Energy Cyber Sense (ECS)

Cyber Testing for Resilient Industrial Control Systems (CyTRICS™)

Energy Cyber Sense Program Portfolio

Mission Statement: **Implement a national capability for enhancing the cyber security and resilience of critical U.S. energy infrastructure by advancing the state of practice for supply chain risk management.**

CyTRICS -

Cyber Testing for Resilient Industrial Control System

- Identify, prioritize, and test critical components in the supply chain
- Identify systemic risks in supply chain components
- Responsibly disclose threats and vulnerabilities
- Mitigate risks in partnerships with energy industry

Advancing Bills of Materials (BOMs)

- Develop and test advanced BOM development approaches
- Address key challenges that limit BOM development at scale
- Expand the BOM repository and enable systemic analysis

Cyber-Informed Engineering

- Helps engineers identify where the consequence of a successful attack could affect safety, reliability, and performance of systems and processes and develop specific engineering protections
- Uses engineering tools to best protect and defend important industrial processes

Supply Chain Cybersecurity Principles

- 10 principles—each tailored for suppliers and end users—established shared expectations for secure behaviors throughout system design and deployment
- Supported by prominent energy sector suppliers and manufacturers

Rapid Technology Supply Chain Risk Assessments

- Rapid Risk Assessments
- Apply a rapid risk assessment framework to identify supply chain risks introduced by foreign entities of concern (FEOCs)
- Prioritization risk mitigation approaches based on potential impact

Cyber Testing for Resilient Industrial Control Systems (CyTRICS™)

CyTRICS Illuminates Systemic Supply Chain Risk

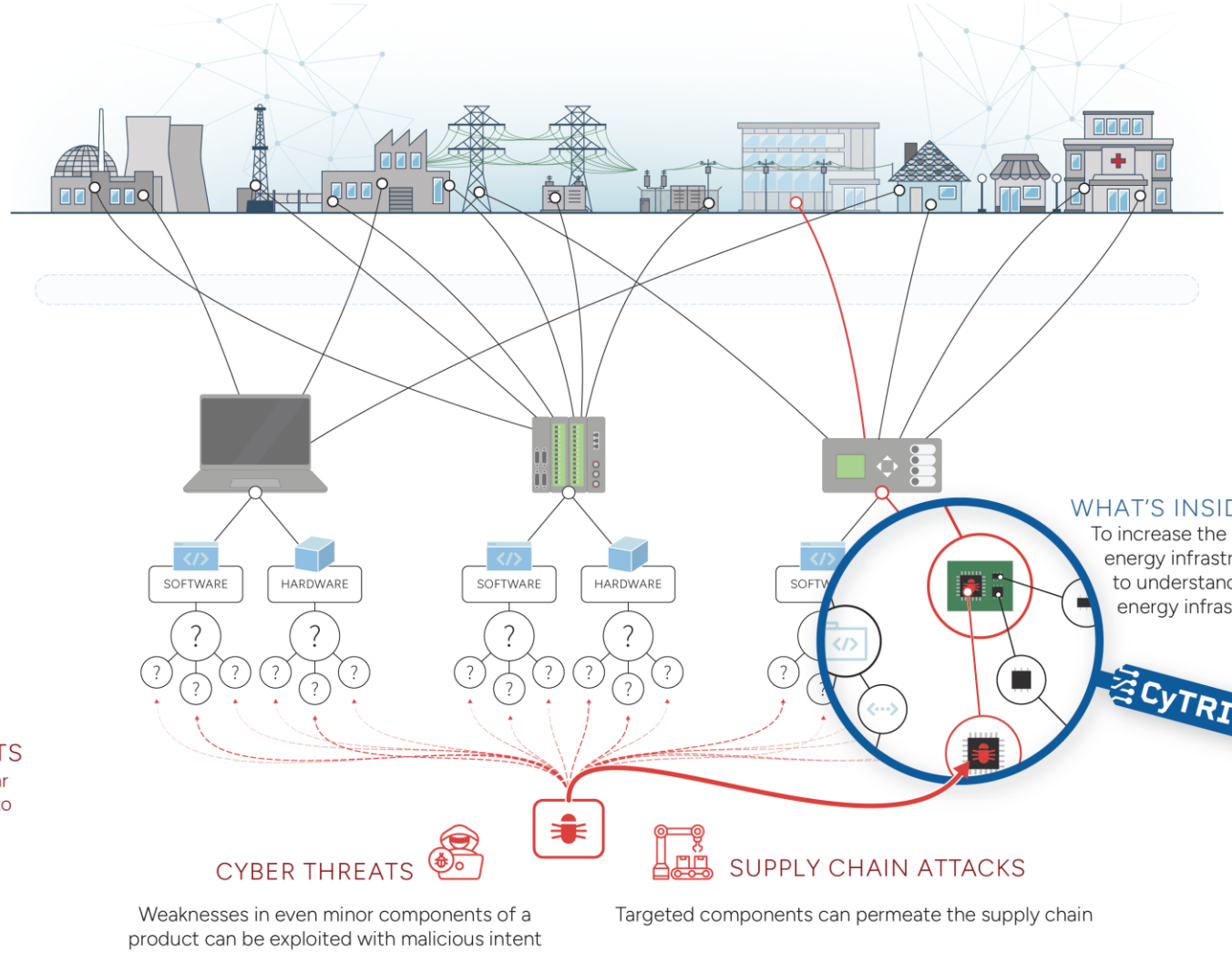
INFRASTRUCTURE
Facilities and services necessary to provide energy

