

01 0 1

00 011

0101



# Securing Digital Energy Infrastructure: BESS Procurement Guidance & Sample Contract Terms

Emma M Stewart  
**Chief Power Grid Scientist**  
National and Homeland Security

Emma.stewart@inl.gov

October 8, 2024

Shari Gribbin – CNK Solutions

Battelle Energy Alliance manages INL for the  
U.S. Department of Energy's Office of Nuclear Energy



Idaho National Laboratory

# Introduction

- Technical Assistance Program
- Today's Focus: Procurement Guide & Sample Contract Terms
- Outcome and Outreach repeat

Who Should Use This Guide? "BESS Consumers"	
<i>BESS &amp; Digital Energy Systems Products &amp; Service Consumers</i>	
 PUBLIC SECTOR	 PRIVATE SECTOR
<ul style="list-style-type: none"><li>• Government Agencies</li><li>• Public Power, Co-Ops &amp; Munis</li><li>• Tribal</li><li>• State</li><li>• Local</li></ul>	<ul style="list-style-type: none"><li>• IBRs</li><li>• DERMs</li><li>• Storage Asset Owners</li><li>• Utilities</li></ul>

<b>BESS Supply Chain Security Procurement Guidance and Sample Contract Terms</b>	Section 1	Introduction
	Section 2	Maturing BESS Cyber Supply Chain Security: <b>General Overview</b>
	Section 3	Maturing BESS Cyber Supply Chain Security: <b>Procurement Bidding and Selection Process</b>
	Section 4	Maturing BESS Cyber Supply Chain Security: <b>Supplier Risk Assessment</b>
	Section 5	Maturing BESS Cyber Supply Chain Security: <b>Vendor Agreements and Procurement Terms</b>
	Section 6	Maturing BESS Cyber Supply Chain Security: <b>Supplier Management Controls</b>
	Section 7	Conclusion <ul style="list-style-type: none"><li>• References</li><li>• Appendix</li></ul>

# Acronyms

- BESS – Battery Energy Storage System
- BES – Bulk Electric System
- DERMS – Distributed Energy Resource Management System
- EVSE – Electric Vehicle Supply Equipment
- OT – Operational Technology
- ICS – Industrial Control System
- TA – Technical Assistance
- SIEM - Security Information and Event Management
- IDS – Intrusion Detection System
- SCRM – Supply Chain Risk Management
- IBR – Inverter Based Resources
- OEM – Original Equipment Manufacturer
- SBOM – Software Bill of Materials
- HBOM – Hardware Bill of Materials
- NERC CIP – North American Electric Reliability Corporation, Critical Infrastructure Protection
- NDAA – National Defense Authorization Act

# Webinar/Outreach Series – Technical Assistance for Digital Assurance (TADA)



Introduction to the TA Program for GRIP Awardees (Kicked off in April – available Online)



Cyber Informed Engineering Introduction & Training (August – Available online)



Procurement and Contracting Guide for BESS & associated components (Today)



Cyber Incident Response, OT Monitoring and building a security program for digital assets (Spring 2025)

<https://inl.gov/csdet-technical-assistance-and-training/>

## Grid Resilience and Innovation Partnerships (GRIP) Program Technical Assistance Resource Center

Grid Deployment Office

[Grid Deployment Office](#) » Grid Resilience and Innovation Partnerships (GRIP) Program Technical Assistance Resource Center

As part of the Bipartisan Infrastructure Law, the Grid Deployment Office (GDO) is administering a \$10.5 billion [Grid Resilience and Innovation Partnerships](#) (GRIP) Program to enhance grid flexibility and improve the resilience of the power system against growing threats of extreme weather and climate change.

In support of achieving these goals and addressing supply chain challenges for securing digital energy infrastructure, GDO's **Reliability, Risk, and Assurance Program** is offering educational resources, training, and technical assistance from the world-class experts and researchers at the U.S. Department of Energy (DOE) national labs.

---

### Digital Assurance Technical Assistance for Securing the Digital Energy Infrastructure

# Technical Assistance for Digital Assurance

**Core Challenge.** Many of the inverters, BESS, EVSE and software packages have a limited domestic supply chain

We must **enable** the **resilient deployment**, while also providing appropriate mitigations, training, support and security management solutions for digital controls

GDO enlisted INL to develop and deliver a **component security evaluation** and **mitigation technical assistance program** for key digital energy components

**Technical Assistance (TA)** is being offered to all GRIP and Grid Resilience State/Tribal Formula Grant Program Awardees at different stages of procurement and design

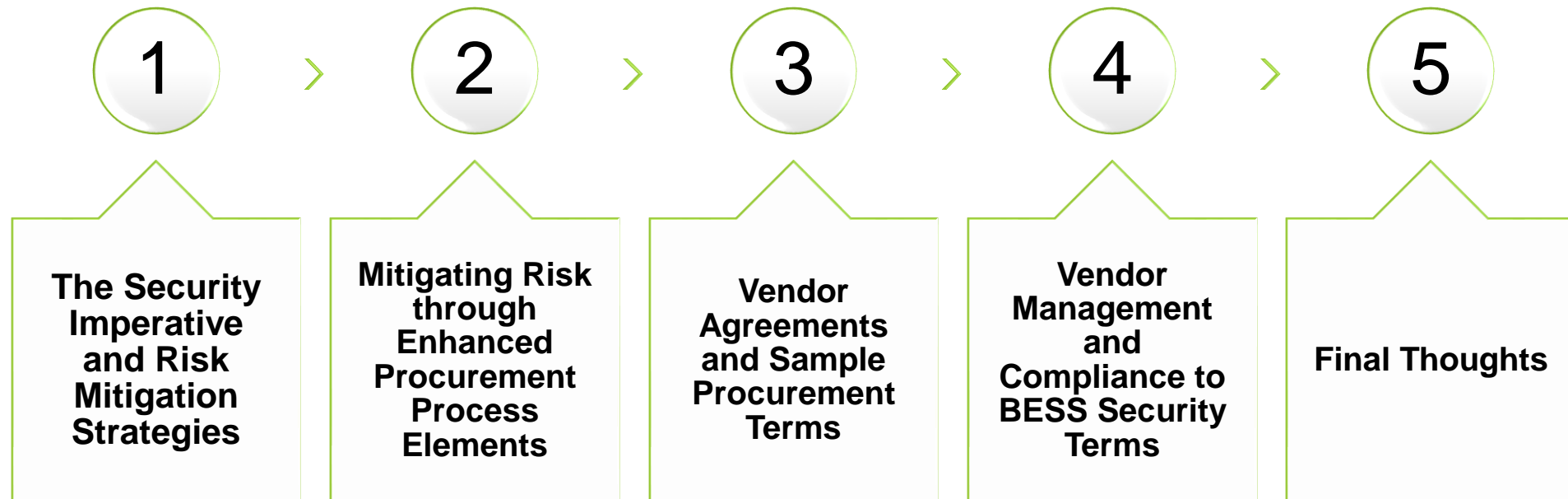
**Program Enrollment.** This program has open enrollment and sign up links are included on this slide.

