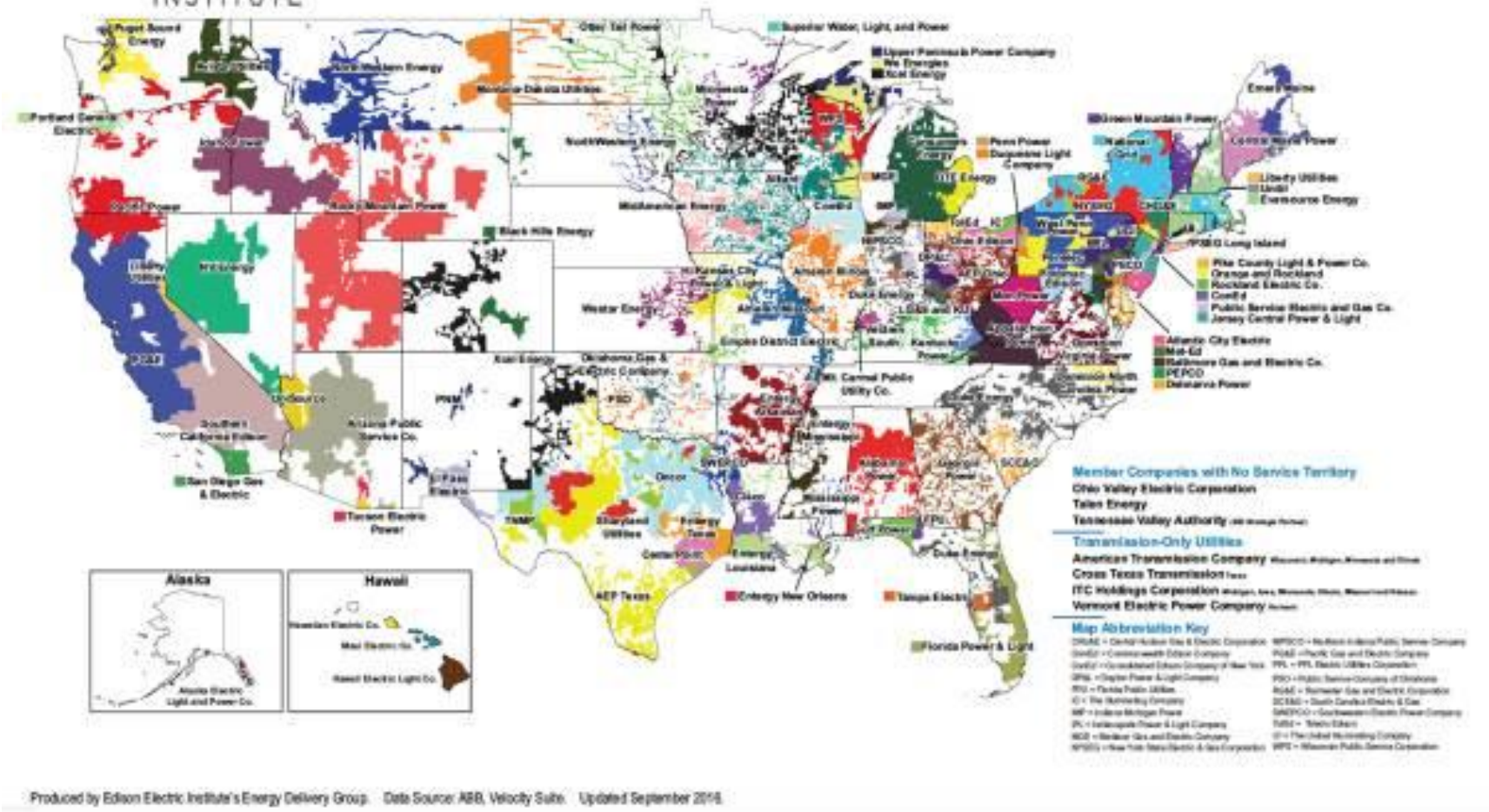
Supply Chain Risk Management

NERC Small Group Sessions
October 30, 2019
Atlanta, GA

Kegan Gerard | Manager, Cyber and Infrastructure Security | Edison Electric Institute

EEI U.S. Member Company Service Territories



Produced by Edison Electric Institute's Energy Delivery Group. Data Source: ABB, Velocity Suite. Updated September 2016.

Overview

- EEI Activities
- Lifecycle
- Risk Profile
- Tiering and Assessments
- Procurement Contract Language
- Measures & Controls
- Considerations & Challenges

EEI Activities

- Supply Chain Workshop – August 2019
- Multi-Disciplinary Working Groups:
  - Supply Chain Working Group
  - Security, Reliability/Compliance, Legal, Procurement
- Vendor/Supplier Relationships

Lifecycle

- Risk Profile
  - Questionnaire / Audits / Assessments
  - Risk rank
- Contracts and Procurement
  - Risk acceptance: business units
  - Contract language
- Security Controls and other Mitigations