SYSTEMS

PRODUCTS
Devices built and purchased by industry for energy infrastructure

COMPONENTS
Digital and electronic components are combined to create products

SHARED COMPONENTS
Create the potential for singular vulnerabilities to compound into system-wide risk



Idaho National Laboratory
Pacific Northwest NATIONAL LABORATORY
Lawrence Livermore National Laboratory
Sandia National Laboratories
OAK RIDGE National Laboratory
NREL Transforming ENERGY

Securing Energy Infrastructure

CyTRICS Delivers:

- System Analysis Report enables vendors to act on findings and release mitigations
- Tool development and validation streamlines CyTRICS testing/analysis and fills capability gaps in commercial tools
- Innovations in supply chain risk management that inform system design
- HBOM/SBOMs that build a strategic database that reflects the critical hardware/software/firmware of the electric grid
- Repository enables identification of systemic risks and threats and enhances understanding of the critical energy infrastructure

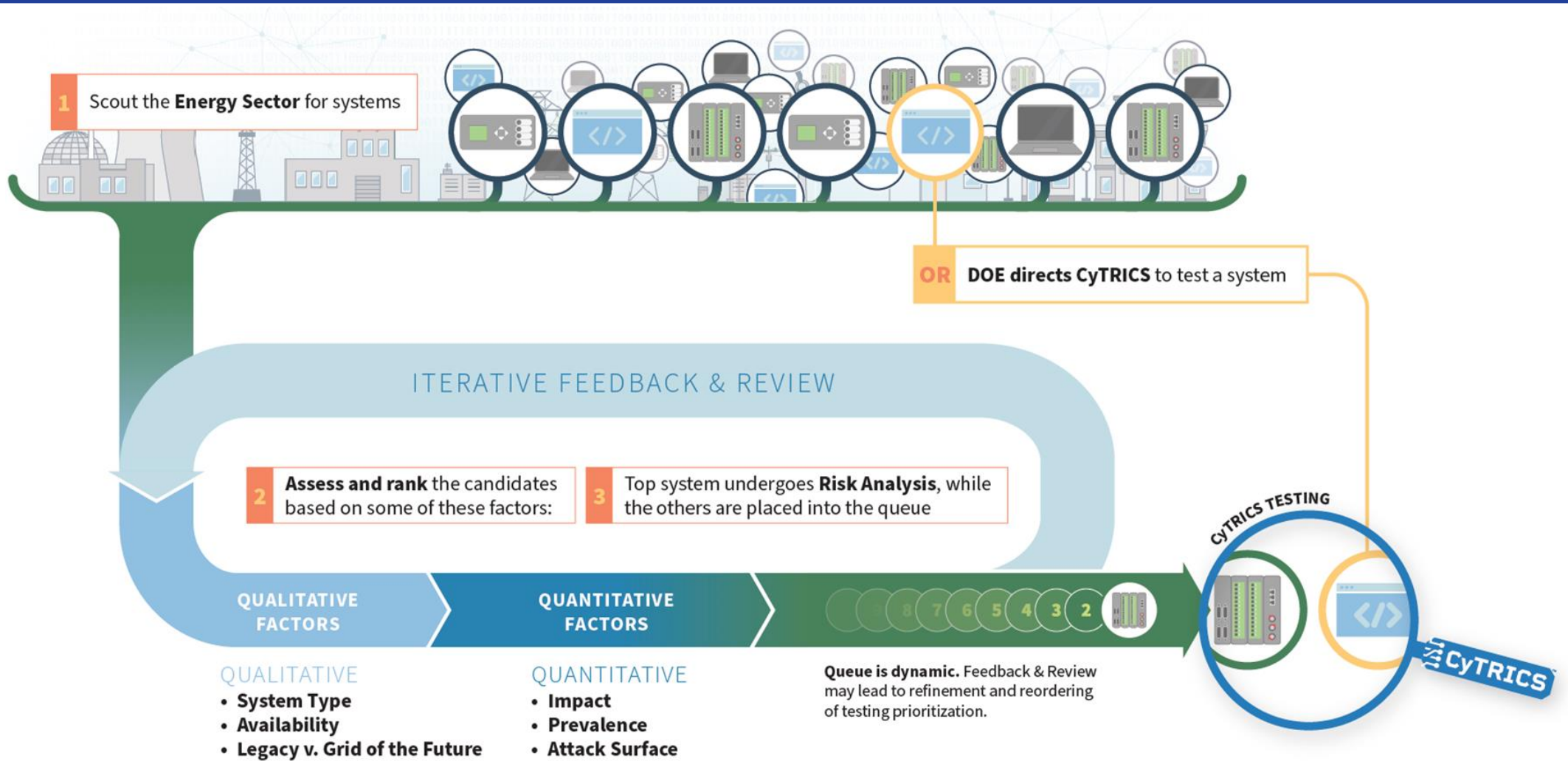
VENDOR PARTNERS

Schneider Electric
Hitachi Energy
SEL SCHWEITZER ENGINEERING LABORATORIES
GE VERNOVA
Rockwell Automation
Westinghouse

UTILITY PARTNERS

Multiple active partnerships

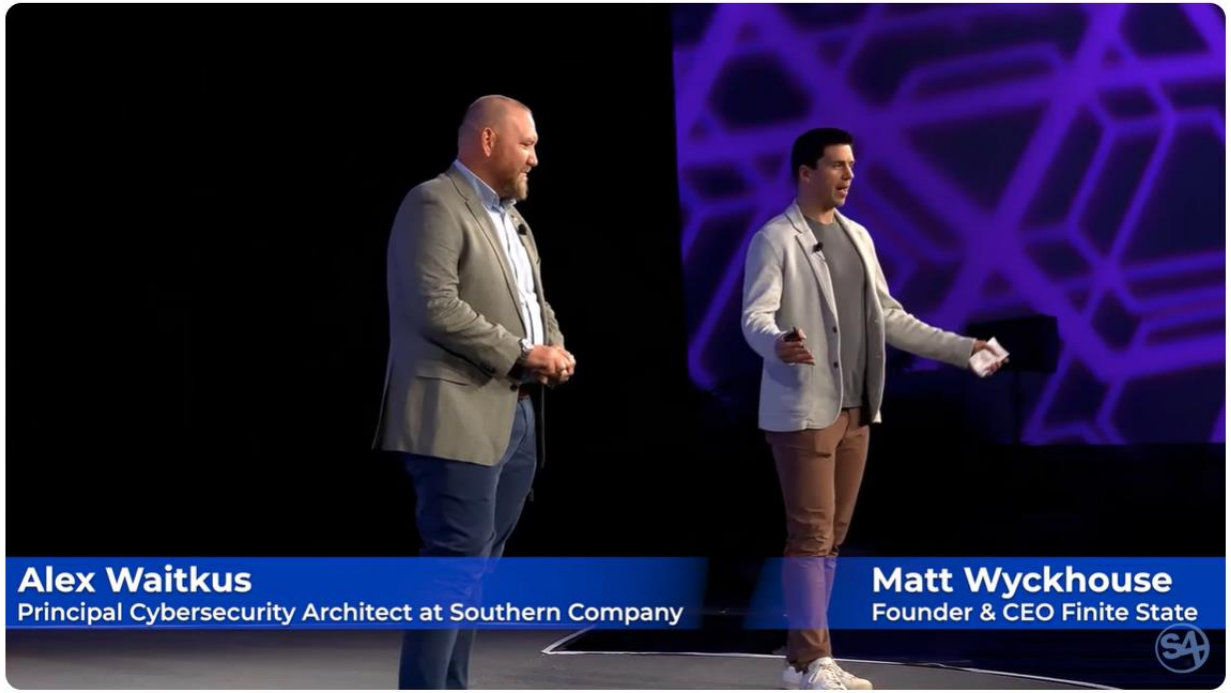
How Does CyTRICS Prioritize Systems for Testing?



