280 - SUPPLY CHAIN RISK MANAGEMENT STANDARD

Purpose

The Supply Chain Risk Management Standard provides documentation of the requirements to achieve compliance with the Supply Chain Risk Management Policy.

Standard

This standard uses the NIST SP 800-53 Rev. 5 framework as the guideline to establish control objectives to address a diverse set of security and privacy requirements. Not all controls within NIST SP 800-53 Rev. 5 may be selected for the Statewide baseline policies and standards. Agencies must classify their data and identify the potential impact (high, moderate, or low), and select controls appropriately. This standard uses Table 3-1 in NIST SP 800-53B for the allocated impact levels (high, moderate, low) of controls and control enhancements. At a minimum, all low controls are selected, and certain moderate controls are selected. Agencies are to reflect their controls through the annual reporting process to DOA-DET.

Executive Branch Agencies are to develop policies, procedures, or processes for their own State information systems and system environments to protect State information, as required. Implementation of the standard controls within this document can be (1) a common (inheritable) control, (2) a system-specific control, or (3) a hybrid control. The control implementation defines the scope of applicability for the control, the shared nature or inheritability of the control, and the responsibility for control development, implementation, assessment, and authorization.

Agencies have defined appropriations under Wisconsin Chapter 20 that determines what they are funded to do. Agencies can define controls where they have clearly been appropriated funds to do this function. Agencies should consider the following for inclusion in their policies, procedures, or processes:

Supply Chain Risk Management Plan (SR-2):

- Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: Agency-defined systems, system components, or system services;
- Review and update the supply chain risk management plan on an Agency-defined frequency or as required, to address threat, organizational or environmental changes; and
- Protect the supply chain risk management plan from unauthorized disclosure and modification.

Supply Chain Risk Management Plan | Establish SCRM Team (SR-2(1)):

- Establish a supply chain risk management team consisting of *Agency-defined* personnel, roles, and responsibilities to lead and support the following SCRM activities: Agency-defined supply chain risk management activities.

Supply Chain Controls and Processes (SR-3):

- Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of Agency-defined system or system component in coordination with Agency-defined supply chain controls; and
- Employ Agency-defined supply chain controls against supply chain risks to the system, system component, or system service to limit the harm or consequences from supply chain-related events.
- Document the selected and implemented supply chain processes and controls in [Selection: security and privacy plans; supply chain risk management plan; Agency-defined document].

Supply Chain Controls and Processes | Diverse Supply Base (SR-3(1)):

- Employ a diverse set of sources for Agency-defined system components and services.

Supply Chain Protection Controls and Processes | Limitation of Harm (SR-3(2)):

- Employ Agency-defined controls to limit harm from potential adversaries identifying and targeting the organizational supply chain.

Provenance (SR-4):

- Document, monitor, and maintain valid provenance of the Agency-defined systems, system components, and associated data.

Provenance | Identity (SR-4(1)):

- Establish and maintain unique identification of Agency-defined supply chain elements, processes, and personnel associated with Agency-defined systems and critical system components.

Provenance| Track and Trace (SR-4(2)):

- Establish and maintain unique identification of Agency-defined systems and critical system components for tracking through the supply chain.

Provenance | Validate as Genuine and Not Altered (SR-4(3)):

- Employ Agency-defined controls to validate that the system or system component received is genuine and has not been altered.

Provenance | Supply Chain Integrity - Pedigree (SR-4(4)):

- Employ Agency-defined controls and conduct Agency-defined analysis to ensure the integrity of the system and system components by validating the internal composition and provenance of critical or mission-essential technologies, products, and services.

Acquisition Strategies, Tools, and Methods (SR-5):

- Employ Agency-defined acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks.

Acquisition Strategies, Tools, and Methods | Adequate Supply (SR-5(1)):

- Employ Agency-defined controls to ensure an adequate supply of Agency-defined critical system components.

Acquisition Strategies, Tools, and Methods | Assessments Prior to Selection, Acceptance, Modification, or Update (SR-5(2)):

- Assess the system, system component, or system service prior to selection, acceptance, modification, or update.

Supplier Assessments and Reviews (SR-6):

- On an Agency-defined frequency, assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide.