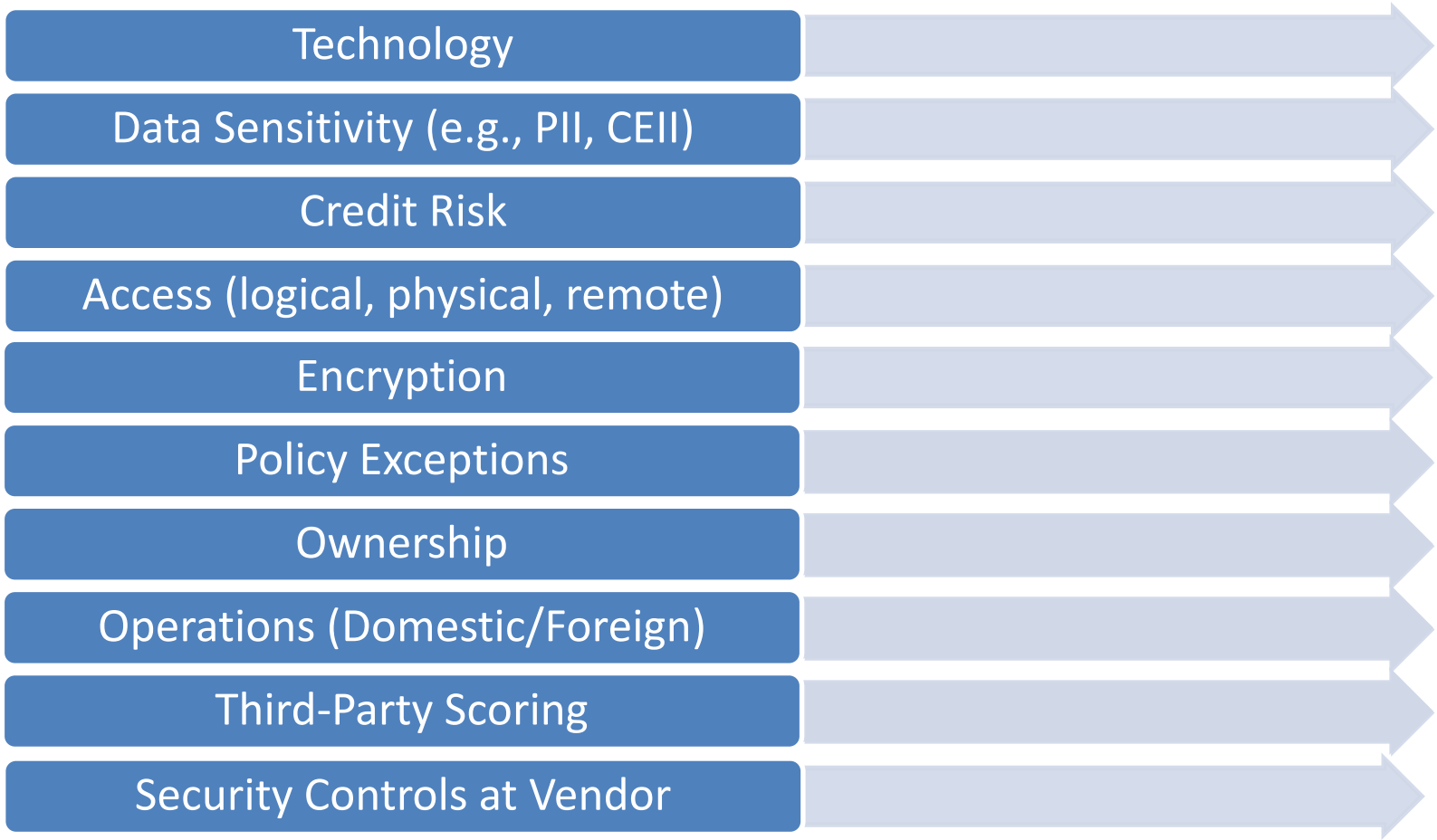
Risk Profile: Tiering and Assessments

- Standardized Assessments

- Build the assessment into your normal supply chain processes
  - when a new vendor arrangement is being considered
  - when an existing vendor arrangement is being renewed
  - when use case has changed
  - other internal or external triggers

- Potential Tiers
  - High (annual review)
  - Medium, (2 year review)
  - Low (as needed)

Risk Profile: Potential Factors

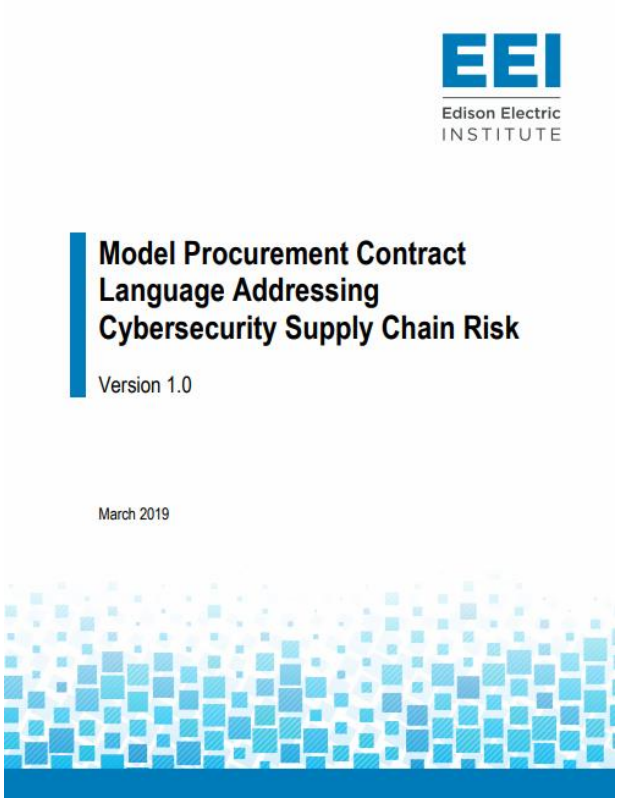


Procurement and Contracts

- Vendor risk assessment report for internal decision makers that provides sufficient information on the security posture of the vendor to enable an informed decision about doing business with the vendor
- Risk approval or acceptance: consider senior-level sign-off
- Include suitable security terms in vendor contracts before signing on the dotted line.
- Consider security, compliance, risk, liability

Procurement and Contracts

- Responsible Entities will address CIP-013-1 requirements by, among other means, inserting contract terms that address the R1.2 security controls in agreements with vendors.
- The model procurement contract language contained in this document targets:
  - the processes required in CIP-013-1 Requirement R1.2
  - supporting contract terms that address related information and data protection to strengthen cybersecurity overall.
- *Link*
- *Disclaimer*



Measures & Controls

- Asset and Supplier Inventory
- Traditional Defense-In-Depth
  - Patching, whitelisting, network segmentation, etc.
- Reducing third-party access to company assets or networks. Transition to access by exception.
- Vulnerability Scanning
- Source Code Escrow
- Audit Triggers
  - If a breach has been reported and vendor did not inform entity
  - On-site assessment if vendor has been breached

Considerations & Challenges

- Examine non-traditional contracts (e.g., law firms)
- Corporate credit cards
  - Assess need, credit limit
- Open source
  - Limited notification capabilities
- Unsupported products
  - Renew risk acceptance at defined frequency

Questions?

The Edison Electric Institute (EEI) is the association that represents the U.S. investor-owned electric industry. Our members provide electricity for 220 million Americans, operate in all 50 states and the District of Columbia, and directly employ more than 500,000 workers. Safe, reliable, affordable, and clean electricity powers the economy and enhances the lives of all Americans.

The EEI membership also includes dozens of international electric companies as International Members, and hundreds of industry suppliers and related organizations as Associate Members.

Since 1933, EEI has provided public policy leadership, strategic business intelligence, and essential conferences and forums for the energy industry.

For more information, visit our Web site at www.eei.org.

Edison Electric Institute
701 Pennsylvania Avenue, NW
Washington, D.C. 20004-2696
202-508-5000 | www.eei.org

North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

NATF Supply Chain Cyber Security Proof of Concept Project Status Update

October 2019

Open Distribution

North American Transmission Forum (NATF) Overview

Guiding Principles

Community *Confidentiality* *Candor* *Commitment*

Mission

- **Promote excellence** in the reliable and resilient operation of the electric transmission system

Vision

- **Continuously improve** the reliability and resiliency of the electric transmission system

Approach

- Aggressively pursue reliability and security excellence by:
  - Fostering **constructive peer challenge** to improve
  - Efficiently **sharing timely, detailed, and relevant information**, including lessons learned and superior practices

