VIAVI Solutions

VIAVI Solutions
Security Posture

VIAVI's Commitment to Security in a Connected World

Version 1.0 | 2026-05-05

VIAVI Solutions

VIAVI's Commitment to Security in a Connected World

Network performance, test, and monitoring infrastructure sits at the heart of some of the world's most critical communications networks. The products VIAVI delivers are used by carriers, enterprises, and defense organizations to observe, diagnose, and assure the networks that billions of people depend on every day. That position carries responsibility.

VIAVI is committed to building and maintaining products that are secure by design, operated with integrity, and supported with transparency when vulnerabilities arise. Our security program spans the entire product lifecycle — from secure development practices and third-party component management, through post-shipment monitoring and vulnerability response.

> *Security is not a feature we add to products. It is a discipline embedded in how we design, build, test, and support everything we ship.*

From an operational perspective, VIAVI is committed to conducting business with integrity. We have programs, policies and procedures designed to:

- Protect the security and privacy of our customers' network data and environments
- Build products that reduce the attack surface of the networks they monitor
- Respond promptly and transparently when vulnerabilities are identified
- Meet applicable security compliance requirements across the markets we serve
- Continuously improve our security posture as threats evolve

Secure SDLC	**CVSS 3.1**	**Coordinated Disclosure**	**Supply Chain Security**
Security at every phase	Industry-standard scoring	Responsible disclosure	Component Integrity

VIAVI Solutions

Product and Solution Security

VIAVI's Product Security program is focused on the cybersecurity of the products and solutions we deliver to customers. Our approach is built on three principles: secure by design, continuously monitored, and transparently maintained.

Secure Development Lifecycle

VIAVI embeds security requirements throughout the product development lifecycle. Security is a continuous activity from initial design through general availability and ongoing maintenance — not a gate applied at the end of development.

Definition phase

- Security requirements defined per product considering legal and regulatory requirements
- Threat modelling conducted by product team
- Third-party component inventory established

Development phase

- Secure coding standards and peer code review applied
- Software composition analysis on all dependencies
- Automated CVE scanning in CI/CD pipeline

Testing phase

- Device hardening testing and verification
- Composition analysis scan and remediation
- Vulnerability assessment and remediation

Monitoring phase

- Continuous post-shipment vulnerability scanning
- Industry advisory monitoring for all shipped components
- Customer vulnerability intake and response

Secure Hardening

VIAVI products are delivered with hardened configurations. Default settings are reviewed and locked down prior to shipment, guided by industry standards including CIS hardening benchmarks and DISA STIGs where applicable. Hardening controls include:

- Closure of unused ports and disabling of unnecessary services
- Removal of default credentials and enforcement of strong authentication
- Principle of least privilege applied to all product access controls
- Encrypted communications using current best-practice protocols and cipher suites
- Secure default configurations that do not require customer intervention to be safe

VIAVI Solutions

Software Composition Analysis

VIAVI uses industry-recognized commercial tooling to perform software composition analysis on all software shipped to customers. This enables product teams to identify, track, and mitigate known vulnerabilities in third-party and open-source components throughout the product lifecycle — not only at release, but on an ongoing basis after shipment.

Cryptography

Sensitive data — including credentials, API keys, and cryptographic material — is encrypted at rest and in transit. VIAVI products use current best-practice encryption protocols and algorithm strengths. Secrets are managed through dedicated vaulting solutions and are never stored in source code or configuration files accessible to end users.

VIAVI Solutions

Vulnerability Management

VIAVI maintains a structured vulnerability management program spanning detection, assessment, remediation, and disclosure. Our program ensures that vulnerabilities in VIAVI products are identified promptly, assessed accurately, and addressed in a manner consistent with the risk they represent to our customers.

Detection and Monitoring

VIAVI continuously monitors for new vulnerabilities affecting shipped products through multiple channels:

- Active monitoring of public CVE databases and security advisory sources
- Vulnerability notifications for third-party components in shipped products
- Customer and security researcher vulnerability reports
- Internal SAST and DAST security testing and post-shipment scanning programs

Assessment

All detected vulnerabilities are assessed using CVSS 3.1 as the primary severity measure. VIAVI combines the CVSS base score with a contextual risk assessment that accounts for specific deployment environments — including network exposure, access controls in place, and the criticality of the affected functionality.

Remediation

VIAVI's remediation program prioritizes vulnerabilities based on assessed severity and real-world exploitability. Patches, mitigations, and workarounds are delivered through VIAVI's standard software update mechanisms. Release notes for all updates include security fix details, including CVE identifiers and CVSS scores where applicable.

Incident and Vulnerability Reporting

Customers, security researchers, and partners can report suspected vulnerabilities in VIAVI products by contacting the VIAVI support team directly. VIAVI is committed to acknowledging all reports and working collaboratively with reporters through the investigation and remediation process.

VIAVI Solutions

Information Security Program

VIAVI's enterprise information security program protects the confidentiality, integrity, and availability of VIAVI's systems and the customer data entrusted to us. The program is risk-based, grounded in industry frameworks, and continuously assessed through independent testing and review.

Security Governance

VIAVI's information security function reports to senior leadership and encompasses policy management, risk management, vulnerability management, identity and access management, incident response, security awareness, and compliance assurance. Security policies are reviewed at least annually.

Risk Management

VIAVI's risk management program is used to assess, document, monitor, and report security risks across the enterprise. Risk exposure, avoidance, mitigation, and acceptance decisions are documented and reviewed on a regular cycle. Independent third-party assessments — including penetration testing and compliance audits — validate the effectiveness of controls.

Identity and Access Management

Access to VIAVI systems is governed by the principle of least privilege. Multi-factor authentication is enforced for access to corporate systems. Access rights are provisioned through controlled processes and reviewed and revoked promptly when no longer required.

Security Operations

VIAVI maintains security monitoring capabilities for detection and response to security events across the enterprise. Incident response plans define roles, responsibilities, and communication protocols for responding to incidents, including the notification of affected customers where applicable.

Data Protection

VIAVI's data protection program is aligned with applicable privacy and data protection regulations including the EU General Data Protection Regulation (GDPR). Encryption is applied to sensitive data at rest and in transit. Data handling practices are documented and reviewed against evolving regulatory requirements.

VIAVI Solutions

Standards and Certifications

VIAVI's security program is aligned with recognized industry standards and subject to independent validation. Our approach to product security and information security is designed to meet the requirements of the markets and customers we serve, including regulated and government environments.

ISO 27001 Information Security Management	**CVE / CNA** CVE Numbering Authority	**CVSS 3.1** Vulnerability Severity Scoring	**OWASP** Secure Development Practices
CIS Controls Product Hardening Guidance	**NIST SP 800-218** Secure Software Dev. Framework	**EU CRA** Cyber Resilience Act	**GDPR** Data Protection Regulation

VIAVI also monitors and supports compliance with applicable regulatory requirements relevant to our customers' operating environments, including:

- EU Cyber Resilience Act (CRA) — for products sold in European markets
- GDPR — for products and services handling personal data of EU individuals

VIAVI Solutions

Additional Resources

Report a product security issue
Viavi Support Portal

VIAVI Privacy and Data Protection
www.viavisolutions.com/privacy

VIAVI Product Vulnerability Practices
Available from your VIAVI account team

General Security Inquiries
Contact your VIAVI account team

VIAVI enables network operators, enterprises, and defense customers to observe, diagnose, and assure the networks that the modern world depends on.

www.viavisolutions.com