NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Guideline for the Electricity Sector - Supply Chain

Procurement Language (DRAFT)

Dan Wagner, CISSP, CISA, CRISC
April 27, 2020

RELIABILITY | RESILIENCE | SECURITY




Introduction

- **Introduction**
  - A core measurement of any Supply Chain Cyber Security ***Risk Management Program*** is its value in reducing risk through controls employed by vendors, service providers, and the entities.
    - Regulators have challenged the levels of rigor regarding risk management practices that organizations claim to have attained. The inclusion of targeted controls provided by procurement language during the acquisition of cyber systems, components, maintenance and related services support a "risk-based" approach to cybersecurity.

NIST Cybersecurity Framework

Established with a 2013 executive order issued by President Obama

- Voluntary development of a risk-based cybersecurity framework
- Goal of improving critical infrastructure cybersecurity
- Apply the principles and best practices of risk management
- Improving the security and resilience of critical infrastructure

*Above is taken directly from NIST


NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Announcement

Workforce, Supply Chain Disruptions Key Elements in Ongoing Pandemic Preparations

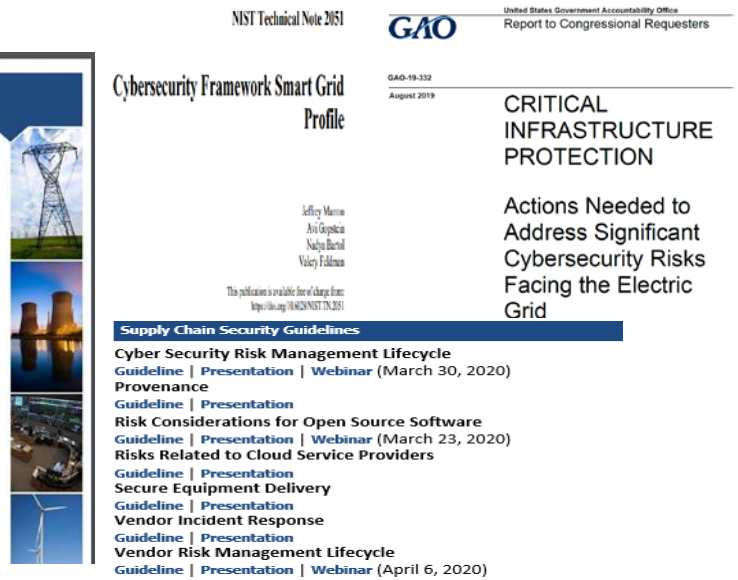
April 23, 2020

ATLANTA – Potential workforce disruptions, supply chain interruptions and increased cyber security threats caused by COVID-19 have elevated the electric industry's reliability risk profile. NERC's special report – *Pandemic Preparedness and Operational Assessment – Spring 2020* – reviews reliability considerations and operational preparedness during this pandemic. The pandemic introduces significant uncertainty that is without precedent and highly challenging even for the most prepared of industries. However, industry is rising to the challenge, coordinating effectively with government partners and taking aggressive steps to confront these threats to grid reliability.

Currently, NERC has not identified any specific threat or degradation to the reliable operation of the bulk power system. However, as pandemic mitigation and containment strategies continue, prolonged periods of operator sequestration and deferred equipment maintenance increase industry's risk profile and could exacerbate impacts to the bulk power system during the summer months, and potentially over the longer-term horizon.

"Industry appears well-positioned for spring operations and is currently preparing for the summer period, which we will focus on in our upcoming *Summer Reliability Assessment* next month," said John Moura, director of Reliability Assessment and Performance Analysis. "While we have not identified any specific threat to the reliable operation of grid, we are in unprecedented territory and must continue to be prepared for the cumulative unknowns that are increasing industry's risk profile."