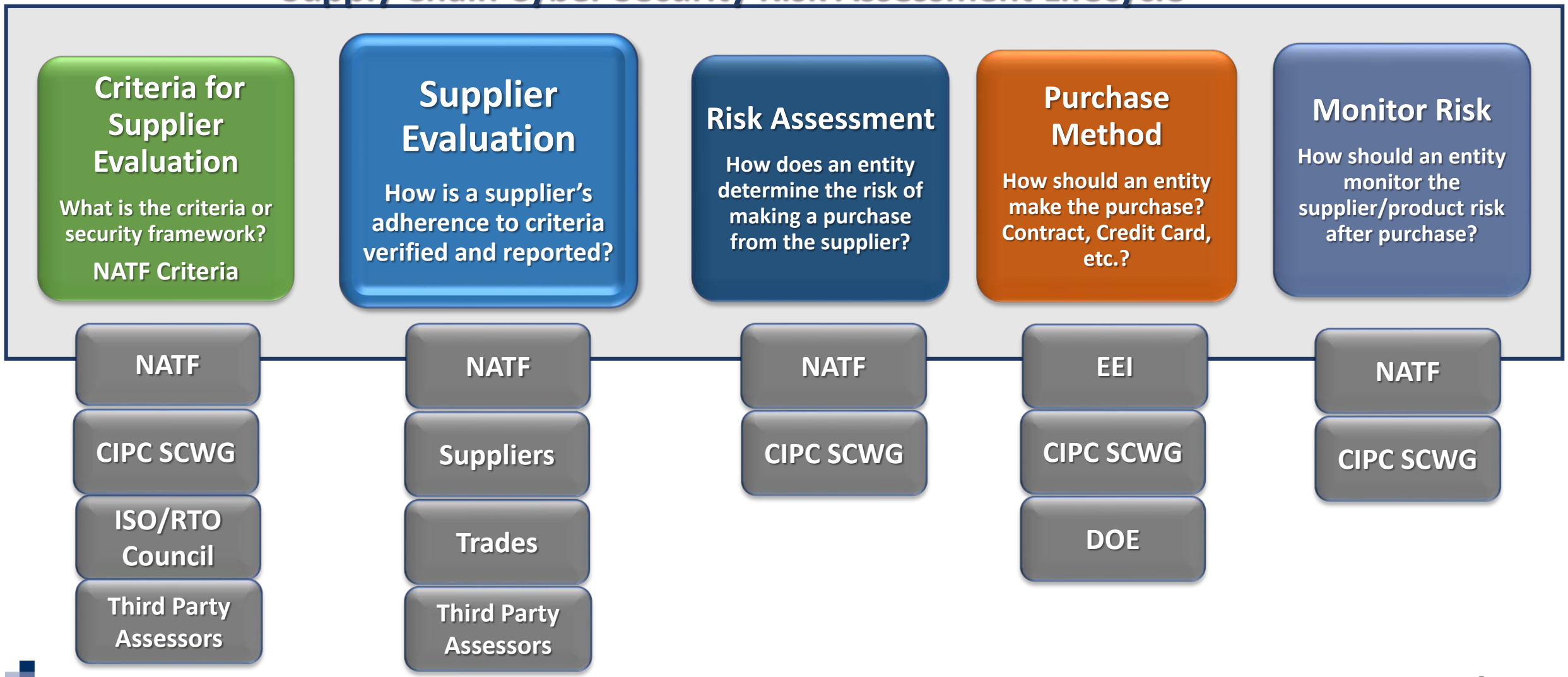
Members

- 89 members
- 73 affiliates
- ~80% miles 200 kV+
- ~90% net peak demand

North American Transmission FORUM

Proof of Concept Project Supports Other Efforts

Supply Chain Cyber Security Risk Assessment Lifecycle



Proof of Concept Project Builds on Cyber Security Foundational Resources

- Cyber Security Supply Chain Risk Management Implementation Guidance (from CIP-013 Drafting Team)
- NATF Cyber Security Supply Chain Risk Management Guidance Whitepaper
- NATF CIP-013 Implementation Guidance v2 (*Reliance on 3rd-party assessments*)
- APPA/NRECA Managing Cyber Supply Chain Risk-Best Practices for Small Entities Whitepaper
- NAGF Cyber Security Supply Chain Management White Paper
- EPRI Supply Chain Risk Assessment Report
- EEI Cyber Security Supply Chain Procurement Language
- NERC Final Supply Chain Report
- SCWG Whitepapers (5 approved by CIPC; 2 pending CIPC approval; 1 in development)

Proof of Concept Project Objectives

Develop an approach or approaches to evaluate a supplier's supply chain cyber security practices that address:

Security

- Identifies cyber security risks introduced via supply chain

Efficiency and Effectiveness

- Converges on common approaches to achieve reasonable assurance of suppliers' security practices and streamlines the process

Compliance

- Addresses requirements in NERC supply chain related CIP standards (CIP-013-1; CIP-005-6 R2.4; CIP-010-3 R1.6)

The NATF Criteria are the basis for the evaluations

The NATF Criteria

What is the criteria or security framework?

The NATF Criteria

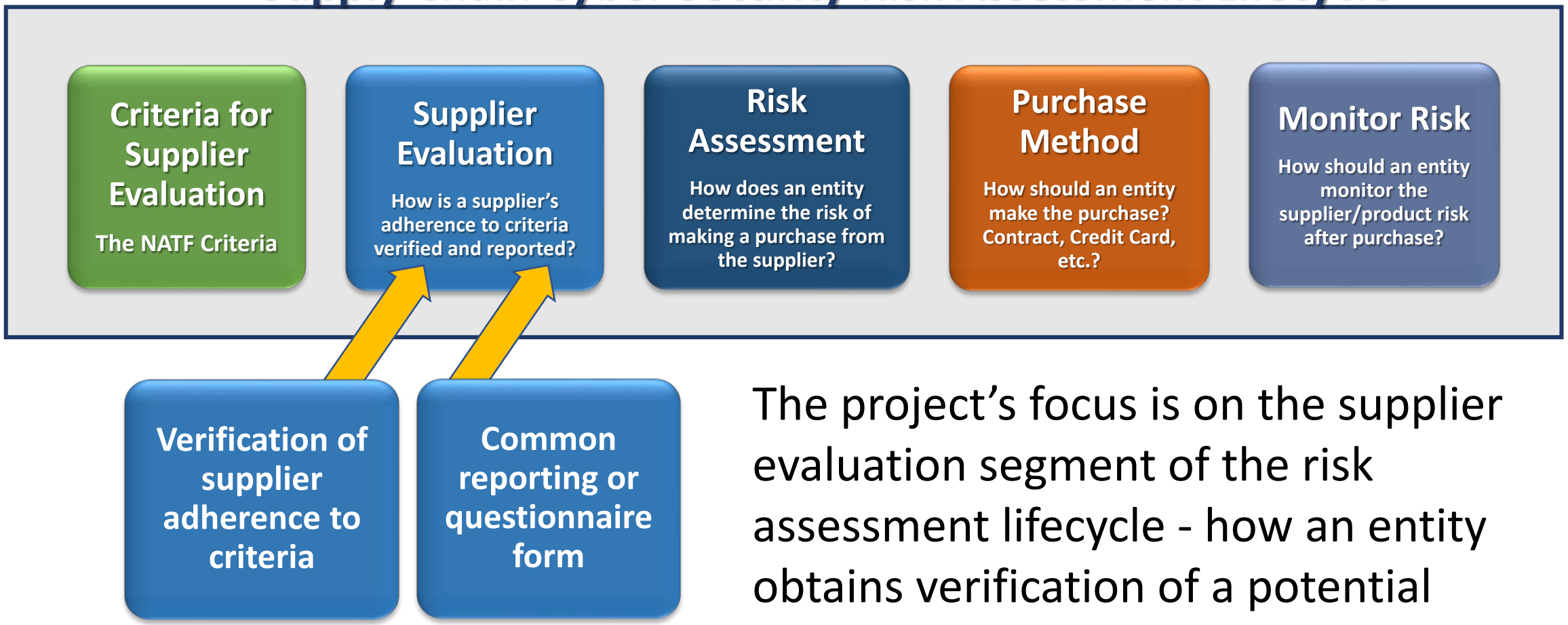
July 2019

Final Criteria Spreadsheet and Application Guide are Posted for Open Distribution

- Criteria focuses on supply chain cyber security practices
  - Criteria requires adherence to an existing cyber security framework to demonstrate broader cyber security practices
- Contains 68 criteria and 26 organizational information considerations
  - Designation of whether each criteria is required by the NERC CIP Standards or included for security practice
  - Originally Mapped to 3 sample existing frameworks (NIST, ISO 27001, SOC2); additional frameworks are being added (CIS Controls v7.1, IEC 62443)
- Application Guide provided contains additional information

