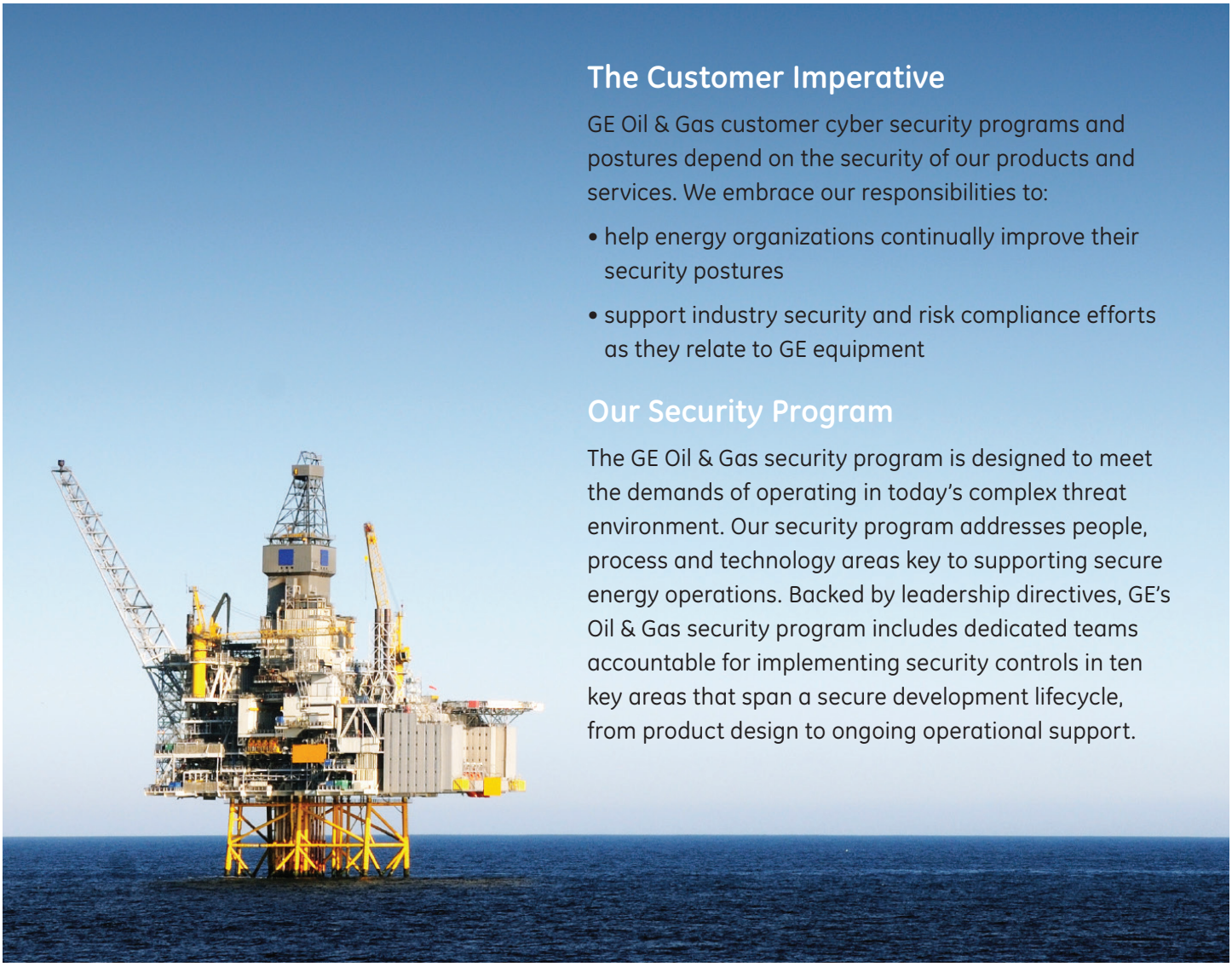
GE Oil & Gas

Cyber Security **OVERVIEW**

The industrial world is becoming more digitally connected, making operations smarter and more productive. But with that connectivity comes vulnerability. GE is committed to a culture of security to protect our systems, products, and customer operations.

This document highlights the key tenets of our GE Oil & Gas security program. We strive to support our customers' efforts to secure energy operations, and we embrace Oil & Gas industry efforts toward achieving cyber security excellence. As energy producers further expand connectivity amidst the Industrial Internet era, we continue to evolve and strengthen our security efforts.



The Customer Imperative

GE Oil & Gas customer cyber security programs and postures depend on the security of our products and services. We embrace our responsibilities to:

- help energy organizations continually improve their security postures
- support industry security and risk compliance efforts as they relate to GE equipment

Our Security Program

The GE Oil & Gas security program is designed to meet the demands of operating in today's complex threat environment. Our security program addresses people, process and technology areas key to supporting secure energy operations. Backed by leadership directives, GE's Oil & Gas security program includes dedicated teams accountable for implementing security controls in ten key areas that span a secure development lifecycle, from product design to ongoing operational support.

GE Oil & Gas

GE Oil & Gas Partnering with Industry

GE Oil & Gas serves as a trusted partner to energy-related operators actively working to improve their security posture.

From reference architecture co-development, operational security requirement input, ongoing lifecycle security maintenance, and solution co-development, we are privileged to support the security efforts of some of the world's leading energy companies. These close security partnerships and collaboration with customers enable GE Oil & Gas to reduce risk in digital and industrial environments.

Our People

GE's commitment to security begins and ends with our employees. This effort begins at the top with comprehensive cyber security policies regularly communicated throughout our organization. We have dedicated teams committed to IT, industrial, and product security. These organizations work together to drive cyber security best practices.

Our employees participate in regular security awareness training and are kept informed of emerging threats/best practices through cyber security relevant alerts. In addition, employees are expected to adhere to our cyber security practices when it applies to intellectual property and company information. We believe security is a team effort and all employees must be prepared to report and respond to issues quickly.

Industry Engagement

Through partnerships with industry leaders, customers, employees, suppliers and contractors, we are able to support major industry initiatives, such as Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC). We are dedicated to on-going ongoing security engagements through our GE Charter Technology customer relationships worldwide. Our security experts readily share and train industry constituents on current topics through GE and third party symposia. These shared insights and experiences will continue to improve our solutions and processes. As industry standards and customer needs change, we will continually adapt our security methods to help protect customers from risk.

Adherence to Global Security Standards

GE Oil & Gas understands the importance of leveraging and integrating industry cyber security practices that have been developed by organizations such as the National Institute of Standards and Technology (NIST) and the International Standardization Organization (ISO). Specifically, the

GE Oil & Gas

internationally recognized frameworks we have chosen to adopt include:

- ISA-99 (Industrial Automation & Control Systems Security)
- ISA/IEC 62443-4-1/2 (Industrial Network & System Security)
- WIB M-2784 (Process Control Domain – Security Requirements for Vendors)
- NIST 800-82 (Guide to Industrial Control Systems)
- ISO 27002 (Enterprise Cyber Security)

GE Oil & Gas standards compliance efforts provide our customers with greater visibility into our secure environments, while offering concrete guidelines to improving operational resilience.

Our Processes

GE Oil & Gas has adopted international security standards related to our infrastructure, as well as processes that impact its resilience. Where applicable, GE Oil & Gas seeks and obtains independent certifications aligned to internationally recognized security standards.

From product development through delivery and maintenance, our policies and procedures address security throughout an energy operation's lifecycle. Adoption of secure development lifecycle processes support the implementation of critical security controls for the delivery of both products and services.

A dedicated GE Oil & Gas team maintains relationships with key operating system, network device, and application vendors to closely track security issues, software updates, and newly released patches – with the intent to alert product users when needed. Newly available patches, malware detection signatures and anti-virus are evaluated and tested for applicability to the system.

GE Oil & Gas

Our Technology

GE Oil & Gas equipment is engineered with security in mind. Our product development lifecycle includes product assessments (both internal and third party testing) and security design reviews as a regular practice within our development process. Updated tools and methods in both IT and OT security are applied throughout the product life-cycle to reduce risk and address vulnerabilities.

Customer Role in Security Partnership

We recognize that solid business relationships are fundamental to the success of our security programs. In the case of an incident, our product security response team (PSIRT) evaluates, takes actions and handles communication related to the vulnerability or incident.

If a threat is detected, we will implement corrective action as appropriate. We encourage our customers to report suspicions and events pertaining to security or other irregular business matters to security@ge.com. Additionally, our public website for security reporting can be found at: ge.com/security

Summary

We recognize the high level of trust customers expect from GE Oil & Gas solutions and the integral role our products play in secure customer operations. We have instituted a comprehensive security program to proactively mitigate risks. Based on industry standards, our security program engages GE Oil & Gas people, process and technology, to support customer efforts to secure operations. Our solutions and processes evolve as industry standards and customer needs change. Through collaborative partnerships with customers, employees, suppliers, contractors and industry leaders.

GE Oil & Gas embraces its role in helping make the energy industry more resilient to cyber threats.

GE Oil & Gas
4424 W. Sam Houston Parkway,
Suite 910-E
Houston, TX 77041
T +1 713 458 3731
ge.com

GEOGPS_SP_0116