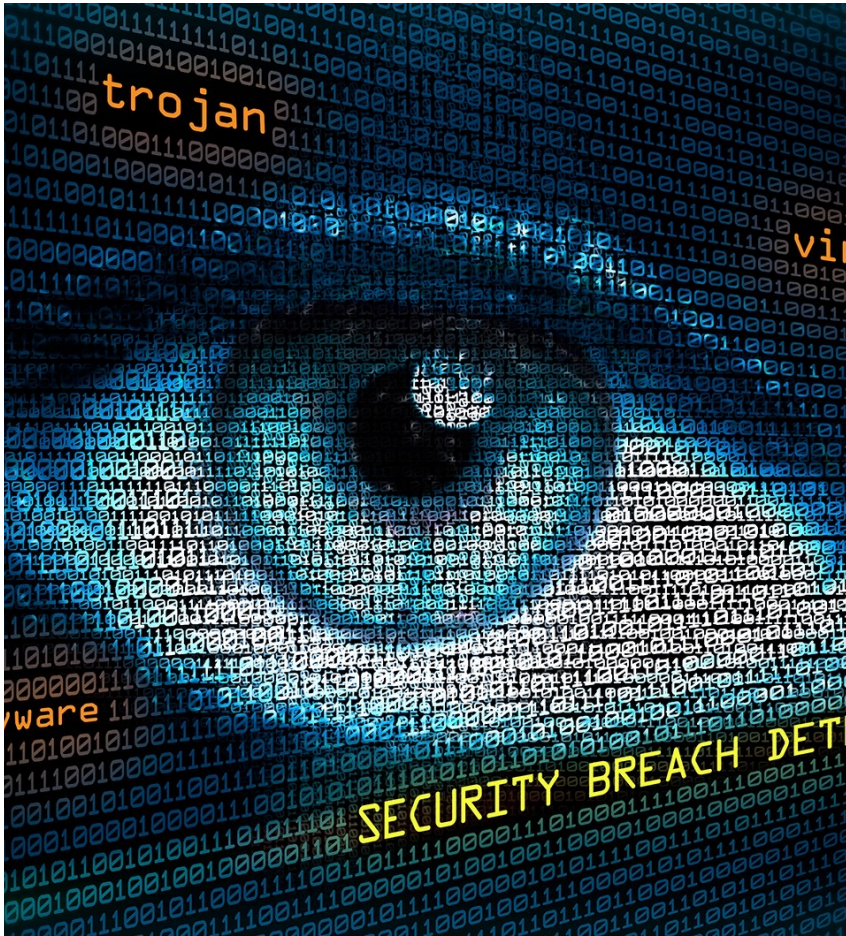
- Develop an incident response plan and incident response team
- Useful resource: CSIC incident response guide
  https://www.caloes.ca.gov/LawEnforcementSite/Documents/California-Joint%20Cyber%20Incident%20Response%20Guide.pdf

“This document is designed to assist governmental and non-governmental entities within California, including State, Local, Tribal, Territorial and Private Sector (SLTTP) understand the importance of establishing and maintaining an Incident Response Plan (IRP) and incident response capabilities, including an Incident Response Team (IRT).”



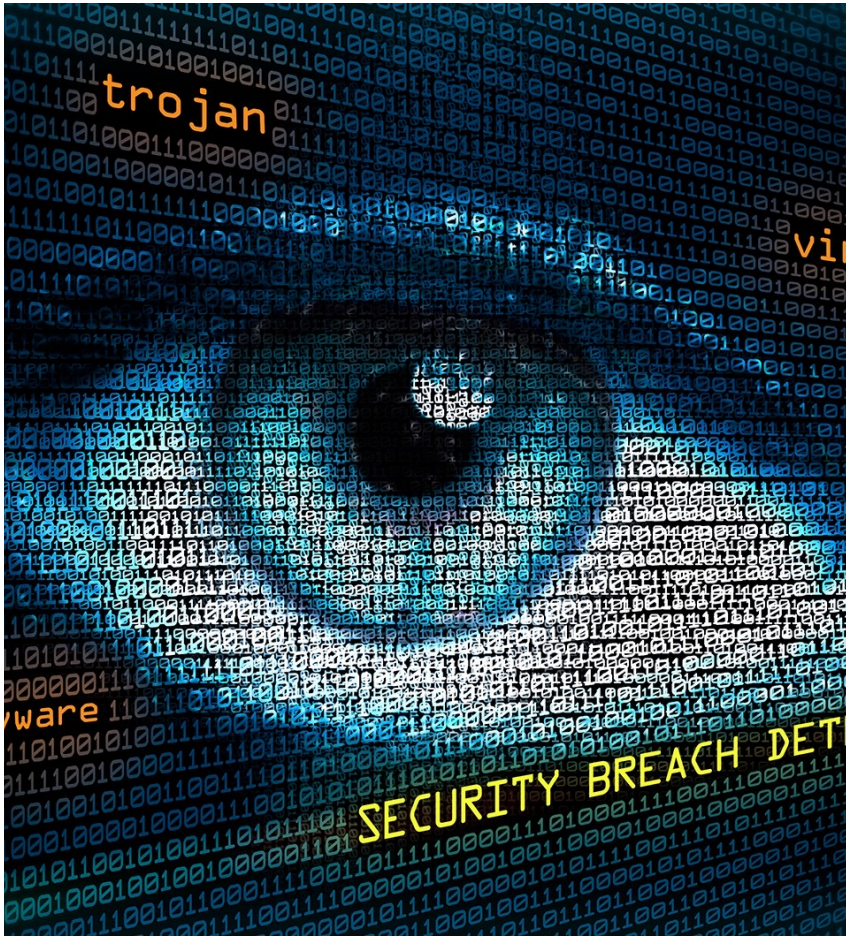
# RECOMMENDATIONS

- **Cyber insurance**
  - Cal JPIA insured programs
    - Cyber Liability Program
      https://cjpia.org/coverage/insured-programs/
- **Risk management organizations**
  - California Intergovernmental Risk Authority; CAL JPIA.



# RECOMMENDATIONS

- **Vendors to public entities:**
  - Lesser thought of vulnerability vector for public agencies: your vendors
  - Review Contracts with vendors for cybersecurity related terms and cyber insurance requirements
  - Useful resource: Alliant insurance requirements in contracts *https://www.cira-jpa.org/wp-content/uploads/2021/11/IRIC.pdf*




THANK YOU!
Presented by: Nora Wetzel