California's Internet of Things Security Requirement

California State Assemblywoman
Jacqui Irwin

IoT Threat Landscape

- Threat to Personal Safety
  - Access to operational devices that can endanger life
  - Access to operational devices that can harm property

- Threat to Personal Privacy
  - Access to devices with microphones
  - Access to devices with cameras
  - Access to devices with various other sensors

- Threat to Society at Large
  - Botnets engaging in DDoS (Distributed Denial of Service)
  - Devices in Critical Infrastructure Environments

AB 1906 (Irwin, Chapter 860 Statutes of 2018)

- Equip the device with a reasonable security feature or features that are all of the following:

  (1) Appropriate to the nature and function of the device.
  (2) Appropriate to the information it may collect, contain, or transmit.
  (3) Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.

- Directed manufacturers away from using generic default passwords, and designing with hardcoded passwords.

- Oregon enacted a similar law in 2019, and the following Legislatures have introduced similar bills HI, IL, KY, MA, MD, NJ, NY, RI, VT, WA

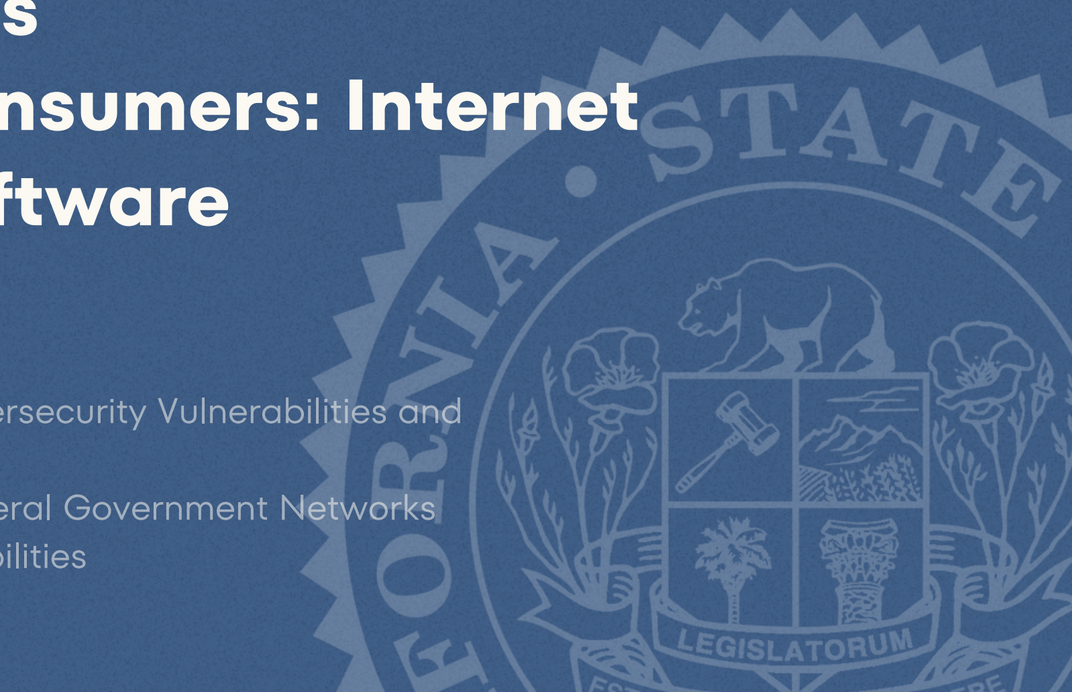
EO 14028 Improving the Nation's Cybersecurity

Sec. 1 - Policy
Sec. 2 - Removing Barriers to Sharing Threat Information.
Sec. 3 - Modernizing Federal Government Cybersecurity

Section 4 -Enhancing Software Supply Chain Security

- **Directs NIST to Develop Standards**
  - **Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software**

Sec. 5 - Establishing a Cyber Safety Review Board
Sec. 6 - Standardizing the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents.
Sec. 7 - Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks
Sec. 8- Improving the Federal Government's Investigative and Remediation Capabilities
Sec. 9 - National Security Systems



NIST Cybersecurity White Paper

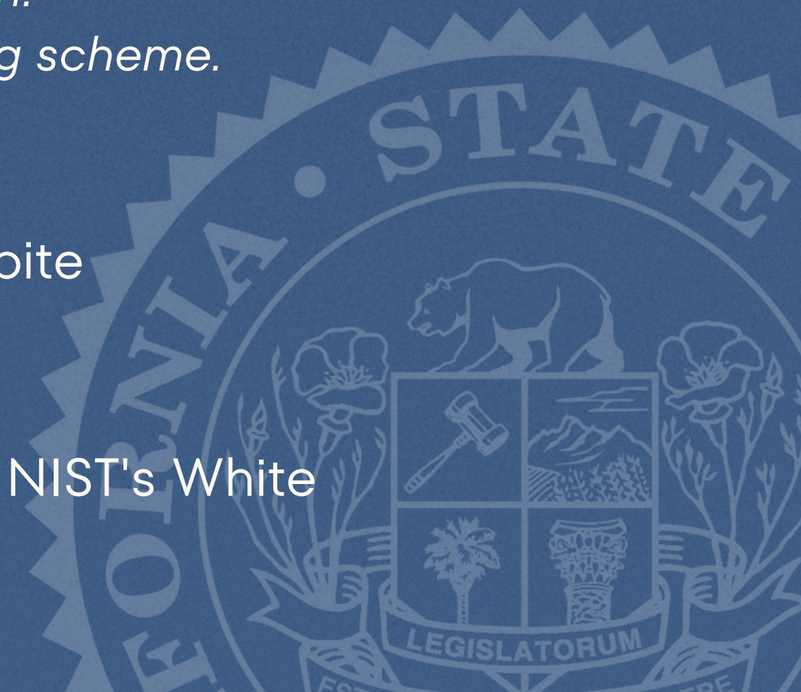
Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products *February 2, 2022*

- Recommended Baseline Product Criteria
- Labeling Considerations
  - Support non-expert, home users of IoT products
  - A binary label (a single label indicating a product has met a baseline standard) should be adopted for an IoT cybersecurity label. NIST also recommends coupling the binary label with a layered approach with a URL or scannable code for consumer education
- Conformity Assessment Considerations
  - Declaration ⟶ Third-party Testing ⟶ Third-party Certification

AB 2392 (Irwin, 2022)

- Provides that a manufacturer will satisfy CA's security requirement if the IoT device
  - *Meets or exceeds the baseline product criteria of a NIST conforming labeling scheme.*
  - *Satisfies a conformity assessment as described by a NIST conforming labeling scheme that includes a third-party test, inspection, or certification.*
  - *Bears the binary label as described by a NIST conforming labeling scheme.*

- Next logical step after AB 1906, motivated by:
  - Lack of Enforcement of AB 1906 by Public Prosecutors despite widespread non-compliance
  - Little to no incentive coming from Federal Government for manufacturers to adopt and create labeling scheme from NIST's White Paper



Contact Info
Brandon Bjerke
Brandon.Bjerke@asm.ca.gov
Legislative Director,
Office of Asm. Jacqui Irwin