SIA 2019 State Policy Priorities

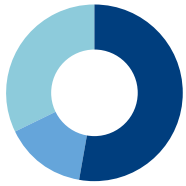
SIA
SECURITY INDUSTRY ASSOCIATION

Who SIA Represents

Nearly

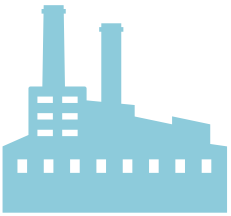
1,000

Member companies representing thousands of security professionals



Membership Breakdown

- Manufacturers, 53%
- Integrators, 15%
- Service Providers, 32%



$25B

In physical security products produced at factory gate prices

Markets Served

- Airports/Seaports
- Chemical Facilities
- Commercial/Retail Facilities
- Data Centers/IT Infrastructure
- Energy Sector
- Government/Military Facilities
- Health Care/Pharmaceutical
- Homeland Security
- K-12/Higher Education
- Law Enforcement/Corrections
- Mass Transit
- Residential

Advancing the Industry

Visit **securityindustry.org/advocacy** for the latest information on SIA federal/ state policy priorities and related actions.

Contact

Jake Parker
Director of Government Relations
jparker@securityindustry.org; 301-804-4722

Joe Hoellerer
Sr. Manager of Government Relations
jhoellerer@securityindustry.org; 301-804-4714

Drake Jamali
Manager, Government Relations
djamali@securityindustry.org; 301-804-4707

Licensing and Permitting

Security Industry Association (SIA) members strongly believe in investing in a highly-trained, licensed and skilled workforce that readily meets customer needs for security and life safety systems installation and maintenance, and we support a regulatory structure appropriate for low-voltage alarm work. Security systems installers are highly trained in their field; they typically undergo security industry-specific classroom training and must complete continuing education courses to maintain their license. SIA is concerned with proposals that would make it harder for currently licensed personnel to conduct low-voltage alarm work by imposing unnecessary requirements as well as proposals that would weaken essential qualifications. Additionally, SIA supports addressing long-outdated and unnecessary local permitting requirements by providing a statewide exemption for wireless, low-voltage alarm systems.

2019 Session Highlights

Legislation SIA Supports:

Tennessee – HB 602/SB 1443: Prohibits local governments from requiring an alarm systems contractor or business to acquire electrical permits for the operation of alarm systems and prohibits local governments from imposing fines or fees on an alarm systems provider (versus the property owner) for false alarms.

California – AB 1289: Prohibits a local government from fining an alarm company for requesting emergency dispatch to an unregistered user if it was not the alarm company's responsibility to register or renew that customer's registration.

Legislation SIA Opposes:

Texas – HB 1141: Would remove a current exemption from electrical licensure requirements for alarm installers performing low-voltage work by establishing a threshold triggering the requirements at 50 volts, which would force such workers to obtain unnecessary licenses.

School Safety

SIA supports increased state and local assistance to schools struggling with the cost of meeting security needs, along with the adoption of successful statewide safe schools programs and nationwide use of best practices for school security. Supporting proven, effective school safety programs and practices at the state level is a key policy priority for SIA as more school districts seek to evaluate and enhance the safety of K-12 facilities. SIA endorses the work of the Partner Alliance for Safer Schools (PASS), which has brought together expertise from the education, public safety and industry communities to create the K-12 school safety and security guidelines found at passk12.org.

2019 Session Highlights

Legislation SIA Supports:

Georgia – SB 15: Allows public schools to request funding from the state for safety improvements or initiatives, such as the installation of safety equipment, including video surveillance cameras, metal detectors, alarms, communications systems and building access controls.

Indiana – SB 266: Allows schools to use available security grants for emergency communications systems and encourages districtwide electronic access to facilities for responders in the event of emergencies and access to video security system data from a central location.

Legislation SIA Opposes:

Wisconsin – AB 44/SB 53: Allows local jurisdictions to exempt classroom door "barricade" devices from fire and life safety code requirements. Offering no security advantage over a lockset appropriate for classrooms, the devices are unnecessary from a security standpoint, can be difficult for occupants to both deploy and remove to exit and can be misused to prevent entry by responders.