TA Sign up here (for more info):

<https://inl.gov/csdet-technical-assistance-and-training/>

<https://www.energy.gov/gdo/grid-resilience-and-innovation-partnerships-grip-program-technical-assistance-resource-center>

# What is supply chain risk management in the context of electric grid modernization: Overview







# **BESS Supply Chain Security Risk Management**

---

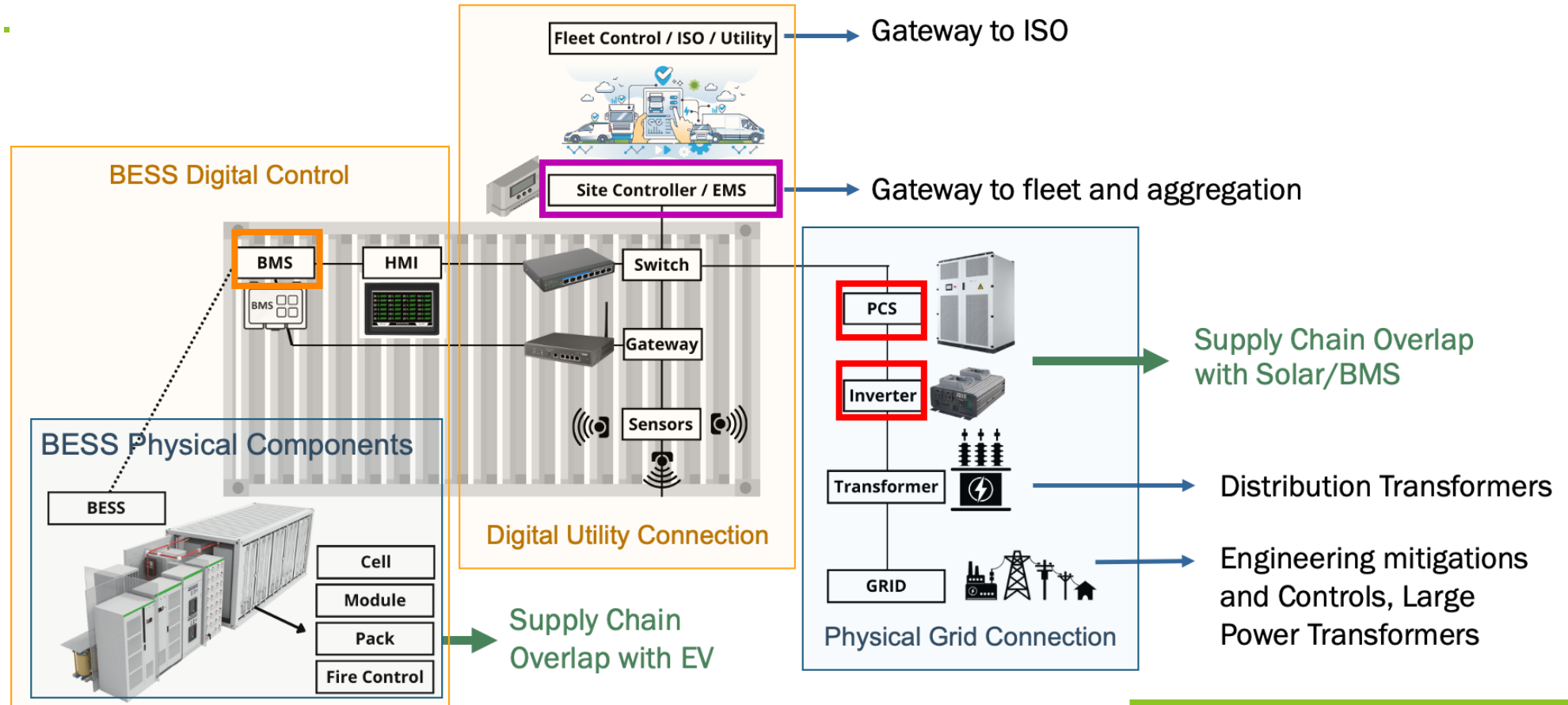
## **The Security Imperative & Risk Mitigation Strategies**

# Complex BESS, DERMS and IBR Supply Chain Extends across Energy Ecosystem

Battery component OEMs have evolved to be integrators and suppliers across the energy ecosystem, not just BESS. Integrator and supplier relationships create a complex web that obfuscates hardware origin and foreign influence.

Supply chain reports are challenging to interpret as they mix:

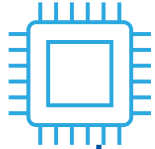
- Integrator vs. Core Supplier
- OEM products and “white-labeled” products
- EV & BESS components





# Supply Chain Challenges & Securing Digital Assets: Common Global Challenges - Procurement & Integration

1. Failing Chips



2. Persistent Communications



3. Hardcoded Passwords



4. Operation & Maintenance Models

5. White Labeled Products



6. Insecure Support Software

7. No SBOMs or HBOMs



8. Unknown Supply Chain 'Spiderweb' for Integrated Systems

9. Limited Threat and Consequence Modeling Capabilities



# Supply Chain Challenges & Securing Digital Assets: Common Global Challenge - Lack of Transparency & Control

## Introduction of Risk During Production Process

- Design
- Procurement of Subcomponents (e.g., processing chips)
- Manufacturing
- Assembly
- Shipping

**Limited  
Transparency &  
Control**

## Foreign Entity of Concern Organization (FEOC) Risks

- No regulation/oversight of design and manufacturing processes
- Foreign government pressure (adversarial action or provide customer information/data)
- Limited legal rights in foreign jurisdiction

# Supply Chain Challenges & Securing Digital Assets: Mitigation of Risk is Key

## Digital Asset Risks (Illustrative)

Remote Monitoring and Control Capabilities (expanding adversary attack surface)

Remote software and firmware update capabilities, which can allow suppliers to quickly deploy patches, but also expose the equipment to the potential of malicious firmware uploads

