GE VERNOVA

FACTSHEET

GE Vernova's Cybersecurity Solution – OTArmor

CYBER SOLUTION COMPLIANCE

OVERVIEW

GE Vernova's support for regulations and standards – a trusted partner for compliance
As a manufacturer of industrial controls, GE Vernova embraces its responsibilities to assist critical infrastructure owners to improve their security postures and support adherence to industry standards.

GE Vernova aligns to multiple best practices frameworks and standards, and helps customers meet regulations such as NERC CIP and NEI 08-09.

In addition to regulations, our team is well versed in supporting common architecture frameworks and standards such as the NIST 800 series, CIS Controls, and ISO 27002. Our extensive experience can also help those organizations who are working toward developing and meeting internal standards.

NIST 800-82 GUIDE TO INDUSTRIAL CONTROL SYSTEMS

The NIST 800 series of special publications addresses process, organizational and technical aspects required to implement a full life-cycle cybersecurity management program. NIST 800-82 is one of the few non-vendor funded publications that specifically addresses Industrial Control System Security. GE Vernova's security governance services can help organizations develop and implement full life-cycle frameworks that consist of customer-specific requirements, international standards, and GE's own critical infrastructure and process control cybersecurity best practices.

IEC 62443-2-4
IEC 62443-2-4 is a published international standard, defining cybersecurity capabilities that Industrial Automation and Control System (IACS) service providers may implement and offer. The standard was developed by IEC Technical Committee 65, in collaboration with the International Instrumentation Users Association (previously WIB) and ISA 99 committee members. The table below represents GE Vernova's alignment to specific requirements of this standard.

Solution Staffing	Network Security	User Security	Application Security	Security Information & Events Management (SIEM)	Patch Management
◐	● ◐ ○	● ◐	●	●	● ○

● OTArmor　◐ Services　○ Patch Validation Program

NERC CIP REV 5 & 6

Many U.S. electric utilities are now federally mandated to comply with NERC CIP requirements that dictate industrial security and remediation technology. To be considered in adapting operations to these regulations is the difficulty of patching industrial controls and the frequent attacks on the equipment. In addition, customers need to address known ICS vulnerabilities without disrupting operations. Because of these factors, electric utilities require a solution that is easy to implement and provides visibility into the industrial network and compliance. The table below represents GE Vernova's alignment to specific requirements of this regulation.

CIP-002 Asset Identification and Classification	CIP-003-6 Policy and Governance	CIP-004-6 Personnel & Training	CIP-005 Network Security	CIP-006-6 Physical Security of Cyber Assets	CIP-007-6 System Security Controls	CIP-008 Cybersecurity Incident Response	CIP-009-6 Recovery Plans for BES Cyber Systems	CIP-010-3 Change and Vulnerability Management	CIP-011-2 Protection of BES Cyber System Information
●	● ◐	◐	●	●	● ○	● ◐	● ◐	● ○ ◐	●

● OTArmor ◐ Services ○ Patch Validation Program

NEI 08-09

GE Vernova supports nuclear compliance efforts for NEI 08-09 by providing baseline configuration documentation for current and certain legacy controls, and by supporting asset operator cyber vulnerability assessments and associated mitigations. The table below represents GE Vernova's alignment to specific requirements of this regulation.

Access Controls	Audit & Accountability	Critical Digital Assets, System, and Communications Protection	Identification & Authentication	System Hardening	Contingency Planning
●	● ○	●	● ○	●	● ○

● OT Armor ○ Patch Validation Program

CIS (CENTER FOR INTERNET SECURITY) CONTROLS

OTArmor assists customers with managing their plant's HMI cybersecurity by implementing 16 of the 18 CIS Controls, and 60% of the sub-controls for that standard. Applying the CIS Controls supports owner compliance towards cyber security regulations, standards and guidelines, such as NEI 08-09, NERC CIP, WIB, ISA 99, NIST SP 800-82 and NIST SP 800-53. OTArmor provides support for all CIS Controls excluding 15 (Service Provider Management) and 17 (Incident Response Management) by using advanced technology, which reduces the amount of labor to support the system. The specific mapping of CIS Controls to OTArmor Components are listed below for controls covered by OTArmor + Patch Validation program.

OTArmor Component	CIS Controls
Appliance	N/A
Patch Validation Program	2,7,14,16,18
System Hardening	2,4,9,10,16
Anti-malware	10
User Security Policies	3,4,5,6
User Policy Governance	4,5,6
Backup and Recovery	3,11
Log Aggregation	1,3,8,13,16
Network Device Management	3,4,12

NOTE: The above table and figures are representative of how OTArmor provides features that enable end users to meet regulatory compliance standards. It is the responsibility of the end user to reach compliance, and as a supplier of cybersecurity solution, GE Vernova will support the end users.

GE VERNOVA

gevernova.com

Information contained in this document is indicative. No representation or warranty is given or should be relied on. Information provided is subject to change without notice.