FOR IMMEDIATE RELEASE
September 28, 2018

CONTACT: Brandon Bjerke
brandon.bjerke@asm.ca.gov

Assemblymember Irwin Bill to prevent hacking of IoT devices signed into law by Governor Brown

"We must stop our own devices from being leveraged against us"

SACRAMENTO – AB 1906, authored by Assemblymember Jacqui Irwin (D- Thousand Oaks), was signed by Governor Jerry Brown today, after passing the Legislature last month with bipartisan support. The law will require manufacturers to equip smart devices with a reasonable security feature or features to prevent cyberattacks.

"With our growing reliance on Internet of Things (IoT) devices, the threat that unsecure devices pose to individuals, businesses, and our state looms large, ensuring we have the right tools to keep our devices and information secure is critical," said Assemblymember Irwin. "This new law was the result of hard work with many stakeholders from the business, technology, privacy, and consumer communities."

In 2016 the Mirai BotNet, a collection of infected routers, cameras, and digital video recorders conducted distributed denial of service (DDoS) attacks that clogged servers and shut down popular websites like Twitter and Netflix for six hours. Another DDoS attack on a popular cybersecurity blog shut down access for even longer, nearly 77 hours. A February 2017 attack on 160,000 vulnerable printers from popular brands resulted in a hacker sending a print job to each one, warning the user of their failed security. All of these attacks were the result of inadequate security on IoT devices.

To combat these types of attacks, and other emerging ones like "crypto-jacking", the security requirement in AB 1906 is a flexible standard, taking into account that IoT devices can vary widely. Manufacturers would need to make security features appropriate to the nature and function of the device, appropriate to the information stored on the device, and design the features to prevent unauthorized remote access. The law follows the general practice in technology related public policy of avoiding prescriptive or technology specific requirements, which are doomed to be quickly outdated and restrictive of innovation.

Over the past decade the world has seen an exponential growth in "smart" devices, leveraging internet connectivity to make our lives more efficient. From smart thermostats, smart locks, to smart trash cans, the ability to remotely sense or control a device has transformed many aspects of home life and hold the promise of changing how governments and businesses serve the public. In 2016 there were 5 billion IoT devices, and industry growth estimates have ranged from 20 billion IoT devices in 2020 to 1 trillion IoT devices by 2025.

This widespread adoption, however, has come with an increase in risk and harm. Security features for these IoT devices are usually less robust than traditional computers or smart phones due to a misconception that they do not provide access to sensitive information, and the user-friendly interest for them to be easily added into a "smart home" network.

These user-friendly settings like default passwords, have allowed millions of devices to become infected with various forms of malware. These devices when used together to conduct DDoS attacks threaten all of us, but do not require sophisticated hackers with money and resources. When using infected IoT devices an attack is at the expense of the victims, the IoT owners who purchase the devices and pay the utility bills to run them.

"The Internet of Things will continue to transform how we live, work, and relax for decades to come" said Assemblymember Irwin. "I applaud the Governor's forward thinking in agreeing to provide this important consumer protection to Californians deciding to add IoT devices into their daily lives. We must stop our own devices from being leveraged against us."

The law will go into effect on January 1, 2020 as stated in the text of the statute. The delayed implementation date will allow manufacturers time to evaluate their current and planned connected devices in light of the new requirement and make any necessary changes before the effective date. Assemblymember Irwin as Chair of the Assembly Select Committee on Cybersecurity plans to engage with manufacturers and technology companies in the coming months to discuss current and emerging trends in IoT security to facilitate rapid and seamless compliance with the new requirement.

AB 1906 passed the Assembly 60-17 and the State Senate 29-8 in the last week of the legislative session.

Assemblymember Jacqui Irwin represents California's 44th Assembly District, which includes the communities of Camarillo, Casa Conejo, Channel Islands Beach, El Rio, Lak e Sherwood, Moorpark, Oak Park, Oxnard, Port Hueneme, Santa Rosa Valley, Thousand Oaks, and Westlake Village.

Assemblymember Irwin's website: http://asmdc.org/irwin

###