Reliance of critical systems on the software and firmware in digital equipment

Capability to rapidly change the functionality or behavior of devices through malicious or error-filled code updates

Proliferation of stakeholders who need, or claim to need, access to digital devices and their data



## Digital Asset Risk Mitigation (Illustrative)

SIEM/IDS, access management, packet monitoring

Isolate systems/assets/components; manual review and approval processes

Supply chain risk management and procurement processes for critical asset support software and firmware

Remote access and internal change management; internal network monitoring controls

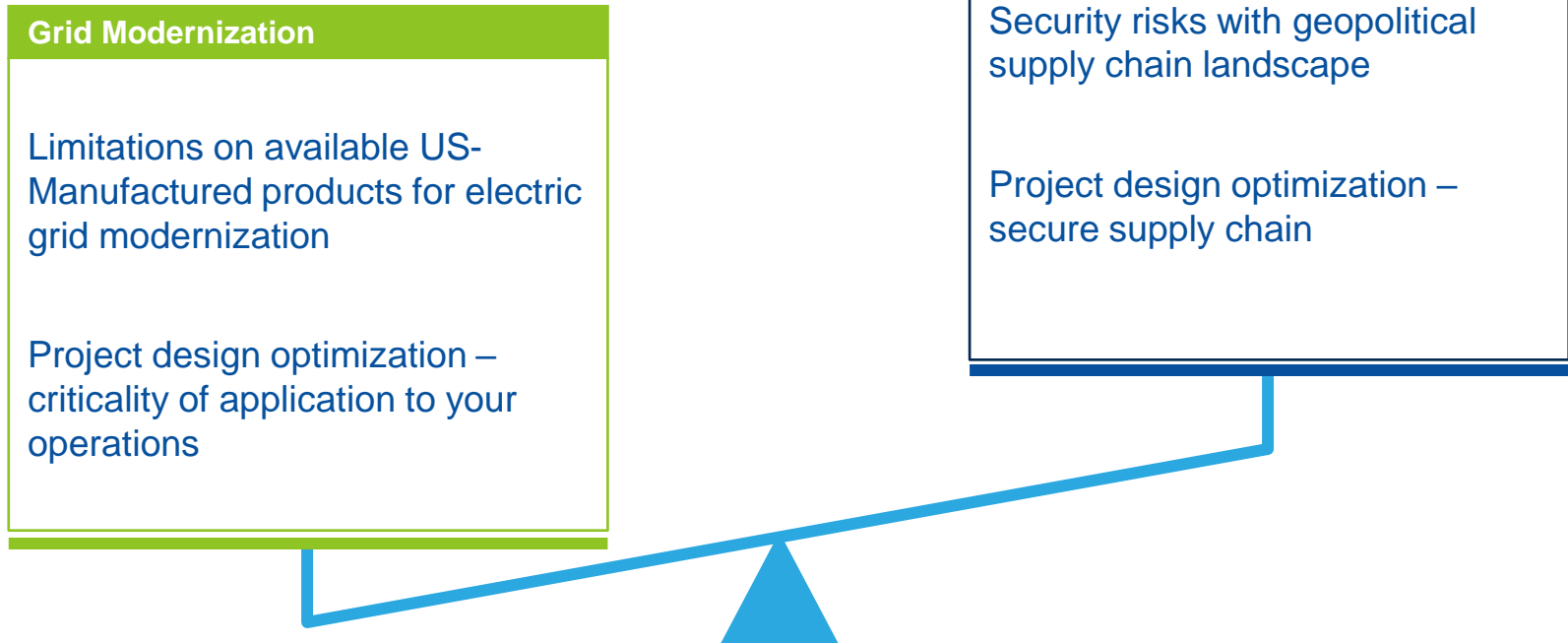
Rigorous access management processes, frequent review, confirm and updates; internal network/access monitoring

*Illustrative examples provided for discussion purposes, lists are not exhaustive*

# Supply Chain Challenges & Securing Digital Assets

## *Building Resilient Systems for Electric Grid Modernization*

- **Electric Vehicles (EVs) Supply Infrastructure**
- **Battery Energy Storage Systems (BESS)**
- **Management Systems Inverters**
- **Orchestration software (Distributed Energy Resources Management Systems (DERMS))**
- **Advanced Distribution Management Systems (ADMS)**



[Critical-and-Emerging-Technologies-List-2024-Update.pdf \(whitehouse.gov\)](#)

See the following sections of the FOA for information on disclosure requirements, domestic content, and related information: IV.D.xxi; IV.I; VI.B; Appendix B; Appendix C.

# BESS Supply Chain Risk Management: Policy Trends

## 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.

# BESS Supply Chain Risk Management: Regulation and Legal Trends

Common Approaches	<i>Regulatory-Legislative</i>	<i>Contractual &amp; Other Obligations</i>
<b>Enforcement</b>	Government/Agency Oversight and Enforcement Protocol	Private Party Contract Terms, Civil Litigation
<b>Implementation</b>	Compliance Program, Governance, Executing Controls	Internal Controls, Risk Management Programs
<b>Penalties</b>	Financial Penalties, Regulatory Directives, Increased Scrutiny, License & Authority Revocations	Termination of Agreement/Policy, Financial Assessment/Damages

## NERC CIP

[summary text placeholder]

## NDAAs

[summary text placeholder]





