



Supply Chain Security Efforts by Other Federal Agencies

Simon Slobodnik

Supply Chain Risk Management (SCRM)
Technical Conference

January 28, 2016


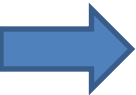
Introduction

- Notice of Proposed Rulemaking (NOPR) – Revised Critical Infrastructure Protection Reliability Standards – July 16, 2015
- Proposed to direct NERC “to develop a new or modified Reliability Standard to provide security controls for supply chain management...”

Office of Management and Budget

- Draft Guidance - Improving Cybersecurity Protections in Federal Acquisitions
 - Guidance applies to information collected or maintained by or on behalf of an agency.

Office of Management and Budget Proposed Guidance

- NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations
 - applies to Government systems maintained by contractors
 - NIST SP 800-171 - Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations
 - applies to contractor's own systems
- Security Controls
 - Cyber Incident Reporting
 - Information System Security Assessments
 - Continuous Monitoring
 - Business Due Diligence

Department of Defense Interim Rule

- Interim Rule amending acquisition regulations
 - Implements sections of NDAA FY2013 and FY2015
 - Requires contractors and subcontractors to report on network penetrations
 - Incorporates security controls from NIST 800-171
 - Establishes policies when contracting for cloud computing services
- Interim Rule works in conjunction with DoD Instruction 8500.01 on Cybersecurity, March 14, 2014
 - Outlines policy on vulnerabilities inherent in IT, global sourcing, and distribution
 - Risk Management of IT acquisition

Department of Defense

Applicable Guidance to SCRM

- Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services, December 2014
- DoD Cloud Computing Security Requirements Guide, January 12, 2015
- DoD Instruction 5200.44 “Protection of Mission Critical Functions to Achieve Trusted Systems and Networks”, November 5, 2012

Trusted Systems and Networks (DoD)

- DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks
 - Reduce Vulnerabilities in the System Design through System Security Engineering
 - Quality, Configuration, Security Control of software, firmware, hardware and systems throughout lifecycles
 - Component Supply Chain Risk Management
 - Detection, Likelihood reduction and Mitigation of Counterfeit and Malicious components
 - Vulnerability detection in custom hardware
 - Tailored acquisition methods for Critical Components
 - National level Traceability for Critical Components via Item Unique Identification (IUID)

Department of Energy (DOE)

- Cyber Security Procurement Language for Control Systems - 2009
- Cybersecurity for Energy Delivery Systems - 2011
- Cybersecurity Procurement Language for Energy Delivery Systems - 2014

DOE/NIST/NERC Cybersecurity Procurement Language for Energy Delivery Systems

- Baseline Cybersecurity Procurement Language
 - Access control, Account management, Session management, Authentication, Logging, Malware detection
- Product Life Cycle Security Program
 - Design, Development, Manufacture, Storage, Delivery, Implementation, Maintenance, Disposal

Office of Comptroller of the Currency

Bulletin 2013-29

- Guidance on Risk associated with Third-Party Relationships
 - Contractor's experience in Identifying, Assessing, and Mitigating known and emerging risks
 - Assess contractor's infrastructure and application security programs including Software Development Lifecycle, and Vulnerability and Penetration test results
 - Assess ability to implement Effective and Sustainable Corrective Action

Federal Financial Institutions Examination Council – Cybersecurity Assessment Tool

- External Dependency Management, Baseline Level
 - Risk-based Due Diligence
 - Independent party Validation of contractor’s controls
 - Identify responsibility for Security Incident Response
- Evolving Maturity Level
 - Critical Business Processes mapped to Supporting External Connections
 - Security incident notification Responsibility documented in contract
 - Third Parties monitored based on their Risk
- Advanced Maturity Level
 - Annual audits of high-risk vendors
 - Security policies meet or exceed those of the Institution
 - Confidential Data Access actively tracked

Summary

Highlighted programs could be used to inform or help guide the development of a new or modified Reliability Standard to provide security controls for supply chain management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations.