U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Supply Chain Cybersecurity Principles

The Supply Chain Cybersecurity Principles characterize the foundational actions and approaches needed to deliver strong cybersecurity throughout the vast global supply chains that build energy automation and industrial control systems (ICS). The principles aim to create an enduring framework to drive best practices today, while informing international coordination to advance those practices into the future.

The Need for Supply Chain Principles

Energy ICS are inherently complex and securing them is even more so. A single product or system may contain hundreds of subcomponents sourced from suppliers and manufacturers across the globe; that technology may then be further integrated into a complex system before it reaches the end user.

This creates a dense web of stakeholders that all play a role in the security and resilience of the resulting energy infrastructure. Security is inevitably a shared responsibility among the engineers, manufacturers, integrators, service providers, and system operators along a complex, global supply chain.

The Supply Chain Cybersecurity Principles are explicitly written to address points where both supplier and end-user actions are necessary to achieve the desired security outcomes. Virtually all frameworks and standards are written from the perspective of a single entity, be that a supplier or an end user. Our principles capture the mirror-image of responsibilities between both the supplier and user relationship—including relationships between manufacturers and their upstream suppliers.

This effort is particularly important in light of increasing cyber threats to operational technology systems in the energy sector from nation-states and criminal actors.

A Call to Action

The principles draw from national and international cybersecurity regulations, requirements, frameworks, guidelines, and standards, both regulatory and voluntary. They condense the universe of guidance into concise, high-level objectives that we can use to align best practices and identify opportunities to collaboratively accelerate advancements in supply chain cybersecurity.

In developing these principles, the United States is issuing a collective call to action for ICS suppliers and end users across the globe to support and adopt the principles. The principles characterize the best practices that are exhibited today by cybersecurity leaders in the energy industry, and can help to create shared expectations that ripple throughout the supply chain, informing and lifting up manufacturers and owners and operators with less mature supply chain risk management efforts.

How the Principles Were Developed

The U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) developed the principles with input from leading ICS manufacturers and asset owners who participate in CESER's supply chain research and development, and drawing from research and insights at Idaho National Laboratory.

We are launching an effort with our international government and industry partners to align the principles to existing requirements, develop guidance for interpreting and adopting the principles, and identify gaps where international coordination could advance supply chain security throughout the global energy sector.

Supply Chain Cybersecurity Principles for Suppliers

Impact-Driven Risk Management
Embed consideration of impacts, specifically including those in your own upstream supply chains, throughout the entire systems engineering lifecycle, seeking to manage risks to functions that are aided by digital technologies.

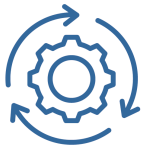
Framework-Informed Defenses
Incorporate appropriate principles and practices from recognized cybersecurity frameworks into the design of your organization's defenses of its critical functions, infrastructure, and information.

Cybersecurity Fundamentals
Follow relevant domain-specific regulations and international standards, and consider secure and cyber-informed engineering and design principles, to produce products and deliver services with appropriate security features and controls.

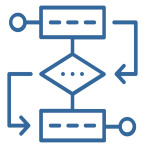
Secure Development & Implementation
Use a secure systems development lifecycle process informed by internationally accepted frameworks and standards to encourage adequate security practices throughout an offering's lifecycle.

Transparency & Trust Building
Provide appropriate information to your end users and the public regarding your cybersecurity posture, interoperability, product security, testing methods, independent verifications, and software and hardware composition of your products.

Implementation Guidance
Provide hardening and secure implementation guidance to end users, including transparent information on default settings and behaviors that must be changed or managed in implementation.

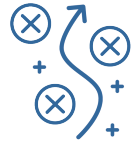


Lifecycle Support & Management
Provide appropriate product support, including security patches and mitigations, from transaction through the announced end of lifecycle support.



Proactive Vulnerability Management
Maintain a vulnerability management process—aligned to industry best practices and applicable coordinated vulnerability disclosure processes—for the responsible handling and coordinated disclosure of vulnerabilities.

Proactive Incident Response
Develop and maintain appropriate incident response plans for incidents within your own environments and when supporting end users in responding to incidents involving your products or services.



Business & Operational Resilience
Continually improve your organization's practices and offerings by identifying and implementing adaptations informed by observations, insights, and lessons learned from ongoing operations, end-user experiences, and incident response.

Supply Chain Cybersecurity Principles for End Users

Impact-Driven Risk Management
Embed consideration of impacts, specifically including those in your own upstream supply chains, throughout the entire systems engineering lifecycle, seeking to manage risks to functions that are aided by digital technologies.

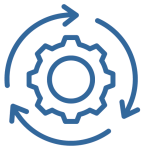
Framework-Informed Defenses
Incorporate appropriate principles and practices from recognized cybersecurity frameworks into the design of your organization's defenses of its critical functions, infrastructure, and information.

Cybersecurity Fundamentals
Follow relevant domain-specific regulations and international standards, and consider secure and cyber-informed engineering and design principles, to employ products and services in a secure manner, taking into account accumulated technical and security debt.

Secure Development & Implementation
Engage with suppliers to understand the security features and controls of their offering to ensure they are adequate for your intended purpose or identify necessary compensating controls.

Transparency & Trust Building
Include contractual language for those terms, conditions, and testing requirements that will influence your security outcomes, and which you are able and willing to enforce.

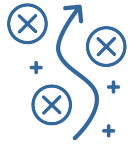
Implementation Guidance
Develop and maintain appropriately secure operating environments, following suppliers' hardening and secure implementation guidance.



Lifecycle Support & Management
Conduct business planning and provide resources to acquire, maintain (including patch management and fixes recommended by the supplier), and replace equipment through its lifecycle, considering continued availability of supplier technical support.

Proactive Vulnerability Management
Maintain a risk-informed vulnerability management process that aligns with the supplier's published process for responsible disclosure of vulnerabilities discovered through use of their products.

Proactive Incident Response
Proactively coordinate supplier support during response to incidents involving their products or services.



Business & Operational Resilience
Continually improve your organization and its practices by adaptation from observations, insights, and lessons learned from ongoing operations, supplier experiences, and incident response.