Bills of Materials (BOM) Advancement

Industry Recognizes BOM Potential…and Gaps

- Southern Company's public experiment: Gather BOMs to define the supply chain for 1 substation
- Needed 38 device BOMs from 17 vendors—60% couldn't provide them
- Took 60 days and dozens of meetings to get BOMs in hand
- BOM validation testing revealed several out of date
- Only a handful of associated vulnerabilities were exploitable, out of hundreds or thousands of vulnerabilities associated with a BOM

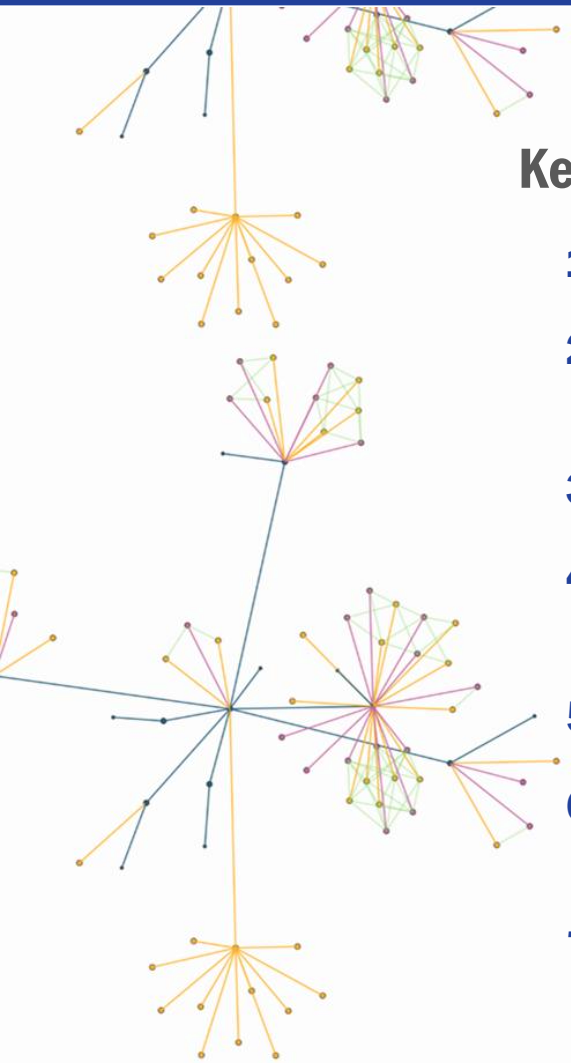


A SBOM'd Substation

S4 Events
7.62K subscribers
Subscribe
20
Share
Download

"SBOM sharing is clunky right now. If you're just collecting SBOMs and you can't do anything with the data, they are just JSON documents in a folder." – Matt Wyckhouse, Finite State