# **BESS Supply Chain Security Risk Management**

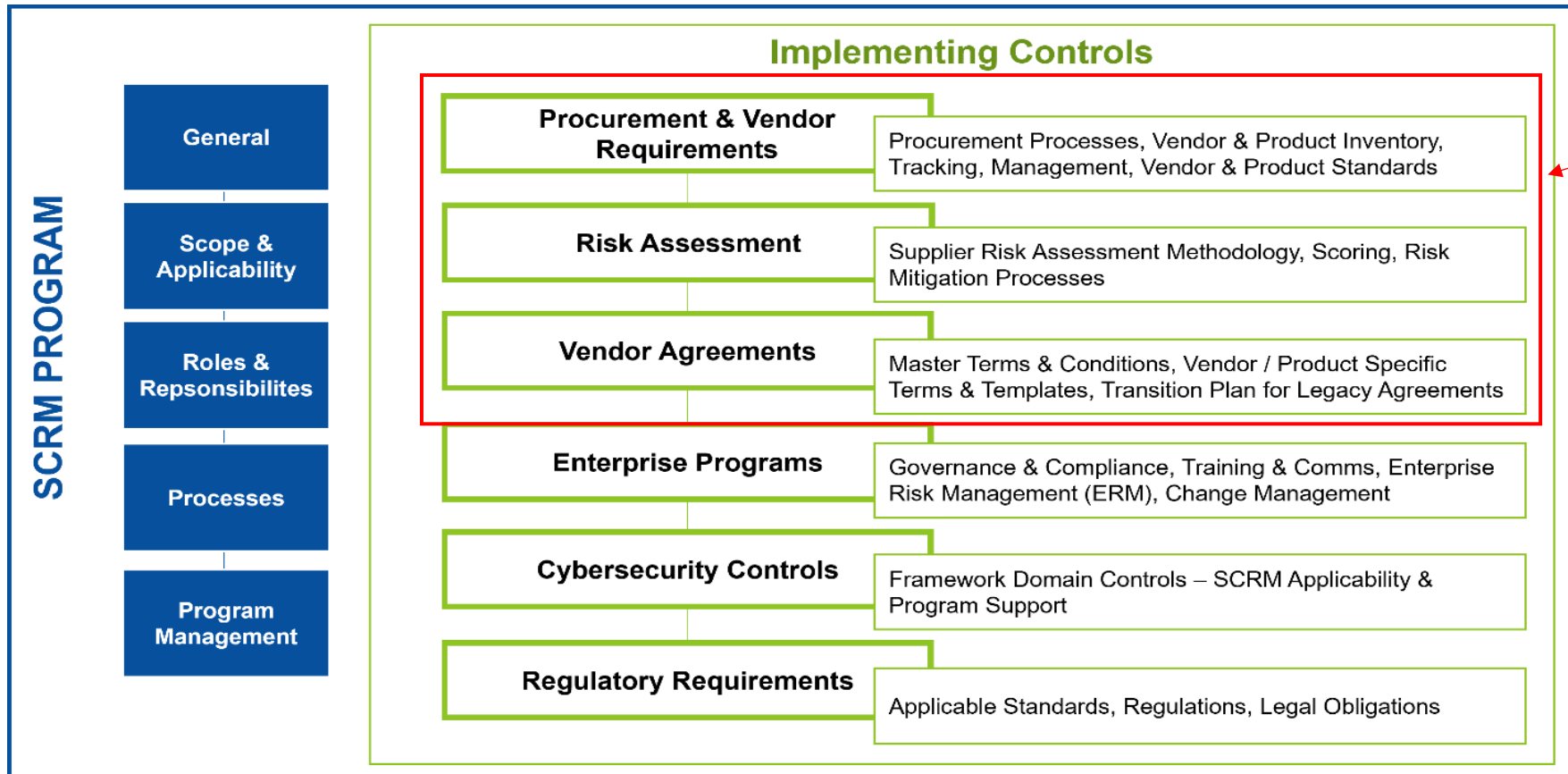
---

## **Mitigating Risk through Enhanced Procurement Process Elements**

# Securing the BESS Supply Chain

## Maturing Cyber Supply Chain Security

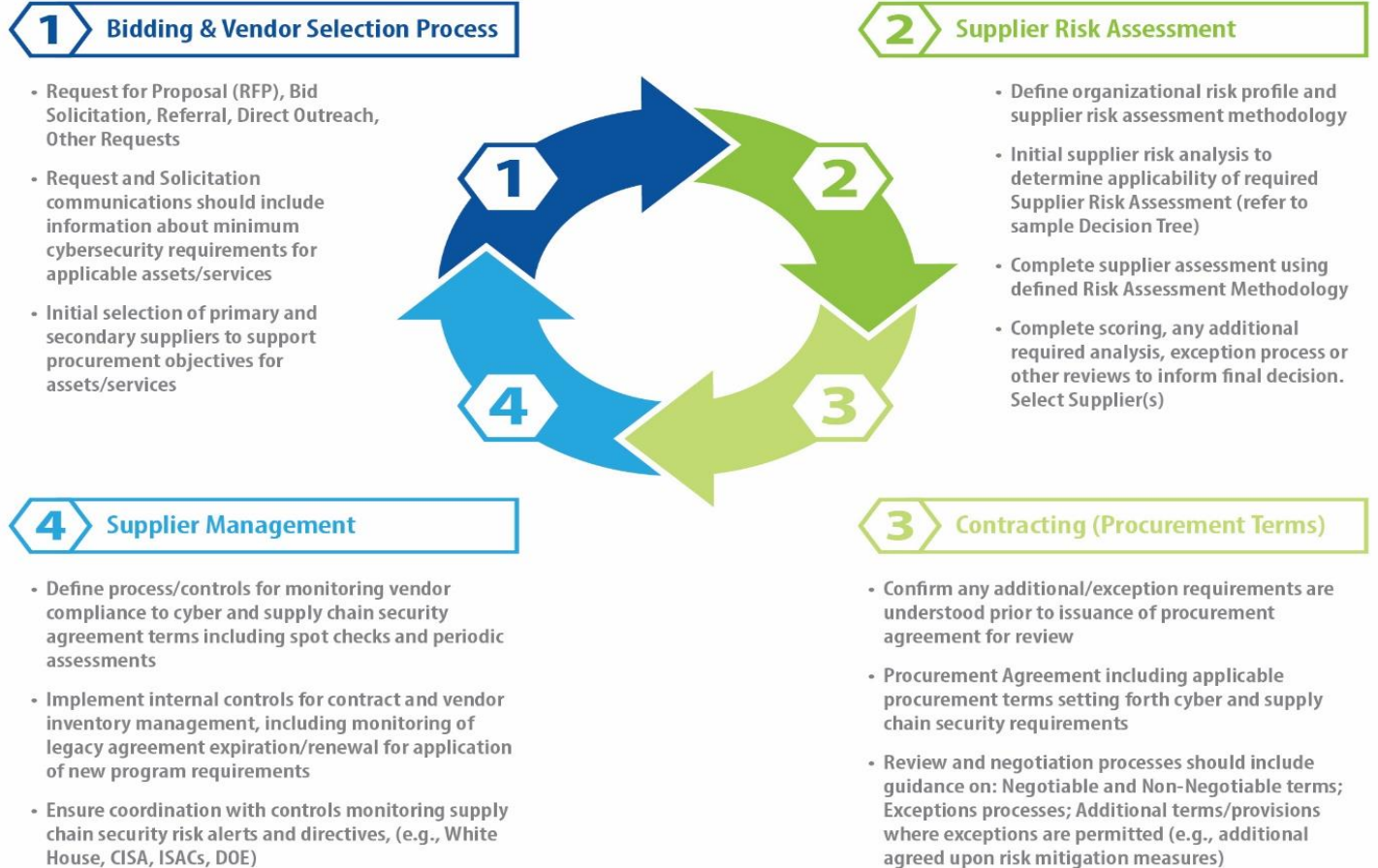
### Supply Chain Risk Management (SCRM) Program Basics