The NATF Proof of Concept Project

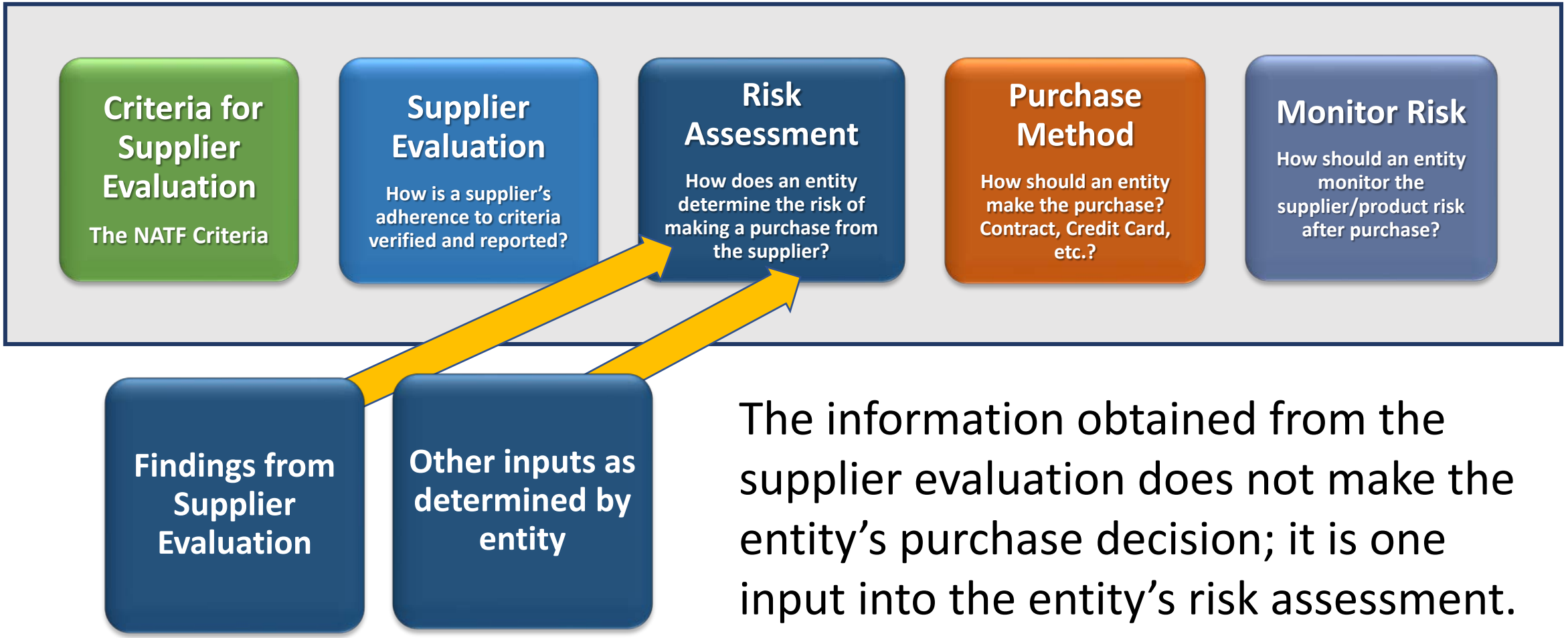
Supply Chain Cyber Security Risk Assessment Lifecycle



The project's focus is on the supplier evaluation segment of the risk assessment lifecycle - how an entity obtains verification of a potential supplier's adherence to the NATF Criteria.

The NATF Proof of Concept Project

Supply Chain Cyber Security Risk Assessment Lifecycle



The information obtained from the supplier evaluation does not make the entity's purchase decision; it is one input into the entity's risk assessment.

NATF Proof of Concept Team

How is a supplier's adherence to criteria verified and reported?

Proof of Concept October 2019

Proof of Concept Team developed a Strawman Model

- Collaborated with entities, suppliers and third-party assessors to develop strawman model
- Use of established reporting systems and existing frameworks/standards recognized by other industries for streamlining verification and reporting
- Model provides for scalability

NATF Proof of Concept Team Members

How is a supplier's adherence to criteria verified and reported?

Proof of Concept October 2019

Entities

- Ameren
- AEP
- Duke
- Exelon
- NPPD
- PPL
- PJM
- Southern Co

Suppliers

- ABB
- GE Grid Software Solutions
- OSI
- Siemens Industry, Inc.
- Schneider Electric
- Schweitzer Engineering

Third-Party Assessors

- Ernst & Young
- KPMG LLP
- PWC

The Successful Solution

How is a supplier's adherence to criteria verified and reported?

For Entities

- Streamlined, Effective and Efficient
  - Flexible (doesn't require one method)
  - Simple
  - Clear
- Timely (completed so it is available for entities' use)
- Scalable and inclusive for all entities and suppliers
- Suppliers support solution
- Provides value to entities as input for risk assessments
- If executed properly, meets compliance requirements

The Successful Solution

How is a supplier's adherence to criteria verified and reported?

For Suppliers

- Streamlined, Effective and Efficient
  - Adoption across electric industry
    - Industry all using the same model/criteria provides suppliers with the ability to share assessments
- Be transparent about criteria
  - Be clear about what is really being considered
  - Consider international challenges

For Third-Party Assessors

- What type(s) of assessments will be successful in meeting need
  - Consistent criteria
  - Differentiate between standard and good practice (i.e., what needs to be included in certification or opinion)

Proof of Concept Strawman Model Principles

How is a supplier's adherence to criteria verified and reported?

Proof of Concept October 2019

- The NATF Criteria provides a consistent basis for evaluating a supplier's supply chain cyber security practices
- Verification of supplier adherence to NATF Criteria may be accomplished in a variety of ways
- Qualified third-party verification provides the highest level of assurance
- Level of assurance an entity requires for supplier adherence to NATF Criteria depends upon:
  - product risk
  - entity risk
  - available risk mitigation actions

NATF Proof of Concept Socialization

How is a supplier's adherence to criteria verified and reported?

Proof of Concept November/ December 2019

Obtain Socialization Across Industries

- Electric Power Industry
  - Collaboration with trade organizations and forums
- Suppliers
  - Various sizes/situations - Model must provide for scalability
- Third-Party Assessors
- Regulators

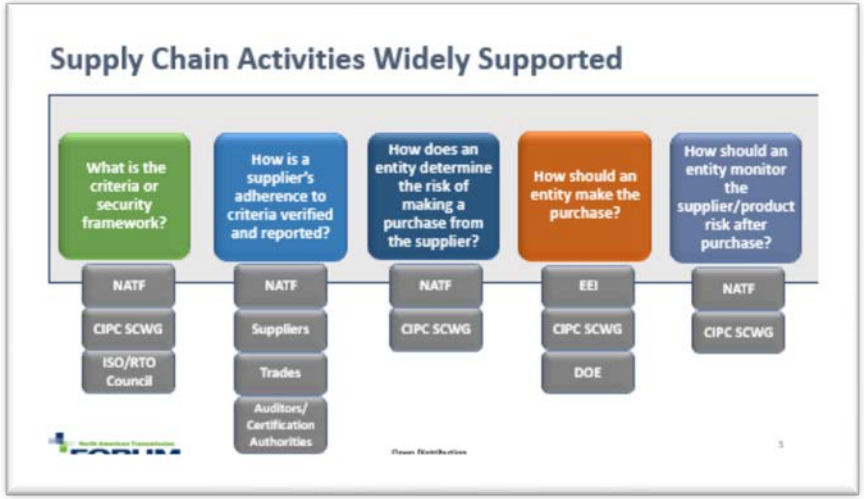
NATF Proof of Concept – Timeline

How is a supplier's adherence to criteria verified and reported?