The Electric Reliability Organization (ERO) Enterprise, which is comprised of NERC and the six Regional Entities, is coordinating with registered entities, regulators and government officials to assure the reliability of the bulk power system during this challenging time. As the pandemic unfolds, the ERO Enterprise is pursuing all available avenues to continue this coordination and identify reliability implications


NIST Technical Note 2051

Cybersecurity Framework Smart Grid Profile

Jeffrey Marron
Avi Gopstein
Nadya Bartol
Valery Feldman

This publication is available free of charge from: https://doi.org/10.6028/NIST.TN.2051

GAO

United States Government Accountability Office
Report to Congressional Requesters

GAO-19-332
August 2019

CRITICAL INFRASTRUCTURE PROTECTION

Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid

Supply Chain Security Guidelines

Cyber Security Risk Management Lifecycle
Guideline | Presentation | Webinar (March 30, 2020)
Provenance
Guideline | Presentation
Risk Considerations for Open Source Software
Guideline | Presentation | Webinar (March 23, 2020)
Risks Related to Cloud Service Providers
Guideline | Presentation
Secure Equipment Delivery
Guideline | Presentation
Vendor Incident Response
Guideline | Presentation
Vendor Risk Management Lifecycle
Guideline | Presentation | Webinar (April 6, 2020)

Introduction

IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	· **CIS CSC** 4 · **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 · **ISA 62443-2-1:2009** 4.3.4.2 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	· **COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 · **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	· **COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 · **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 · **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	· **COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 · **ISA 62443-2-1:2009** 4.3.2.6.7 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	· **CIS CSC** 19, 20 · **COBIT 5** DSS04.04 · **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 · **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 · **ISO/IEC 27001:2013** A.17.1.3 · **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9

- **Introduction**
  - Procurement language, beginning at the planning stage and at each step of an acquisition, is a critical element of a Supply Chain Cyber Security Risk Management Program.
    - *Procurement language* includes negotiated agreements that formalize the division of responsibilities, performance requirements, and expectations for compliance monitoring.
    - *Procurement language** is expressed in the form of contract clauses developed during the procurement of industrial control system hardware, software, and computing and networking services associated with bulk electric system operations.

Risk Identification

- **Risk Identification and Assessment**
  - NERC entity Supply Chain Cyber Security Risk Management Program efforts begin by identifying important risks to the cyber security of the bulk electric system (BES) supply chain
    - A thorough understanding of the risks associated with vendor relationships to critical cyber systems and particularly BES cyber systems, determines the type and quantity of conditions and stipulations appropriate to include in the procurement language to achieve security and reliability goals. The risk assessment should include an analysis of likelihood and magnitude of harm and consider threats, vulnerabilities, and impact to organizational operations and assets, individuals, and the BES.

- **Risk Identification and Assessment**
  - Procurement language within contracts is one among several means at an entity's disposal to formalize risk mitigation for the relationship between the vendor, service provider and the entity. ***Let's Consider:***
    - Acceptance or transfer of risk as it relates to a third party which may carry specific liability and should be authorized by the CIP Senior Manager or other similarly senior manager or executive with a solid understanding of the ramifications of these decisions.
    - Procurement language should also enable the audit mechanisms and metrics necessary for an entity to ensure their vendors are meeting the contractual requirements and changes related to industry risks.
    - Procurement contracts should be treated as living documents that need to be reviewed and updated regularly to ensure entities are continually identifying, assessing, and mitigating residual and new risks posed by the vendors.

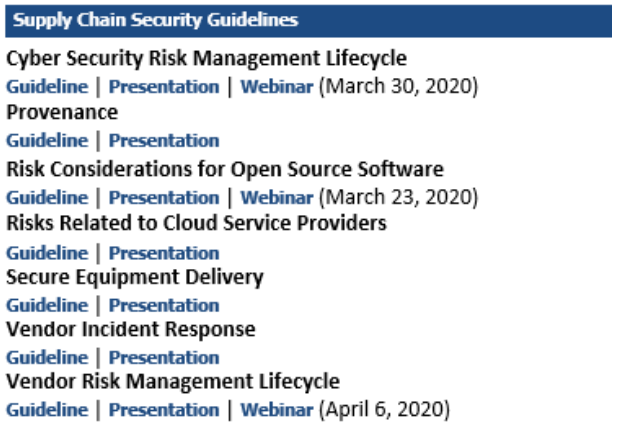
Procurement Language

- **Procurement Language Examples**
  - Critical Infrastructure Protection Committee (CIPC/RSTC) on March 6th 2019 released a 'Letter to the Electric Industry Vendor Community', in that letter CIPC encouraged product and service vendors to provide several reasonable controls.