Critical Risk Mitigation Elements focus for this Guide

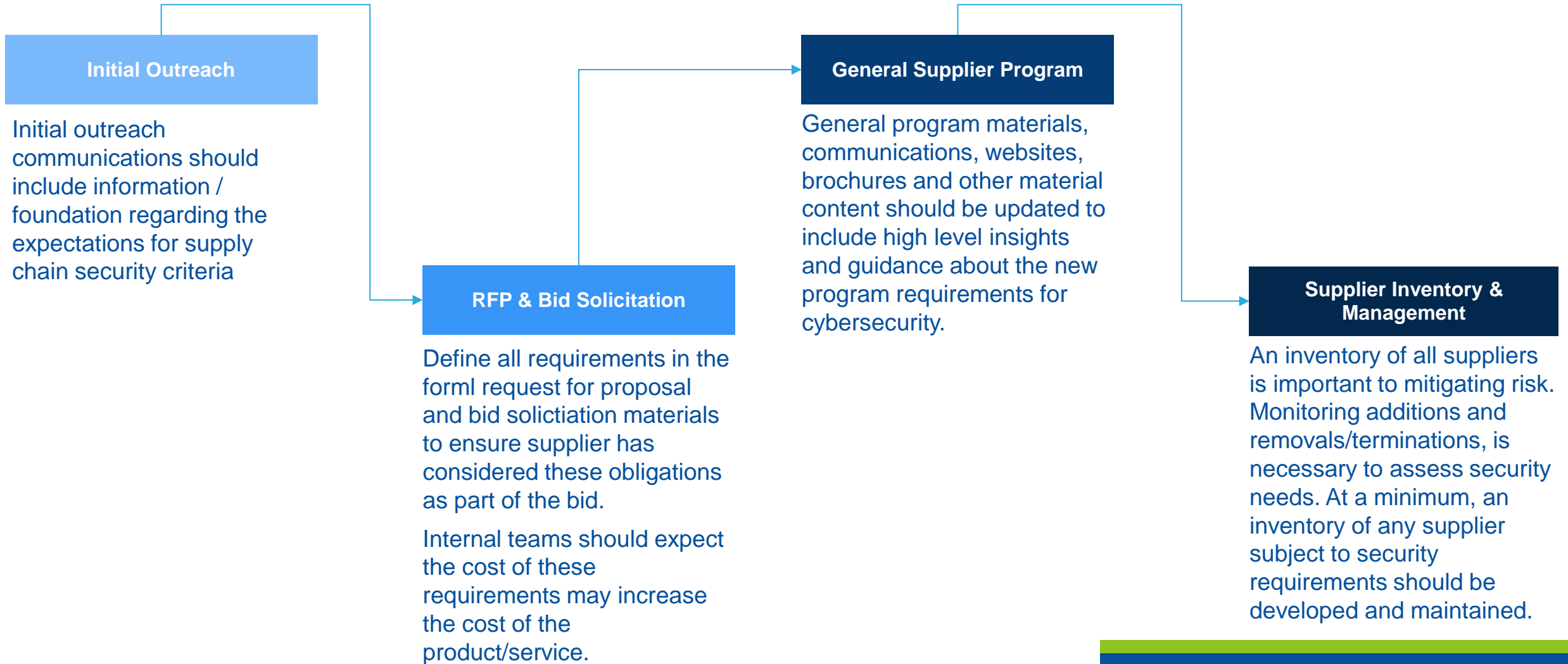
# Securing the BESS Supply Chain: Integrating Cybersecurity into Procurement Programs

Focus on **critical elements** that will support ability to **maximize risk mitigation** in early stage and less mature programs. Established programs focus on these elements as priority areas for improvement.



*This BESS Procurement Guide is part of a series of INL publications and supporting initiatives focused on enhancing BESS cybersecurity. For additional information on INL Digital Assurance project initiatives and other available resources, visit the [Center for Securing the Digital Energy Transition](#)*

# Procurement Bidding and Selection Processes



# BESS Vendor Risk Assessment

## *Key criteria and considerations for stronger SCRM programs*

### Products vs Services Vendors

- Risks for products vendors may be different than risks for services vendors. Mitigation controls may differ as well. Important to distinguish.

### Legacy vs New Suppliers

- Program applicability to legacy assets will likely need to be longer term initiative to transition vs. immediate applicability to new suppliers.

### Define Risk Priorities

- Risk profile and priorities differs for every entity. Critical to understand cross-implications to all business, operational, security, and other org risks.

### Risk Assessment Methodology

- Well-defined methodology that accounts for risk-based approach to applicability, assessment, exceptions processes helps prevent backlogs.

### Supplier Inventory & Management Controls

- Supplier inventory as important as inventory of products and services. Need to develop and manage to ensure ability to apply risk-based controls.

### Exemption Processes

- Exemption processes should be considered and defined within the program. These should be reviewed and updated with periodic updates.