Energy Cyber Sense BOM Advancement - Project Sparkle

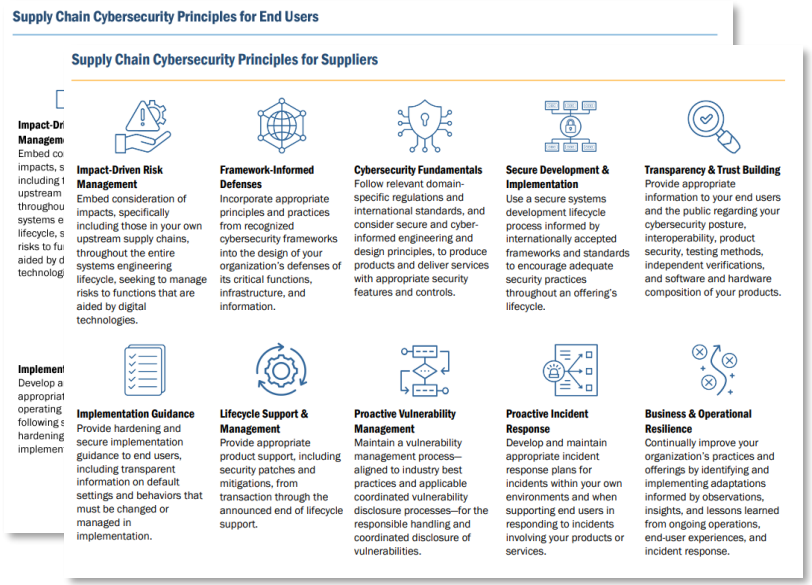


Key Challenges

1. **CVE correlation** – Associating a CVE with a product does not mean it's vulnerable.
2. **Effective sharing** – What should be shared between OEMs and asset owners, when, and how?
3. **Handling variability** – Do we focus on eliminating variability or accept it and normalize it?
4. **Quality and suitability of SBOMs** – Because SBOMs are intended to be exchanged, it is important to be able to measure their quality.
5. **Acknowledging SBOM types** – Which SBOM types are useful for vulnerability management?
6. **How should BOMs be mapped to products**– How does software map to consumer products and systems?
7. **Scaling BOMS** – What challenges arise when leveraging hundreds or thousands of BOMs at enterprise scale?

Supply Chain Cybersecurity Principles

Supply Chain Cybersecurity Principles


Supply Chain Cybersecurity Principles for End Users

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.

Partners Expressing Support:

GE VERNOVA · SEL Schweitzer Engineering Laboratories · Siemens Energy · Schneider Electric · Honeywell · Rockwell Automation · Siemens · Westinghouse · Hitachi Energy · INGAA

The Supply Chain Cybersecurity Principles establish expectations for the foundational actions and approaches needed to deliver secure global ICS supply chains.

Currently 10 double-sided principles explicitly address areas where both supplier and end-user actions are necessary to achieve security objectives.

NEXT STEPS (FY26):

1. **Partner Engagement**: Major system integrators will be engaged as additional partners to validate, adopt, and lend credibility to the updated principles.
2. **Background Research**: A document analysis of Singapore's OT Cybersecurity Masterplan will be undertaken to provide a model for defining the 3rd party integrator role.
3. **Updating Principles and Documentation**: The Supply Chain Principles will be revised to explicitly include the 3rd party integrator role.

U.S. DEPARTMENT *of* ENERGY

Office of Cybersecurity, Energy Security, and Emergency 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 coordinated 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.

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.

How can Asset Owners contribute to CyTRICS?

- Prioritization guidance of equipment in use, paired with operational context
- Configuration use cases and insights into how AOOs design and protect
- Cyber supply chain risk management priorities and investment / budget considerations
- Insights into critical capability gaps that can inform CyTRICS research and development
- Feedback on the value of government programs (e.g., CyTRICS, CISA, or other DOE programs)
- Insight into emerging industry technologies, capabilities, trends, and sector-specific knowledge
- Quantifiable information on security impact of fixing vulnerabilities
- Contact cytrics@hq.doe.gov if you are interested in collaborating with CyTRICS!

What can CyTRICS offer AOOs?

- Independent third-party evaluation of systems important to AOOs
- Access to OT cybersecurity expertise and actionable insights, including:
  - Sharing of processes and technology
  - Independent evaluation of business processes addressing digital supply chain security
- Participation and influence of a national security effort
- Reputation-building with customers, vendors, and the greater community
- Mitigation recommendations while waiting for a vendor patch
- Cyber supply chain risk management best practices