    Examples of supply chain cyber security risks and procurement language considerations include:
    - **Energy Sector Control Systems Working Group (ESCSWG)**
    - **Utilities Technology Council (UTC)**
    - **Edison Electric Institute (EEI)**
    - **National Institute of Standards and Technology (NIST)**

Additional Information Sources

- **CIPC approved guideline / letter to industry**
- **North American Transmission Forum (NATF)**
- **North American Generator Forum (NAGF)**
- **NERC Frequently Asked Questions Supply Chain**



Non-Contractual Purchases

- **Non-Contractual Purchases**
  - Non-contractual purchases should be documented, assessed for risk, and include steps taken to mitigate identified risks. ***Let's Consider:***
    - Purchases, made without a contract, perhaps in response to an emergency to obtain something quickly, pose risks and lack formal oversight.
    - In some cases, the means of acquisition may affect the support that the entity will receive from the equipment manufacturer, or may impose additional requirements to obtain support, thereby requiring additional steps to mitigate risk. Consider, for instance, the risk of ***using credit cards*** without the protections of procurement language.
    - The registered entity should document the emergency procurement process in a Supply Chain Risk Management (SCRM) procurement plan, along with documentation that registered entity personnel or approved contractors validate after-the-fact risks and mitigations of the procurement.

Context

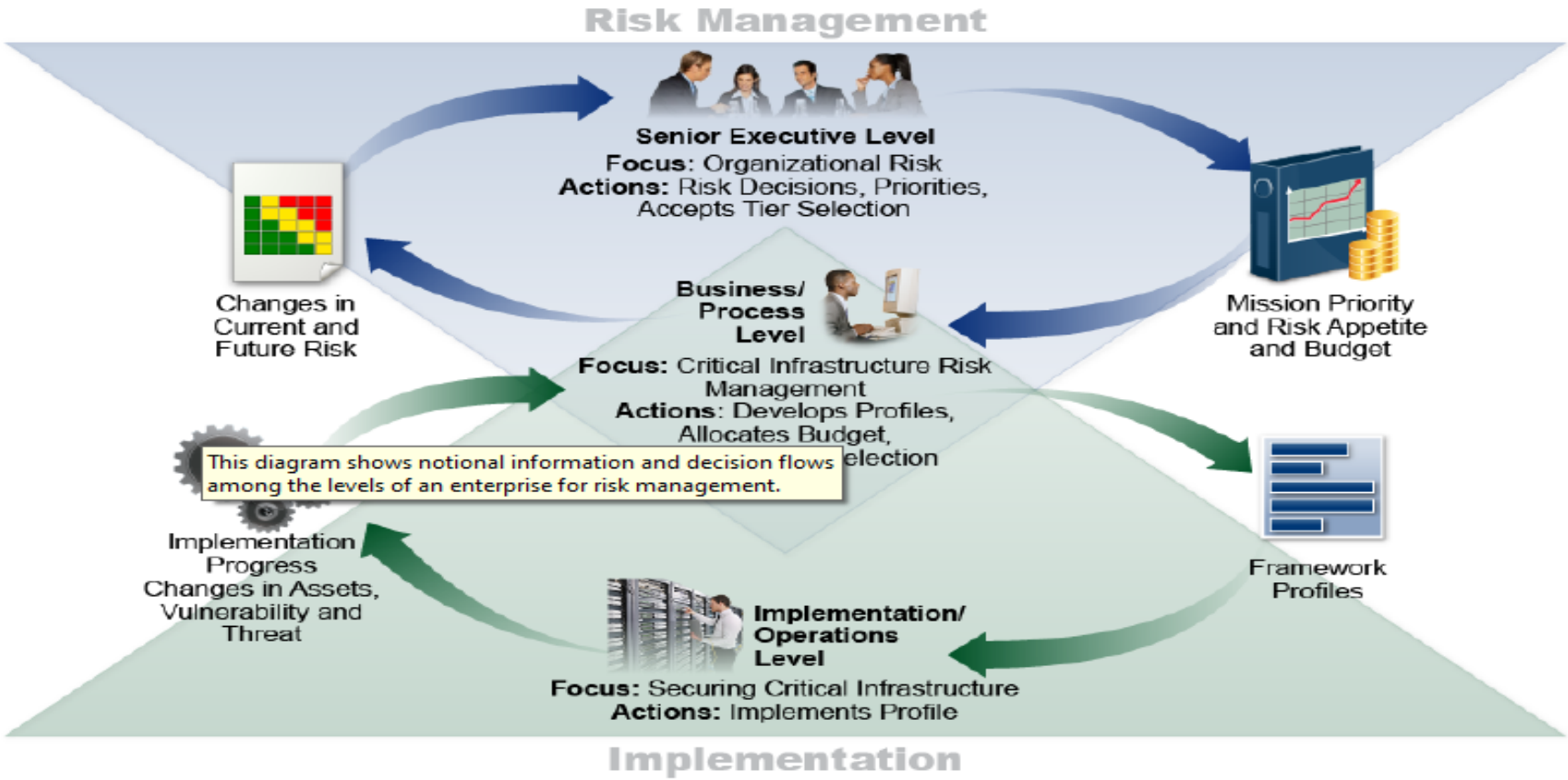
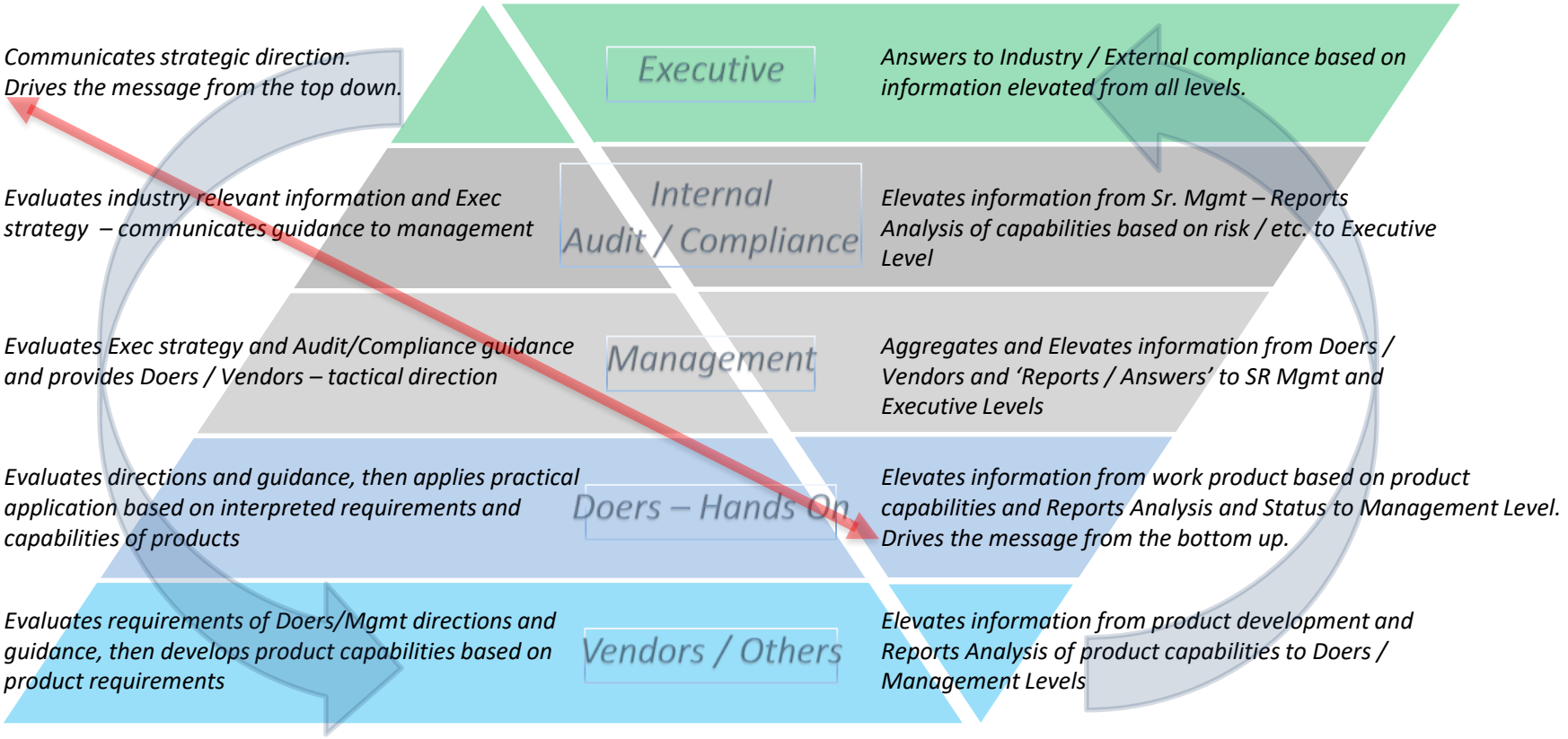