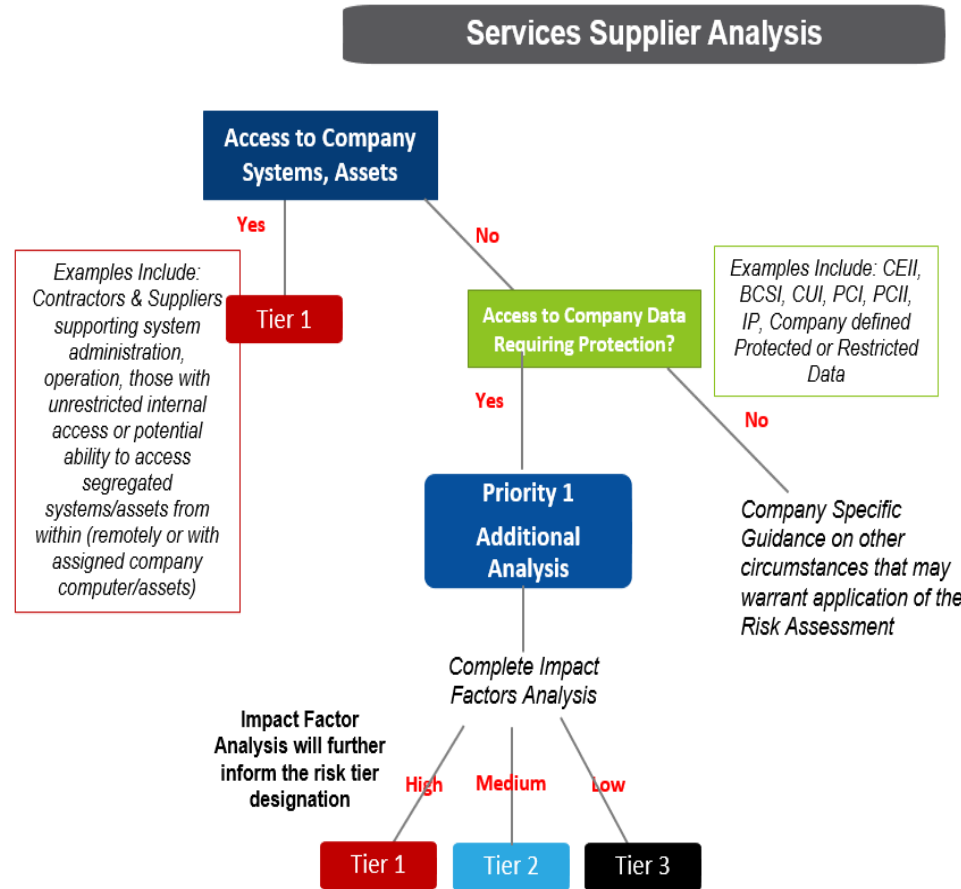
### Small Business & Independent Contractor Models

- Current assessment models do not account for unique infrastructure/ architecture of smaller business and independent contractors.

# BESS Vendor Risk Assessment: Initial Intake Analysis

May not be able to assess all vendors. Risk-based initial analysis will help focus on higher risk and maximize risk mitigation objectives

Illustrative: Sample Initial Analysis Risk Decision Tree for Services Suppliers



Examples Include: Contractors & Suppliers supporting system administration, operation, those with unrestricted internal access or potential ability to access segregated systems/assets from within (remotely or with assigned company computer/assets)

Examples Include: CEII, BCSI, CUI, PCI, PCII, IP, Company defined Protected or Restricted Data

Determination of Initial Risk Tier guides Decisions about the application of Risk Assessment & security specific procurement terms

**Tier 1**  
High Risk

Complete full Risk Assessment for Tier 1 Suppliers & use all applicable Cybersecurity & Supply Chain procurement terms (based on company risk profile and preferences)

**Tier 2**  
Medium Risk

Complete full or partial Risk Assessment for Tier 2 Suppliers & use any applicable Cybersecurity & Supply Chain procurement terms (based on company risk profile and preferences)

**Tier 3**  
Low Risk

Complete partial Risk Assessment for Tier 3 Suppliers **if warranted** & use any applicable Cybersecurity & Supply Chain procurement terms (based on company risk profile and preferences).

Some organizations may create "Tier 1, 2, 3" categories for the Cybersecurity & Supply Chain Risk Procurement Terms to be included to provide additional guidance.

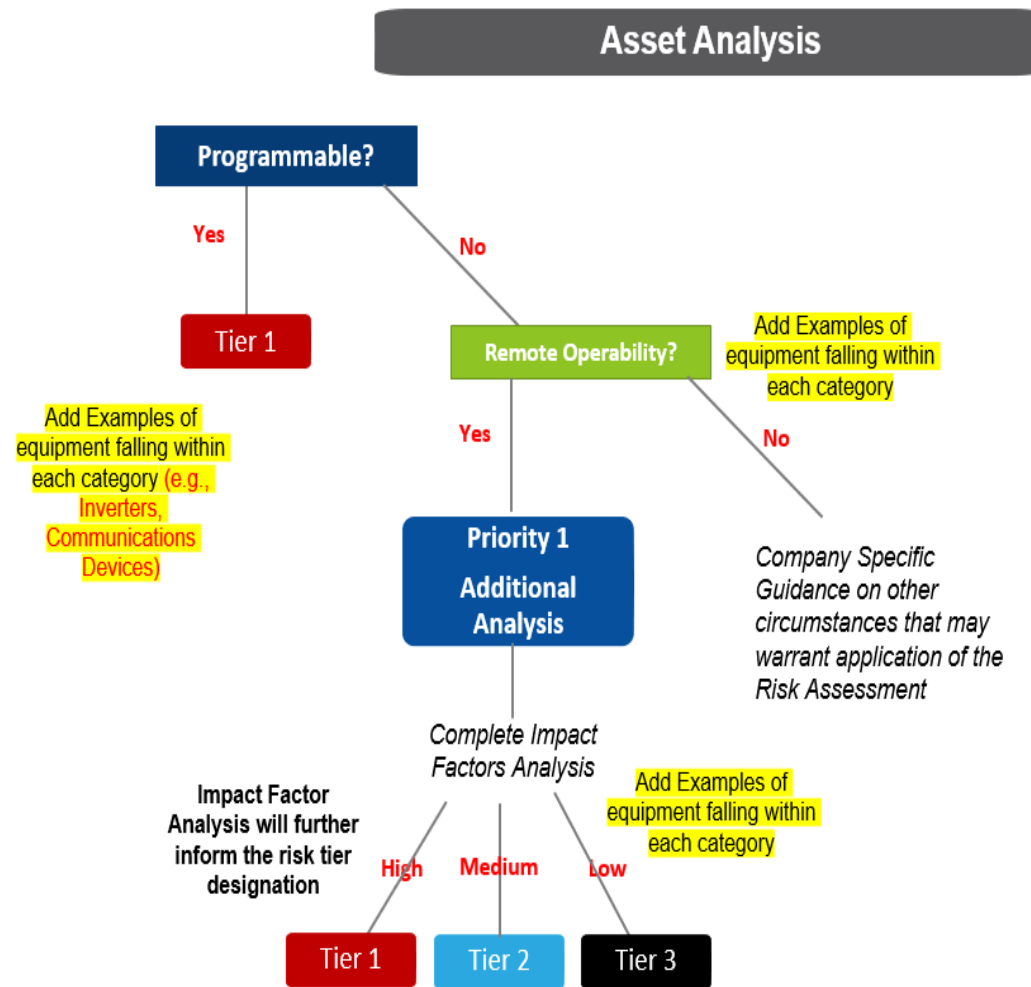
Impact Factor Analysis should include the following in addition to company specific considerations:

