Inner Range Cybersecurity Statement – November 2020

Cybersecurity is one of the most significant issues facing organisations today. Networked Security and Access Control systems are a potential point of vulnerability and thus these systems must be designed and installed to provide customers with the safest possible solution. Inner Range deploy a range of technologies and processes to ensure the products we develop and maintain are secure from both physical security and cybersecurity vulnerabilities. In its thirty-year history, Inner Range products have not had a single reported cybersecurity breach.

In 2019 Inner Range engaged the services of a one of the world's top 5 software consulting companies to undertake a cybersecurity governance audit of the company. Inner Range is continuously evolving its cybersecurity efforts to ensure our products, systems and processes keep up with the rapidly evolving nature of cyber threats.

There are a number of key areas that form the foundation of Inner Range's Cybersecurity Defences. These include:
A Cross Functional Cybersecurity Governance Team
- Penetration testing of all networked products by independent accredited laboratories
- A Product Development Process that includes cyber threat assessment
- Deployment of hardened cybersecurity technologies
- Supply of cyber hardening installation guidelines for Inner Range products

Cross Functional Cybersecurity Governance Committee
Inner Range's cross functional cybersecurity governance committee has senior management representatives from R&D, Production, Technical Support and IT and the company's Executive leadership. This committee manages Inner Range's policies and procedures relating to cybersecurity, reviewing, and updating them to meet new challenges in the evolving threat landscape, and ensuring that the organisation is following them successfully.

Penetration testing of networked products by independent accredited laboratories
Inner Range utilises the services of independent accredited laboratories to assess the security and probe for vulnerabilities of its products using a wide range of tools and techniques. Penetration testing has been applied to Inner Range's IP network-connected products, including Integriti, Inception, Multipath and SkyCommand. The results of these tests directly improve the security of our platforms and are incorporated back into the development processes so that future products maintain that high standard.

A Product Development Process that includes cyber threat assessment
For over 15 years Inner Range has been ISO 9001 certified which ensures all its processes, including R&D are undertaken in a controlled manner. The Inner Range Product Development process includes cyber threat assessment at each stage of the product development process. No IP network enabled product can pass through the product development process without going through the independent penetration testing described above. Additionally, strict access control

permissions are allocated to source code to ensure only relevant staff have access to code repositories.

Supply of cyber hardening installation guidelines for Inner Range products

In order to deploy an Inner Range system safely, it must be deployed within a secure network environment. Inner Range's installation hardening guides provide advice for system integrators relating to security mechanisms that can be implemented within their systems and environments. This includes recommendations around security, network access control, firewalls, identity management, vulnerability management, etc.

Deployment of hardened cybersecurity technologies

Inner Range's cloud services such as Multipath and SkyCommand are hosted in an industry leading cloud hosting environment which has multiple Certifications from ISO/IEC, CSA, ITAR, CJIS, HPIAA and IRS 1075. These systems are optimised for cloud deployment and offer redundancy and load balancing across multiple locations.

Inner Range's devices utilise cryptographic implementations including AES encryption that are certified by NIST through their Cryptographic Algorithm Verification Program to the FIPS 140-2 standard. The cloud services, servers, web clients, and mobile apps are secured with HTTPS / TLS and the MS SQL database can support TLS and TDE which uses AES 256-bit encryption

Inner Range's Architecture is specifically designed to minimise the attack surface area available to potential Bad Actors. This includes dedicated local LAN networks that are extremely resilient against all known forms of cybersecurity attack and, where appropriate, utilize lightweight real time operating systems that greatly reduce exposure to the many vulnerabilities associated with desktop operating systems.