Proof of Concept Next Steps

- November –
  - NATF Criteria Team and Supply Chain Steering Team reviews NATF Criteria for minor modifications based on Proof of Concept Team inputs and develops modification process
- November/December –
  - Socialization across entities and regulators; Integration of input
  - Awareness to suppliers and third-party assessors
  - Industry outreach communication
- February – Report industry solution to NERC
- February/March –
  - Socialization across suppliers and third-party assessors
  - Development of regulator support (implementation guidance, ERO Practice Guide)

A Developing Opportunity for Collaboration



- **For Proof of Concept Activities**
  - Industry Organizations are coming together
  - Common solutions that benefit the industry

- **For Future Supply Chain Activities**
  - Working towards coordination and collaboration of work for future projects

Take-aways

NATF Supply Chain Cyber Security Criteria

- Is posted and open for industry use
- An industry-wide process for modifications is being developed

NATF Proof of Concept Strawman is completed and being socialized

- With entities, suppliers, third-party assessors and regulators

Key Principles for Proof of Concept Strawman are established

- The NATF Criteria provides a consistent basis for evaluating a supplier's supply chain cyber security practices
- Verification of supplier adherence to NATF Criteria may be accomplished in a variety of ways
- Qualified third-party verification provides the highest level of assurance
- Level of assurance an entity requires for supplier adherence to NATF Criteria depends upon product risk, entity risk, and available risk mitigation actions

Supplier evaluation does not determine an entity's purchase decision; it is one input into an entity's risk assessment

NATF will coordinate with other industry organizations on future projects

Questions

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Supply Chain Risk Assessment

Howard Gugel, Vice President of Engineering and Standards

Member Representatives Committee Meeting

November 5, 2019

RELIABILITY | RESILIENCE | SECURITY




Board Resolution

- Support effective and efficient implementation (e.g. CIP V5 transition)
- **Supply chain risk study**
- Communicate supply chain risks to industry
- Forum and Association white papers
- Plan to evaluate effectiveness of supply chain standards

Recommendations from Study

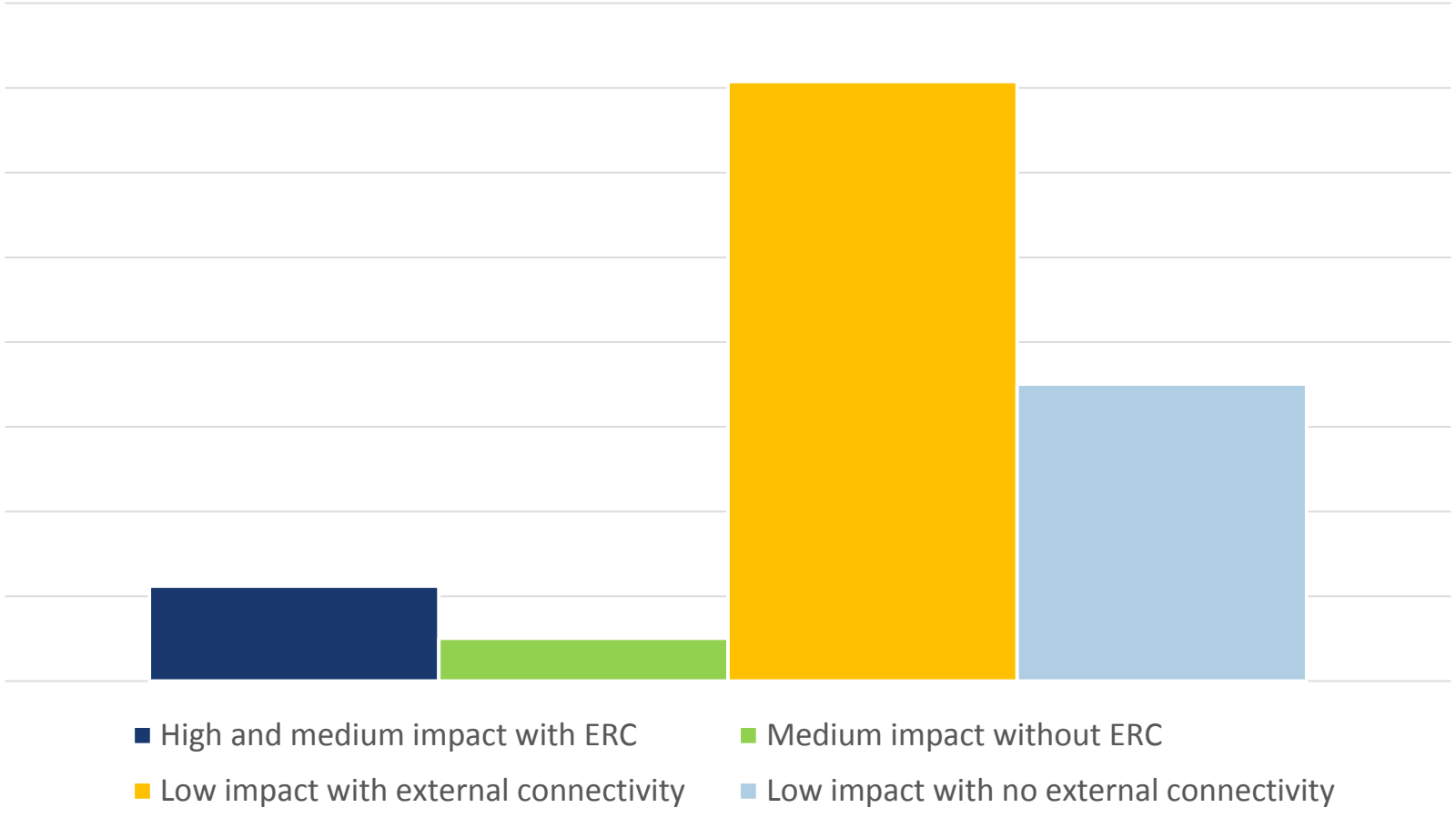
- Include in Supply Chain Standards
  - Electronic access controls for medium and high impact BES Cyber Systems
  - Physical access controls for medium and high impact BES Cyber Systems
- Do not include in Supply Chain Standards
  - Electronic access monitoring and logging
  - Physical access monitoring and logging
  - Protected Cyber Assets
- **Collect more data on low impact BES Cyber Systems**
- Develop guidelines with CIPC Supply Chain Working Group
  - Application to lows
  - Evaluation of PCAs

Data Request Issued

- Issued on August 19
- Responses due October 3
- Applicable to entities in CIP-002-5.1a
- Focused on low impact BES