- Operations - Grid
- Operations - Internal
- Operations – Business Systems (IT, Finance, Billing)
- Reliability – Grid
- Security – Cyber, Physical



# BESS Vendor Risk Assessment: Initial Intake Analysis

May not be able to assess all vendors. Risk-based initial analysis will help focus on higher risk and maximize risk mitigation objectives



Add Examples of equipment falling within each category (e.g., Inverters, Communications Devices)

Add Examples of equipment falling within each category

Add Examples of equipment falling within each category

Impact Factor Analysis should include the following in addition to company specific considerations:

- Operations - Grid
- Operations - Internal
- Operations – Business Systems (IT, Finance, Billing)
- Reliability – Grid
- Security – Cyber, Physical

Determination of Initial Risk Tier guides Decisions about the application of Risk Assessment & security specific procurement terms

**Tier 1**  
High Risk

Complete full Risk Assessment for Tier 1 Suppliers & use all applicable Cybersecurity & Supply Chain procurement terms (based on company risk profile and preferences), **including required SBOM/HBOM**

**Tier 2**  
Medium Risk

Complete full or partial Risk Assessment for Tier 2 Suppliers & use any applicable Cybersecurity & Supply Chain procurement terms (based on company risk profile and preferences). Provide Guidance on **requirements for SBOM/HBOM**

**Tier 3**  
Low Risk

Complete partial Risk Assessment for Tier 3 Suppliers **if warranted** & use any applicable Cybersecurity & Supply Chain procurement terms (based on company risk profile and preferences).

Some organizations may create "Tier 1, 2, 3" categories for the Cybersecurity & Supply Chain Risk Procurement Terms to be included to provide additional guidance.

*Illustrative: Sample Initial Analysis Risk Decision Tree for Product & Equipment Suppliers Analysis*

# BESS Vendor Cybersecurity Risk-Assessment Methodology

For the vendors and suppliers that require a risk-assessment, you will need a methodology



# BESS Vendor Cybersecurity Risk-Assessment Methodology: Supplier Evaluation

1

## Collect Vendor Information

Typically completed through questionnaire aligned to standards framework to verify basic cybersecurity hygiene and selected specific requirements (e.g., SBOM, entity specific criteria)

2

## Conduct Risk Assessment

Application of scoring criteria and risk assessment methodology, identify any existing gaps, evaluate score and gaps

3

## Document Results & Additional Requirements

Results documented with supplier file/detail, identify and document additional requirements to address risk gaps, ensure these are integrated into contract

# BESS Supply Chain Security Risk Management

---

## Vendor Agreements and Sample Procurement Terms

Whereas, company wishes to ensure supplier does not pose security risks to its assets and systems

# Vendor Agreements and Procurement Terms

## Cybersecurity Definitions

## Appendix

- Terms and definitions specific to cyber, physical and supply chain security for review and integration into the agreement.
- Aligned to common / standard definitions (NIST, CISA primary sources).
- Should be reviewed against standard terms and definitions and aligned.
- Periodically review and update to ensure current version.

## Enterprise Cyber Hygiene Requirements

## §5.5

- Aligns to common standards framework and CISA recommended actions and basic maturity security.
- Assessment and Certification from credible assessor may satisfy some of these. Verify assessor prior to accepting.
- Sample terms for all standard cybersecurity framework domains and program controls. Select on case-by-case basis to support the objectives of the service / product relationship.

## Main Contract Review & Integration

*Reminder to review the main contract terms and definitions to ensure alignment and prevent cross-implication issues.*

## General Cyber & Supply Chain Security

## §5.4

- Major security program requirements typically required of most entities.
- Sample terms for incident response and notification of security incidents and breach.
- Hardware Bill of Materials (HBOM) and Software Bill of Materials (SBOM) terms for products. These should be reviewed and aligned to current state models as they evolve.


## BESS Equipment Terms & Conditions

## §5.6

- Terms to address additional BESS specific risks.
- Sample terms for common risks included here.
- Develop additional BESS asset/component specific requirements addressing your security risks (e.g., specific access controls, specific tool or use or services activities).
- This may include HBOM and SBOM if not included in one of the other sections **or** an asset specific SBOM or HBOM.

## Small Vendor & Independent Contractors

*Small **services** vendors and independent contractors may require unique approaches and different terms.*

**Disclaimer:** This BESS Procurement Guide and these terms and conditions do not purport to provide legal advice. Counsel should be consulted to obtain advice and guidance for use within any agreement. 

*Sample Terms provided are based on current leading practice. Where integrated into a program model or template, ensure a control for periodic review and update.*



