February 15, 2024

***Via Electronic Mail***

Sen. Janeen Sollman, Chief Sponsor, SB 1596
Members of the Oregon State Senate
Members of the Oregon House of Representatives

**Re: Alarm Industry Concerns Regarding Oregon Right-to-Repair Legislation (SB 1596)**

Dear Senator Sollman and Honorable Members of the Oregon State Legislature:

The Alarm Industry Communications Committee (AICC), on behalf of the many central station alarm companies represented within its membership, respectfully expresses its concerns about the current version of SB 1596 and urges members of the Oregon State Legislature not to advance the proposed legislation in the absence of an amendment to exempt electronic security and life safety systems from the scope of the bill. AICC does not oppose the concept of allowing Oregon's citizens the freedom to repair the vast majority of consumer electronic devices; however, application of right to repair requirements to central station alarm technology and other security devices would endanger public safety by creating vulnerabilities in alarm monitoring systems that are used protect the citizens of Oregon from the threat of fires, medical emergencies, home invasion and other life-threatening issues. If the disclosure of passwords, access codes, schematics and other information generally required by right to repair bills were to be applied to certain alarm devices, every family, business, hospital, bank, jewelry store, and power plant protected by one of these alarm devices could be put at risk. To the extent that the Oregon State Legislature decides to move forward with digital electronic right to repair legislation, AICC suggests incorporation of an exclusion that that would ensure that those who have purchased alarm systems can continue to rely of on the protections these systems afford:

> *Nothing in this Act (including any requirement to disclose security codes, passwords or system schematics) shall apply to a manufacturer, dealer, distributor, integrator, installer or monitoring service provider of a security device or alarm system (including but not limited to all central station alarm systems and any other digital electronic equipment used to prevent, detect, protect against, or respond to fire, carbon monoxide risks, falls, medical alerts or security incidents or control access to residential, commercial, and governmental property, services, or information systems).*

AICC is a committee formed by The Monitoring Association (TMA), representing the vast majority of entities providing central station alarm security protection services. The Electronic Security Association (ESA) (representing security and fire alarm service providers) and the Security Industry Association (SIA) (representing alarm system manufacturers) are also members of AICC. Central station alarm operations protect tens of millions of families in their homes, a wide range of hospitals, businesses, public utilities and key

government facilities (including military installations). Alarm companies utilize complex wireline, wireless and IP-based security systems. Much of their equipment must be installed and maintained in accordance with Underwriters Laboratories and the National Fire Code (NFPA 72) requirements.

Central station alarm services often act as the "front line" in dispatching municipal police, fire units and emergency medical services. Alarm systems located on a customer's premises sense fire, home and business invasions, medical emergencies, carbon monoxide and other threats, and instantly transmit this data to a central station. The central station in turn screens the alarm and alerts the Public Safety Answering Point (PSAP), *i.e.*, the dispatch office of municipal authorities, usually police, fire or medical/rescue departments, which then dispatches police officers, fire fighters, EMTs/paramedics and other first responders. This partnership between the alarm industry and the public safety community has literally saved countless lives.

Without an exemption for electronic security and life safety systems, AICC is concerned that requiring an "open platform" concept for any central station alarm systems would create the genuine risk that a repaired or modified alarm system would be vulnerable to hacking, either because unscrupulous repair personnel may utilize the access codes, passwords or other information for nefarious purposes, or because these persons may store such sensitive information in a fashion that could be hacked by a third party. The daily news is rife with instances of consumer information being hacked due to poor security practices, which may be a significant risk in the case of what may be undercapitalized small repair shops. If access codes, passwords, or alarm system schematics are either hacked or innocently made public (e.g., as part of a You Tube self-help video or iFixit online manual exhibiting how to power down a system, re-route a signal, or deactivate a system's communication capability), it could allow malevolent actors to shut down entire alarm systems, endangering tens or hundreds of thousands of Oregon's citizens, and potentially millions nationwide. If a bad actor is armed with such information, they can use it to disable similar alarm systems throughout the country. A theft ring could access a bank alarm system and shut it down, allowing robbery. Public transit surveillance camera systems could be shut down. Terrorists could disable the alarm protection system for a power plant and enhance their chances of shutting down the grid. Or worse, access could be gained to important defense installations in Oregon or nuclear power plants throughout the country. Also, with the increasing use of video cameras for protecting homes and businesses, bad actors could gain remote access to video files of alarm customers and use surveillance information to gauge behaviors, timing and related activities of the protective premise for planning break ins or other crimes.

Fortunately, based on input from the alarm industry, the State of New York recognized these risks when considering very similar legislation, which it amended to exempt alarm systems and security devices as part of the state's Fair Repair Act (in SB 4104-A, as amended by NY Fair Repair Act Chapter Amendments S. 1320); the State of California included a broad alarm exemption in its recently enacted Right to Repair Act (SB 244); and the updated version of the Michigan Digital Equipment Repair Act (House Bill 4562) includes an exemption for alarm systems based largely on the exemption language proposed by AICC above. See HB 4562 proposed substitute H-1 (9/12/2023) (mi.gov). Newly-filed right to repair bills introduced in Hawaii (SB 2700), Arizona (SB1536) and Illinois (SB2680) include alarm system and fire protection exemption language similar

to that used in California. AICC asks that as Oregon considers any right to repair legislation, it should recognize the need for a specific and narrow exemption for alarm systems, in order to protect the safety of its citizens.

AICC notes the Oregon legislature's concern over reduction of environmental waste as part of its right to repair initiative. Fortunately, most alarm devices are designed to last several years, often approaching a decade or longer. The purpose of an alarm system is to protect against loss of life and property, and as such quality and reliability is inherently built into the products, thereby limiting the need for repair.

Indeed, the alarm industry has a documented practice of advocating that the Federal Communications Commission (FCC) should allow alarm devices to remain in service for as much of the full lifespan as possible. Thus, AICC urged the FCC to delay the sunset of analog cellular service, since this sunset would require more than a million alarm customers to buy a new alarm radio. See February 21, 2006 Comments of AICC in WT Docket No. 01-108 at p. 8 (AICC requests multi-year extension due to cost of replacement radio for consumers, and because "many of these consumers purchased their analog radios within the past couple of years, and who could normally expect another seven or eight years of use."). Because the alarm industry generally seeks to utilize long-lasting equipment and avoid unnecessary device churn, it also minimizes the environmental waste concern.

Alarm devices also avoid the issue of sealed-in batteries that are difficult to replace, and thus require premature disposal of devices. Most alarm panels and several other alarm devices feature easy-to-remove batteries, and alarm companies often ship a replacement battery to the customer for self-install (since this can be done without compromising the system).[1]

Respectfully submitted,

**ALARM INDUSTRY COMMUNICATIONS COMMITTEE**

Tiffany Galarza, Co-Chair
Sascha Kylau, Co-Chair
c/o The Monitoring Association
7918 Jones Branch Drive, Suite 510
McLean, VA 22102
703-242-4670
www.tma.us

cc: Members of the Colorado General Assembly

[1] *See, e.g.*, How can I replace my alarm system battery? (adt.com) https://help.adt.com/s/article/How-can-I-replace-my-alarm-system-battery#:~:text=To%20replace%20the%20battery%3A,wire%20to%20the%20BLACK%20tab. Another example is Telguard video surveillance units and cellular communicators, which use readily replaceable batteries. *See, e.g.*, Telguard BMR-1208 0.8 Amp-Hour Battery For TG-1B And TG-4 (americanbuildersoutlet.com).