Cybersecurity Law and Networked Lighting Controls

California's Civil Code Title 1.81.26, Security of Connected Devices, approved under Senate Bill No. 327 (2018) is effective on January 1, 2020. This law is the first of its kind and is designed to provide discipline and minimum-security requirements to protect all connected devices and data from unauthorized access and other malicious actions.

Why This Law Matters?

There has been an explosion of electronic devices designed to help us with everyday tasks. Connecting these devices to the internet opens the door to a host of security concerns, including data breaches. Up to this point, there has been a lack of minimum-security requirements imposed by the industry or government. Now California has become the first state to address the security of connected devices to protect data, and there are other states discussing similar legislation.

Connected Device Definition

The law defines a connected device as any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and is assigned an Internet Protocol (IP) address or Bluetooth® address.

One Lithonia Way, Conyers, GA 30012 | Phone: 1.800.705.SERV (7378) | www.acuitybrands.com

Networked Lighting Controls California Civil Code Title 1.81.26, Security of Connected Devices

Acuity Brands is taking this new law very seriously and has engaged in a year-long review of all its connected devices, including nLight®, Atrius®, Fresco™, ROAM®, and Pathway Connectivity Solutions® products. This review consisted of validating existing security measures and implementing additional security features so that all Acuity Brands products/solutions offered for sale in California after January 1, 2020, at a minimum, will comply with Title 1.81.26.

Quick Summary of Title 1.81.26 Main Requirements

- Equip the device with feature(s) to reasonably protect the security of the device and data relative to the risk posed
- If a device is allowed access outside of a local area network, it needs either:
  a. A unique password for each device when manufactured, or
  b. To require users to set their own password the first time they connect, or
  c. Other reasonable measures

Acuity Brands Commitment to Security

Acuity Brands is fully committed to developing and maintaining secure products and has a robust product security program in place. This commitment includes incorporating core security principles and best practices early into the product development lifecycle and implementing security governance policies that follow industry best practices and guidelines.

For more information, contact the Acuity Brands cybersecurity team.
www.AcuityBrands.com/ PSIRT

** This document is for general information purposes only and is provided without any warranty as to accuracy, completeness, reliability or otherwise. It is not offered as legal advice and should not be taken as such. Please consult with your legal advisors to determine compliance of Acuity Brands products/solutions with applicable law.*

One Lithonia Way, Conyers, GA 30012 | Phone: 1.800.705.SERV (7378) | www.acuitybrands.com