# **BESS Supply Chain Security Risk Management**

---

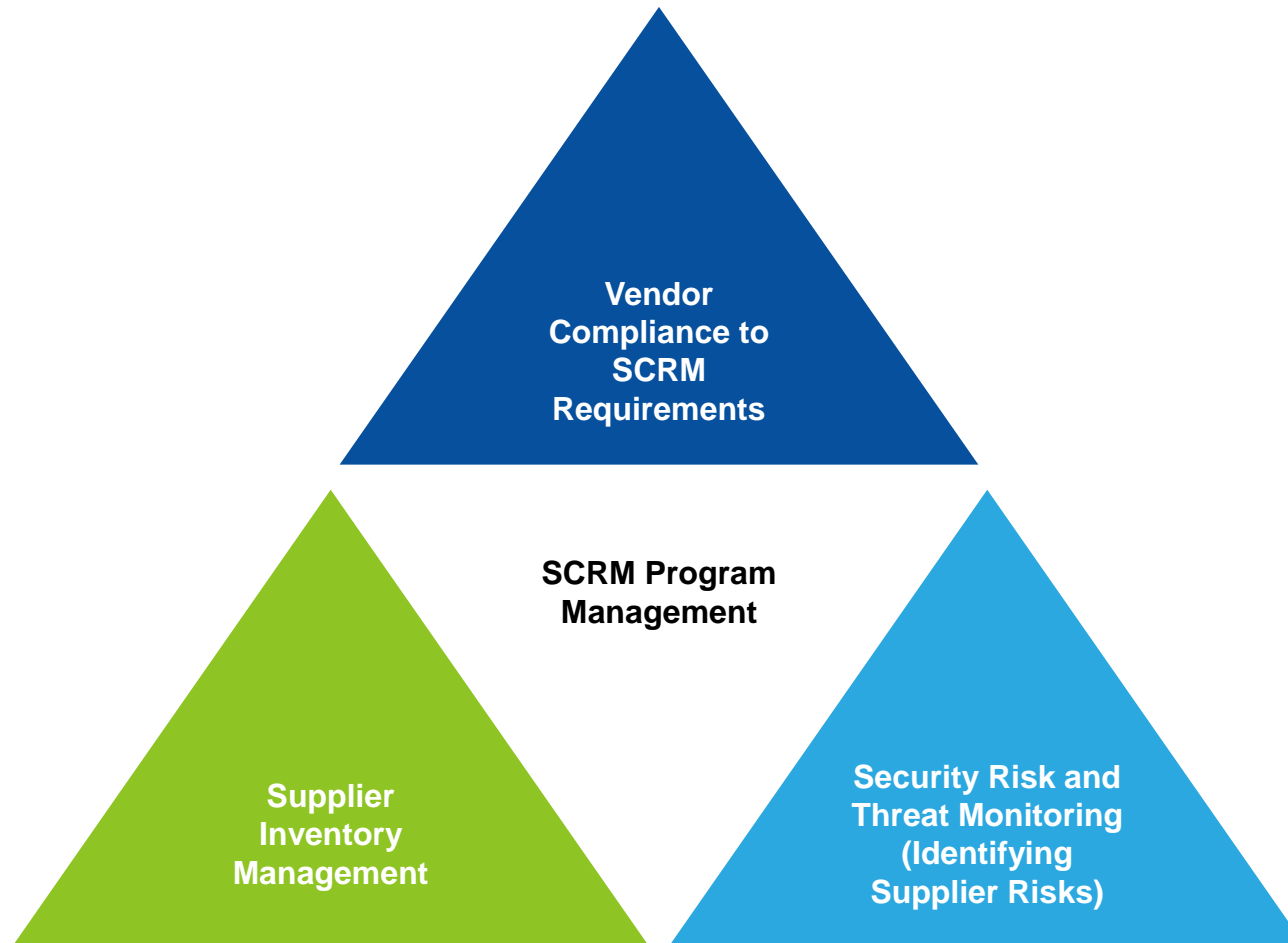
## **Vendor Management and Compliance to BESS Security Requirements**

[Placeholder for picture or graphic]



# Vendor Management Controls

*Important to maintain your program and monitor for new vendors and/or risks that may impact the application of requirements to new and existing vendors.*





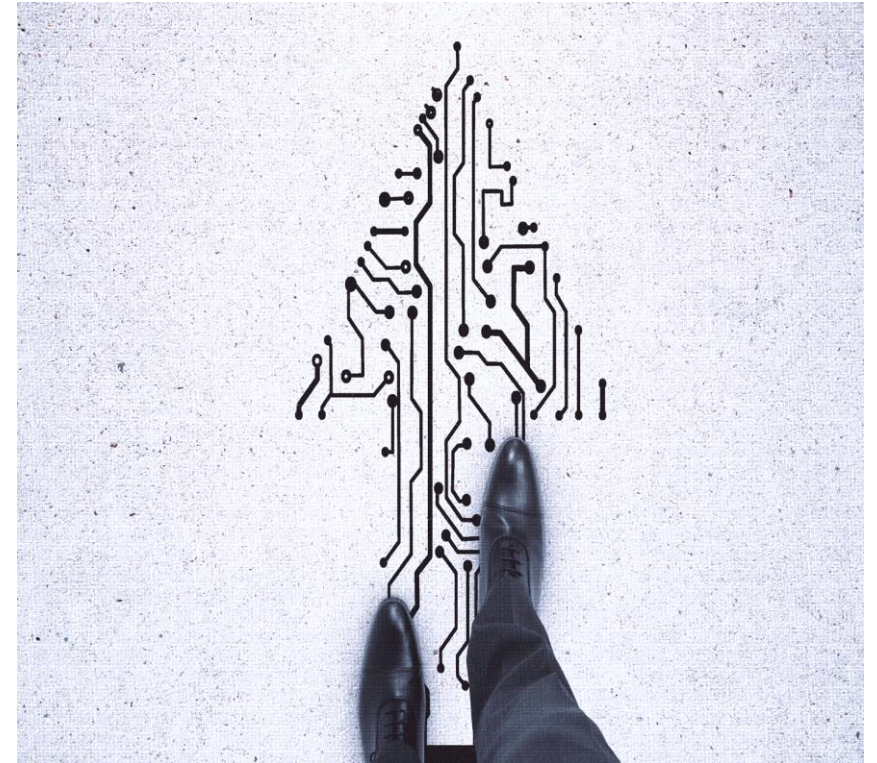
# **BESS Supply Chain Security Risk Management**

---

## **Conclusion**

# Final Thoughts

- Not a one and done
- Things learned here could apply across the range of supply chain
- This is guidance, not prescription - always review your own standards, requirements for compliance etc.
- TA – is available upon completing the application via the link
  - <https://inl.gov/csdet-technical-assistance-and-training/>
- Guide will be released in a few weeks



# Webinar/Outreach Series – Technical Assistance for Digital Assurance (TADA)



Introduction to the TA Program for GRIP Awardees (Kicked off in April – available Online)



Cyber Informed Engineering Introduction & Training (August – Available online)



Procurement and Contracting Guide for BESS & associated components (Today)



Cyber Incident Response, OT Monitoring and building a security program for digital assets (Spring 2025)

<https://inl.gov/csdet-technical-assistance-and-training/>

## Grid Resilience and Innovation Partnerships (GRIP) Program Technical Assistance Resource Center

Grid Deployment Office

[Grid Deployment Office](#) » Grid Resilience and Innovation Partnerships (GRIP) Program Technical Assistance Resource Center

As part of the Bipartisan Infrastructure Law, the Grid Deployment Office (GDO) is administering a \$10.5 billion [Grid Resilience and Innovation Partnerships](#) (GRIP) Program to enhance grid flexibility and improve the resilience of the power system against growing threats of extreme weather and climate change.

In support of achieving these goals and addressing supply chain challenges for securing digital energy infrastructure, GDO's **Reliability, Risk, and Assurance Program** is offering educational resources, training, and technical assistance from the world-class experts and researchers at the U.S. Department of Energy (DOE) national labs.

---

### Digital Assurance Technical Assistance for Securing the Digital Energy Infrastructure



# Idaho National Laboratory

*Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.*