INFOBRIEF

Security policy framework

Ciena is driven by a relentless pursuit of network innovation, enabling our customers to adapt within ever-changing environments to deliver richer and more connected experiences for their business and users. A key driver of those ever-changing environments includes a continually evolving landscape of cyber threats. Ciena's security program is aligned to industry standards and frameworks such as ISO 27001, the National Institute of Standards and Technology (NIST), Cybersecurity Framework (CSF), National Security Agency "Defense in Depth" strategies, the Secure Controls Framework, the Unified Control Framework, the confidentiality, integrity, and availability (CIA) triad security model, and others. Ciena focuses its security program on these industry standards and the following framework that underpins the program:

- Diligence: Protect the company from evolving threats
- Integrity: Do the right things, and do them well
- Transparency: Build trust in our products and program
- Teamwork: Proactive relationships with our customers and suppliers

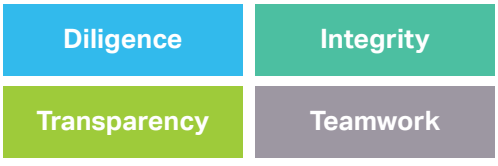

Figure 1. Standards of Ciena's security program

Ciena strives to ensure we have assembled a comprehensive security program so our customers can focus on their business objectives Ciena continues to enhance our global trust and security teams and programs based on industry standards and frameworks.

Ciena maintains a robust corporate policy program in alignment with International Organization of Standardization (ISO) standards and requirements. Based principally on the CIA triad security model, our security program is focused on protecting Ciena and Ciena customer data (where applicable) while still ensuring information is accurate and readily available. Additionally, our policy program is aligned to various industry standards such as the NIST CSF, ISO, AICPA & CIMA System and Organization Controls, the U.S. Sarbanes-Oxley Act, and others, and consists of policies, standards, guidelines, and procedures that meet these industry requirements and cover the following domains:

- Acceptable use policies
- Asset management
- Business continuity and disaster recovery
- Capacity and performance planning
- Change management
- Cloud security
- Compliance
- Configuration management

- Continuous monitoring
- Cryptographic protections
- Cybersecurity and data protection governance
- Data classification and handling
- Data privacy
- Endpoint security
- Human resources security
- Identification and authentication
- Incident response
- Information assurance
- Maintenance
- Mobile device management
- Network security
- Physical and environmental security
- Project and resource management
- Risk management
- Secure engineering and architecture
- Security operations
- Security awareness and training
- Supply chain security
- Technology development and acquisition
- Third-party management
- Threat management
- Vulnerability and patch management
- Web security

Ciena also ensures we have corresponding standards and operating procedures, where appropriate, that align to the above policy domains. Each of these policies, standards, guidelines, and procedures are built to ensure our systems and data—and customer data we are entrusted with—are protected. Our governing documents are reviewed at a minimum annually and updated as necessary.

Ciena is advancing its security program by developing an internal Unified Control Framework, primarily using the Secure Controls Framework. This framework allows Ciena to build, track, and continually govern its systems and processes with direct alignment and mapping to many industry standards, legal and regulatory requirements, frameworks, and other control environments, including the NIST CSF and ISO 27001.