The Internet of Things (IoT) and Cybersecurity

IoT has allowed devices to perform more effectively with better data, including IP-enabled safety and security solutions that are vital to protecting people, property and information around the country. Security technologies can be effectively integrated within broader frameworks of sensors throughout the IoT ecosystem, including smart cities, smart transportation and smart grids, in order to support public safety, increase situational awareness and enhance emergency response. SIA supports policies encouraging smart and secure IoT deployments that leverage security technologies for these purposes.

Cybersecurity is an integral component of the IoT ecosystem, and robust cybersecurity safeguards enable IoT devices to become smarter, data-centric and resilient. Resiliency to cyberattacks targeting IoT is a major concern facing state governments and their residents.

SIA supports policies that bolster IoT expansion and cybersecurity based on best practices and voluntary, consensus-based standards, while opposing overly prescriptive or vague product requirements that could expose technology innovators to unwarranted legal risks.

2019 Session Highlights

Legislation SIA Supports:

California – AB 659: Creates the California Smart City Challenge Grant program and authorizes $10 million for grants to develop innovative smart city projects that benefit the community at large.

Texas – SB 475: Establishes the Texas Electric Grid Security Council to develop best security practices for mitigating the risk of cyber and physical attacks that may affect the reliability of the power grid in Texas.

Legislation SIA Opposes:

Oregon – HB 2395: Sets prescriptive device-level cybersecurity feature requirements in law broadly applicable to almost all internet-connected devices, including components of commercial and industrial systems. Such requirements would eventually become obsolete and even counterproductive to cybersecurity while potentially disrupting core functions and threatening interoperability of IoT devices.

Right to Repair

SIA is concerned with "Right to Repair" legislation proposed in more than 20 states that would force original equipment manufacturers (OEMs) to disclose sensitive information to unauthorized and uncertified repair providers. If any of these measures are enacted, OEMs and authorized repair providers – many of which are small businesses – could see the erosion of stable revenue sources and certification opportunities. While vehicle repair or consumer electronics are often provided as examples, Right to Repair legislation would have a much broader impact. Allowing unauthorized service providers free access to sensitive product information could result in serious consequences for the integrity and functionality of complex residential and commercial security and life safety systems. Liability issues are not addressed in any current Right to Repair legislation, presenting unanticipated risks to property owners that rely on security solutions to prevent burglaries, fires or carbon monoxide leaks. Publishing software updates, source code and encryption keys would not only impact OEMs, but could also put consumers at greater risk of cyberattack.

Biometrics Technology

SIA supports policies that foster growth and the responsible use of biometrically-enabled security technologies across commercial, government and public safety sectors. Legislation supporting and setting parameters for biometrics use in certain security settings, especially public safety agencies, can bring numerous safety and security benefits to Americans. Conversely, legislation that unnecessarily restricts such uses, such as Illinois' Biometric Information Protection Act, inevitably creates a litigious environment in which the private sector has a disincentive to adopt technology solutions that not only streamline business practices, but also protect sensitive data, personnel, critical infrastructure and other physical structures.

2019 Session Highlights

Legislation SIA Supports:

Minnesota – HF 487: Authorizes the use of facial recognition technology as part of the Minnesota driver's license and identification card application and renewal process to ensure no individual is issued multiple licenses or ID cards, prevent identification fraud and expedite application and renewal processing.

New York – A 2830: Establishes the Medicaid identification and anti-fraud biometric technology pilot program as an anti-fraud mechanism and verification tool for Medicaid recipients or providers.

Legislation SIA Opposes:

Washington – HB 1654/SB 5528: Prohibits the use of facial recognition and other biometrics technologies by all state government entities.

California – The city of San Francisco enacted an ordinance banning the use of all facial recognition software by city departments and imposing other types of security technology restrictions that ultimately weaken public safety.

Domestic Procurement Restrictions

Many states have procurement rules that give contractual preferences for construction materials that are produced in the United States or even within the state. Proposals in some states to extend such preferences to manufactured goods can be problematic when it comes to electronics. Many of today's security and life safety systems either incorporate or consist entirely of electronic components, sourced through global supply chains. Unlike federal "Buy American" and related rules, states typically do not include exceptions for commercial IT items or goods manufactured by one of our trading partners. Suppliers to state governments cannot avoid sourcing at least some system components from outside the U.S. for many products that are crucial to fire safety and alarm systems, for example. For these reasons, SIA generally opposes measures that would increase domestic content requirements for manufactured goods unless they incorporate necessary exemptions for security and life safety solutions.