Figure 7: Notional Information and Decision Flows Diagram from NIST Cybersecurity Framework

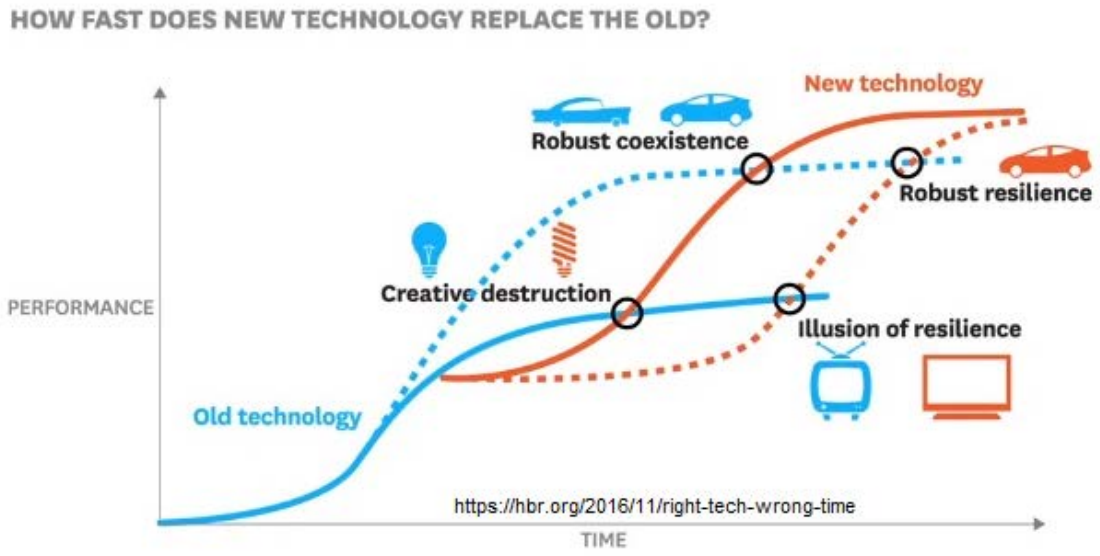
Closing

Context



Closing

- **Closing**
  - The most effective Supply Chain Cyber Security Risk Management Program will prioritize a risk-based and tiered approach to mitigating security threats. Clear communication and expectations between vendors, service providers and entities will result in procurement language that supports entity and industry security controls requirements.



Questions and Answers

Send Questions about the supply chain security guidelines to SCWGWebinars@nerc.net