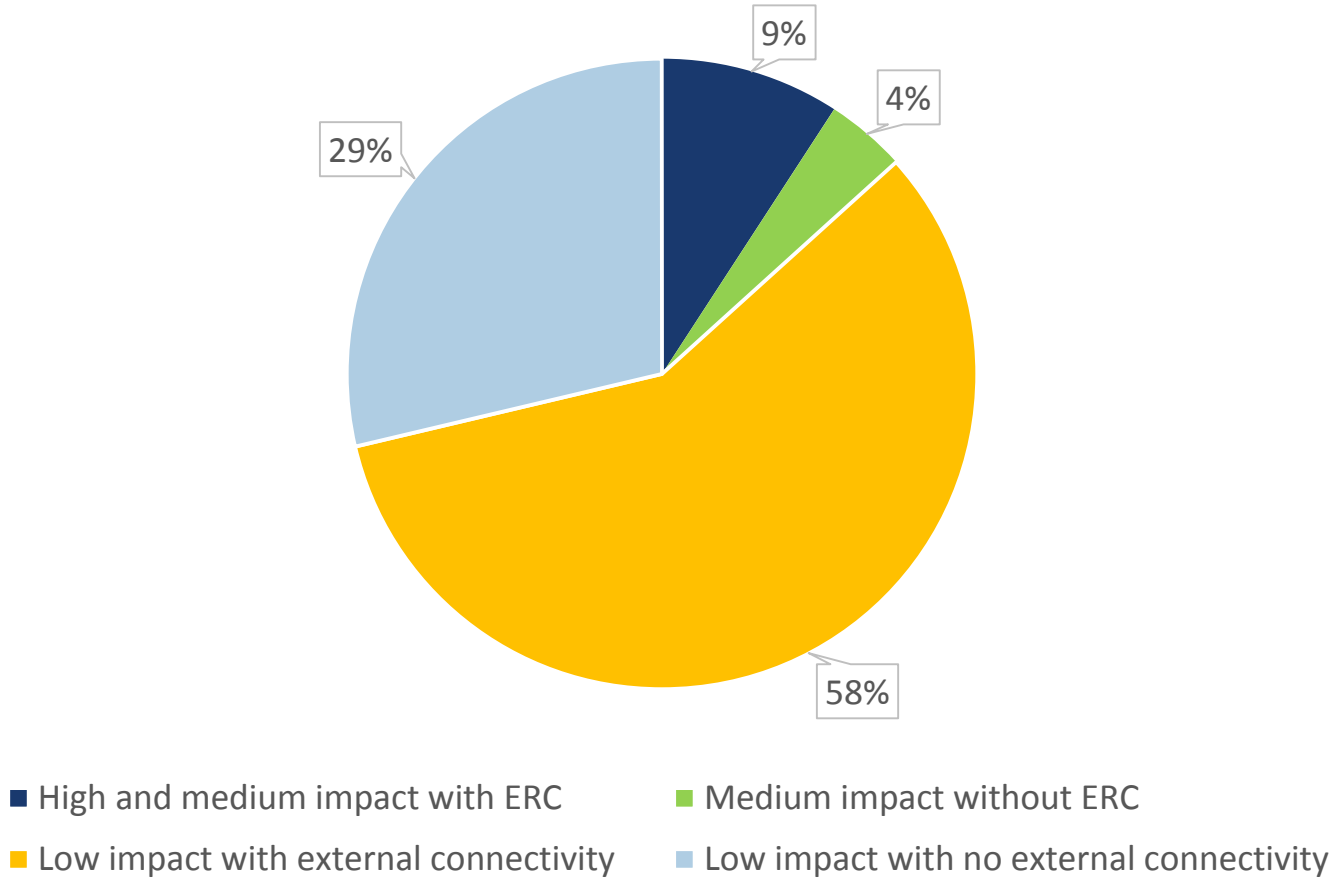
BES Cyber Assets

Assets containing BES Cyber Systems

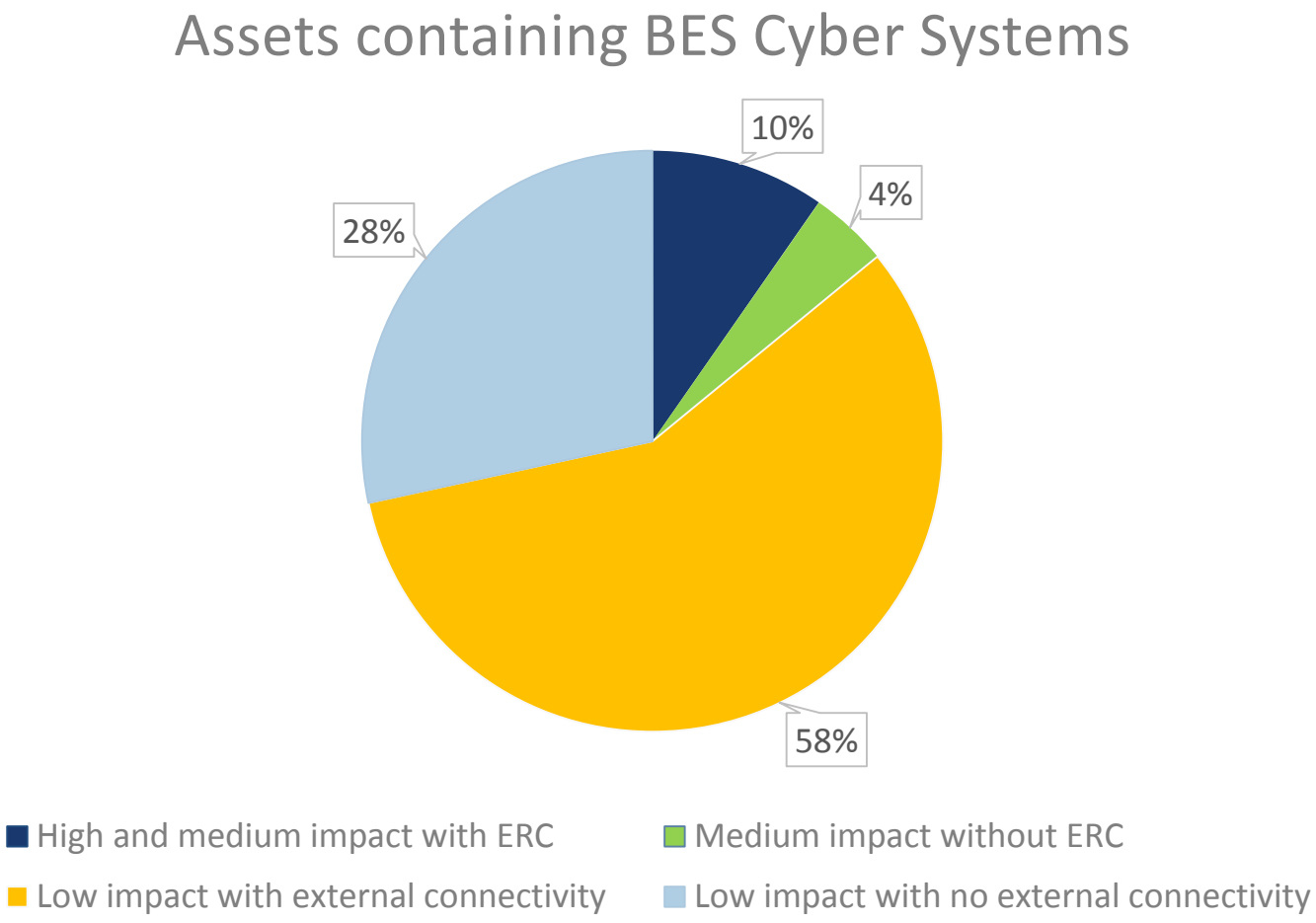


BES Cyber Assets

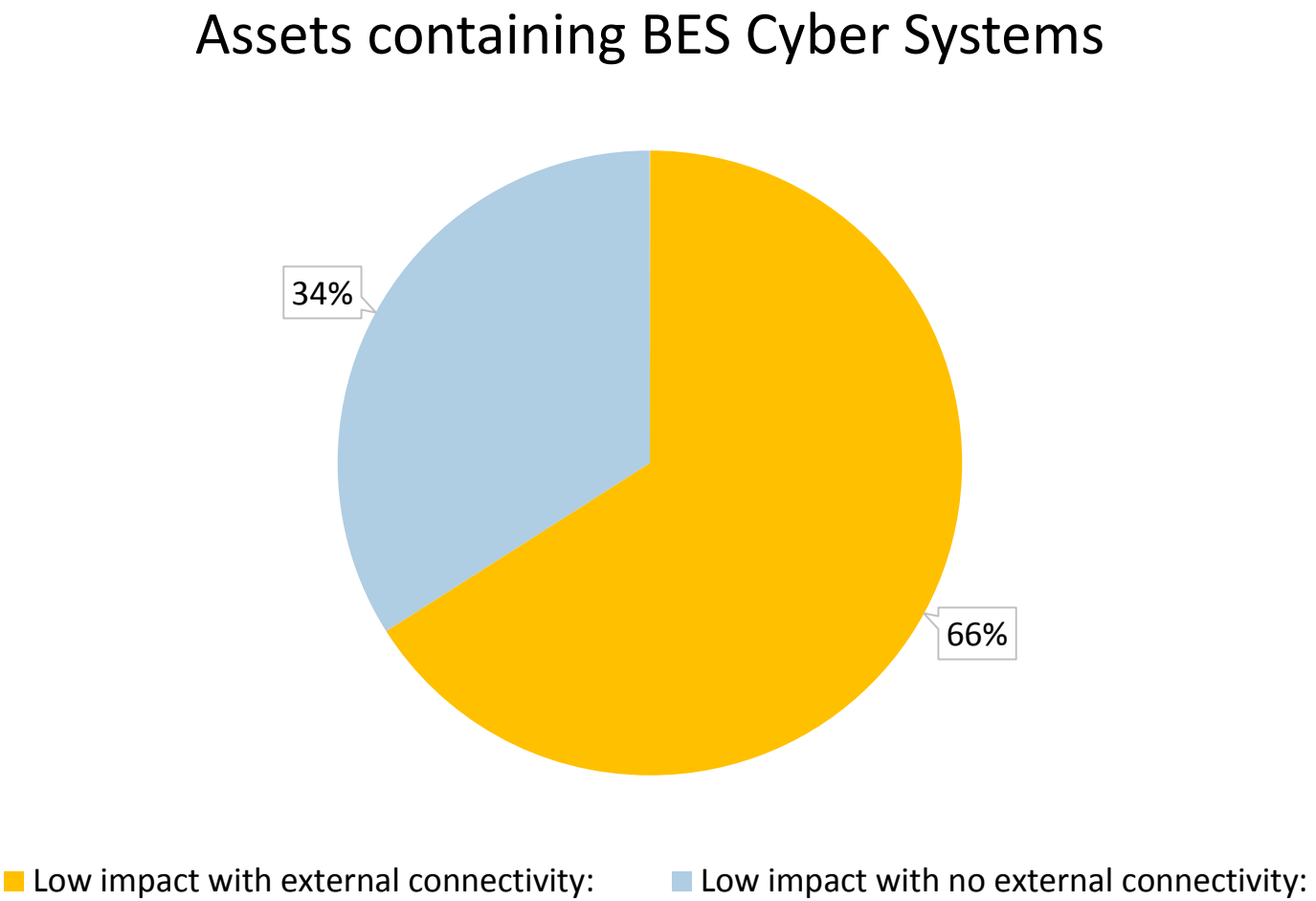
Assets containing BES Cyber Systems



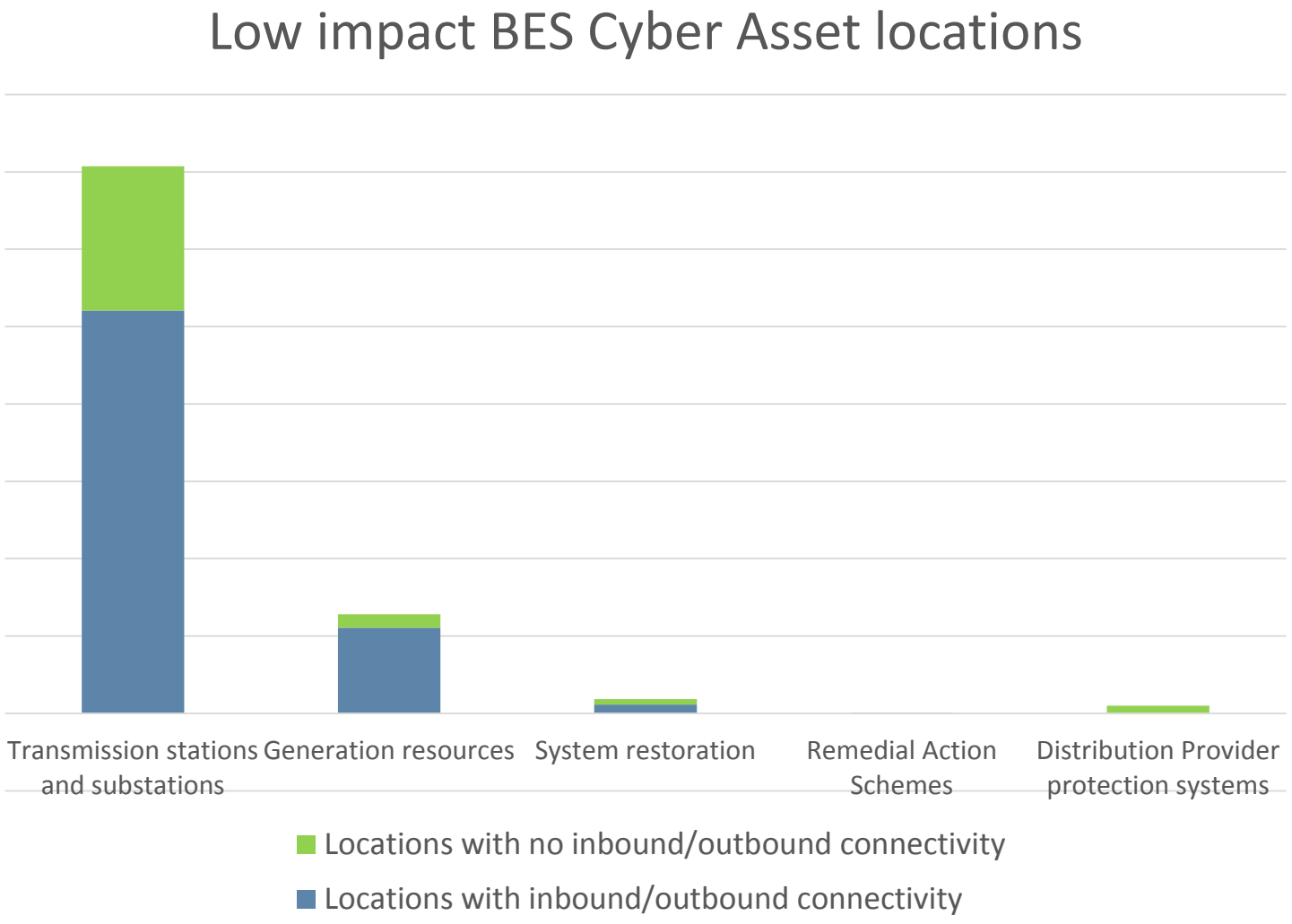
BES Cyber Assets with medium and high



BES Cyber Assets with lows only

