1. **Is WaveLinx secure?**
Yes, The WaveLinx System uses a multi-tiered approach to addressing industry best practices for security risk management and utilizes guidelines promulgated by the Department of Homeland Security (DHS), National Institute of Standards and Technology (NIST) and industry standards organizations to achieve a secure and adaptable lighting control platform.

2. **What are the tiers for security?**
WaveLinx uses a seven layer multi-tiered security approach that includes industry best practices, Eaton ingenuity and the customer as a partner.
- Physical security
- Customer security
- Device communication security
- Network communication security
- Network segmentation security
- OTA update security
- COE assurance
Review the WaveLinx statement of security document for more information on each of these seven layers.

3. **Why is physical security so important?**
Physical security is a partnership between Eaton and its customers. The WaveLinx product includes multiple security measures in the devices. Physical access at the customer location is the first step. Physical access to a device may provide the ability for a potential attack.

4. **Does WaveLinx provide a path to my building intranet (LAN)?**
The WaveLinx Wireless Area Controller (WAC) is the only device that connects physically to the building intranet. In addition to other security measures the WAC isolates the wired Ethernet network from the wireless network which limits the possibility of someone using the WaveLinx system to gain business confidential information.

5. **Why AES 128-bit encryption, why not AES 256-bit?**
WaveLinx uses AES 128-bit encryption for device-to-device communications as recommended by the National Institute of Standard and Technology (NIST) and The Eaton Product Cybersecurity Center of Excellence (PCCoE). AES encryption comes in three standard key sizes (128, 192 and 256 bits). Many people think because there are three sizes AES 256-bit must be better. In fact there were three keys sizes because it was developed for US Military/Government communications which requires three security levels.

AES 128-bit encryption uses a 128-bit key to encrypt the data. That is $3.4 \times 10^{38}$ possible combinations if someone wanted to brute force guess your encryption key. Assuming you were able to guess the correct key 50% of the way through the combinations it would still take over 1 billion years.
6. **Can someone send a command or take over one of the WaveLinx devices?**
No, All WaveLinx devices use AES 128-bit encryption and also require that the commands be sent only to and from the WaveLinx Wireless Area Controller (WAC).

7. **Is the WaveLinx mobile application secure?**
Yes, WaveLinx mobile use HTTPS (TLS1.2) protocols to authenticate communications between the Wireless Area Controller and the mobile device. This inhibits other mobile applications or software from sending commands to the WaveLinx system.

8. **If someone were to hack into my Wireless Area Controller can they see the rest of my system or my building intranet (LAN)?**
No, each Wireless Area Controller employs its own unique key, which limits potential breaches to only a small area. Also the WAC provides segmentation between the lighting Operational Technology (OT) network and the enterprise Information Technology (IT) network. Even if an attack within the lighting (OT) network and its devices is successful, the WAC isolates the enterprise IT network from potential attack.

9. **How do I keep mobile devices from accessing the WaveLinx system?**
Each mobile device must have three things to access the WaveLinx system.

1. First, they must be able to physically log onto the building WiFi in order to access the Wireless Area Controller. This requires that they know the WiFi SSID and have the WPA2 password, provided by your building IT team.
2. Second, they must have installed the WaveLinx mobile application which is available via the Apple and Google stores.
3. Third, they must have the unique Wireless Area Controller login username and passwords in order to access the WaveLinx system.

The key component to keeping unauthorized mobile devices from accessing the WaveLinx system is physical access and customer network authentication policies.

10. **Are firmware updates secure?**
Yes, Eaton firmware updates are digitally signed which means that only our over the air (OTA) firmware updates will be accepted by each device.

11. **If there is a security issue in the future how will we know?**
The Eaton Product Cybersecurity Center of Excellence (PCCoE) maintains a publically available website for information and feedback concerning cybersecurity threats and responses. The PCCoE also independently evaluates Eaton IoT products for vulnerabilities as new cybersecurity threats are exposed.