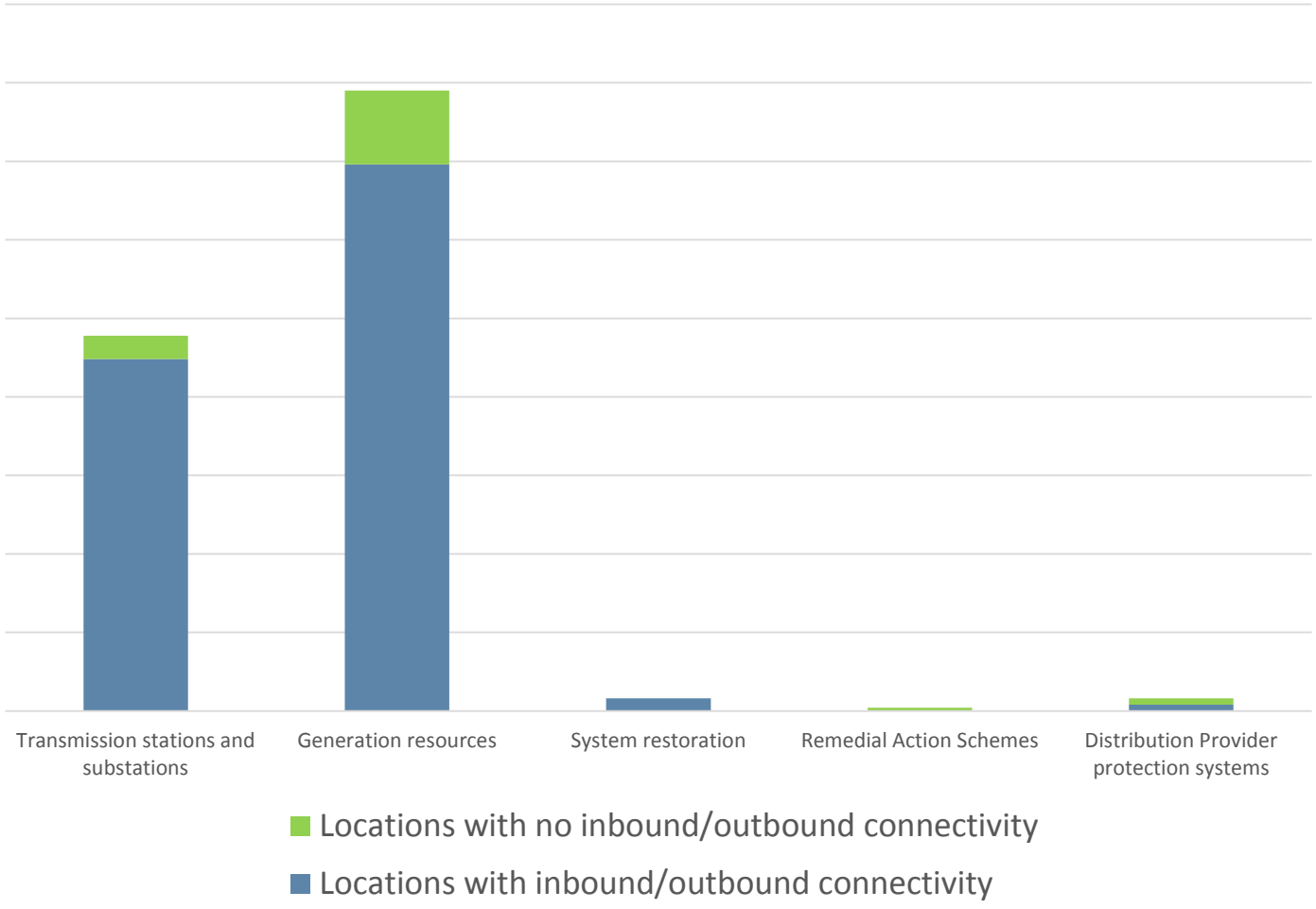


BES Cyber Assets with medium and high

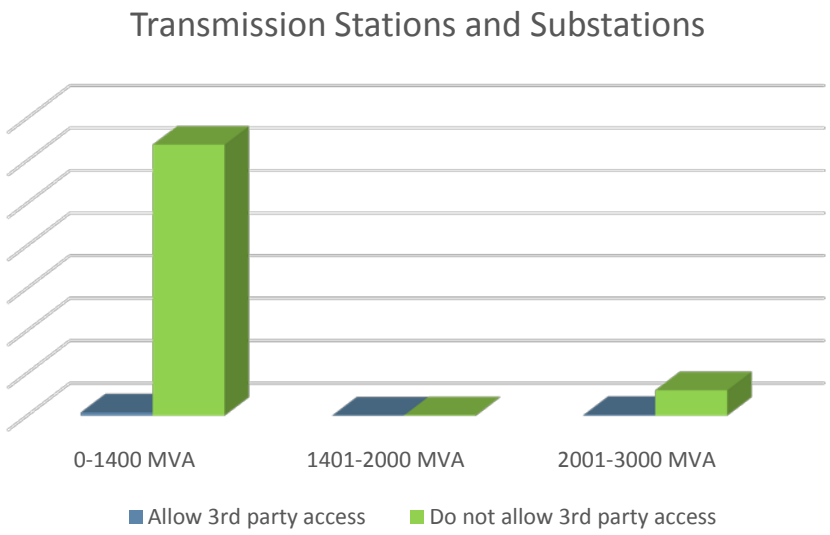


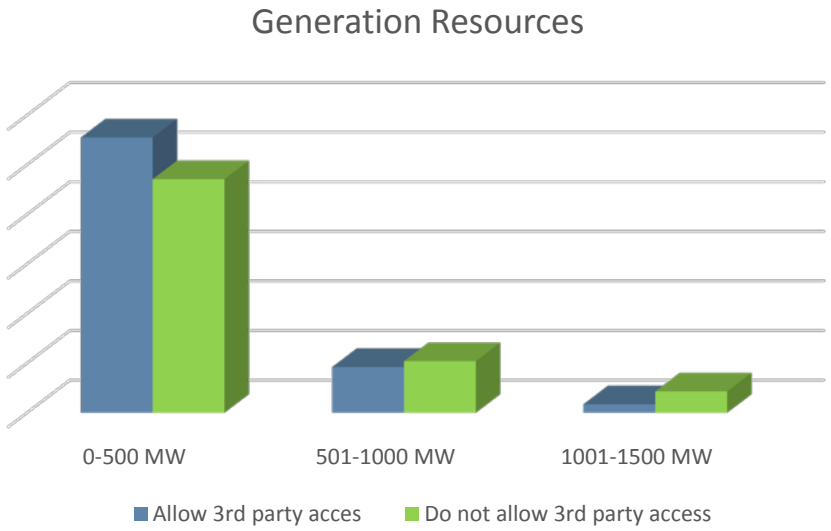
BES Cyber Assets with lows only

Low impact BES Cyber Asset locations

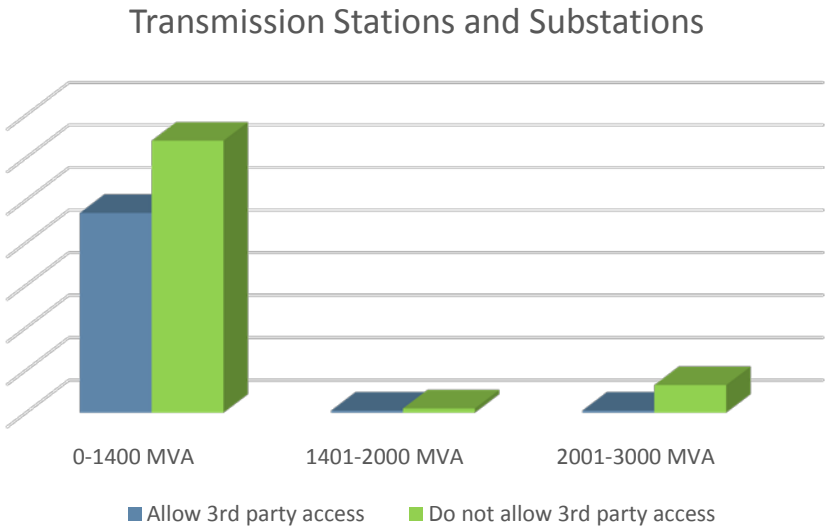


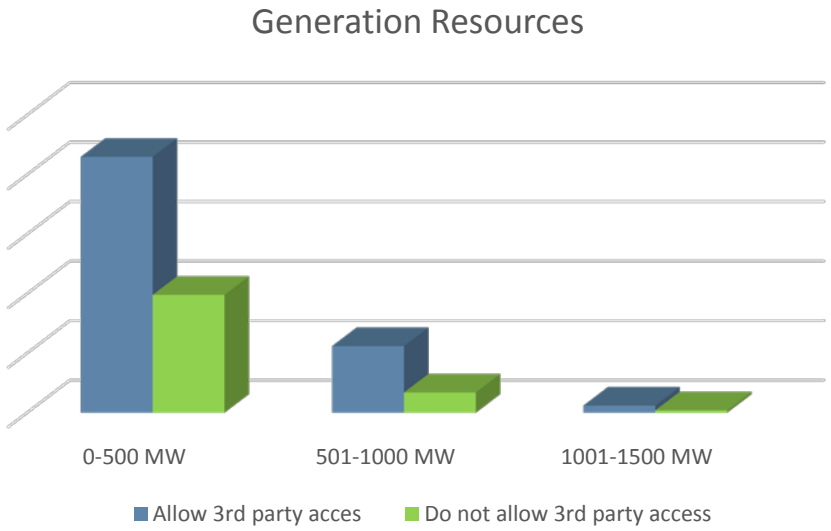
BES Cyber Assets with medium and high





BES Cyber Assets with lows only





Observations

- Most low impact assets reside in organizations with higher impact assets
- Most low impact assets are lower risk
- Significant percentage of generation resources allow third party access
- Significant percentage of “low only” transmission stations and substations allow third party access

Questions and Answers