Supplier Assessments and Reviews | Testing and Analysis (SR-6(1)):

- Employ [*Selection* (one or more): organizational analysis, independent third-party analysis, organizational testing, independent third-party testing] of Agency-defined supply chain elements, processes, and actors associated with the system, system component, or system service.

Supply Chain Operations Security (SR-7):

- Employ Agency-defined Operations Security controls to protect supply chain-related information for the system, system component, or system service.

Notification Agreements (SR-8):

- Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [*Selection* (one or more): notification of supply chain compromises; results of assessments or audits] of Agency-defined information.

Tamper Resistance and Detection (SR-9):

- Implement a tamper protection program for the system, system component, or system service.

Tamper Resistance and Detection | Multiple Stages of System Development Life Cycle (SR-9(1)):

- Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle.

Inspection of Systems or Components (SR-10):

- Inspect Agency-defined systems or system components [Selection (one or more): at random; at an Agency-defined frequency, upon Agency-defined indications of need for inspection] to detect tampering.

Component Authenticity (SR-11):

- Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and
- Report counterfeit system components to [Selection (one or more): source of counterfeit component; Agency-defined external reporting organizations; Agency-defined personnel or roles].

Component Authenticity | Anti-Counterfeit Training (SR-11(1)):

- Train Agency-defined personnel or roles to detect counterfeit system components (including hardware, software, and firmware).

Component Authenticity | Configuration Control for Component Service and Repair (SR-11(2)):

- Maintain configuration control over Agency-defined system components awaiting service or repair and serviced and repaired components awaiting return to service.

Component Authenticity | Anti-Counterfeit Scanning (SR-11(3)):

- Scan for counterfeit system components on an Agency-defined frequency.

Component Disposal (SR-12):

- Dispose of Agency-defined data, documentation, tools, or system components using Agency-defined techniques and methods.

Additional Documentation

- Wisconsin Chapter 20 https://docs.legis.wisconsin.gov/document/statutes/20.505(1)(kL)

  "All moneys received for the provision of document sales services and services under ss. 16.971, 16.972, 16.973, 16.974 (3), and 16.997 (2) (d), other than moneys received and disbursed under par. (ip) and s. 20.225 (1) (kb), shall be credited to this appropriation account."

- Wisconsin Chapter 16.971(2) https://docs.legis.wisconsin.gov/statutes/statutes/16/vii/971
  The Department shall:

  (cm) Prescribe standards for data, application, and business process integration that shall be used by executive branch agencies, to the extent consistent with the statewide strategic plan formulated under par. (m), and that enable local governmental units to integrate their data, application, and business processes into state systems whenever feasible.

  (d) Develop review and approval procedures which encourage timely and cost-effective hardware, software, and professional services acquisitions, and review and approve the acquisition of such items and services under those procedures.

Definitions

Executive Branch Agency - State of Wisconsin legislatively defined Departments and all customers of DET services, equipment, and/or technologies.

State information - Any information/data that is created, accessed, used, stored, or transmitted by an Executive Branch Agency.

State information systems and system environments - All equipment or services used to input, store, process, transmit, and output information, including, but not limited to: network devices, servers, databases, printers, Internet, email, physical, virtual, cloud, and applications accessible to and/or managed by the agency.

Exception Process

Exceptions to any Executive Branch Agencies Security Policies, Procedures or Standards must follow the Executive Branch Agencies Exception Procedure.

Document History and Ownership

This standard was developed as required by the State of Wisconsin Information Technology Security Policy Handbook, under the authority of Wisconsin State Statute 16.971.

This standard is effective upon approval and publication until revised, updated, or retired.

Ownership for this standard is assigned to DOA, DET Bureau of Security. As such, the DOA, DET Bureau of Security is responsible for the maintenance, update(s), and review of this document annually before the anniversary of the effective date.

Version #	Revision or Review Date	Description of Change(s)	Reviewer/Author	Date Approved
1.0	06/24/22	Submitted to and approved by the IT Executive Steering Committee	Reviewer: ITESC Author: DOA/DET	06/24/22
2.0	06/24/22	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: ITESC Author: DOA/DET	06/24/22
NOTE: Keep only the origination and the last 10 years of update information. Only notate prior three revisions. Include only interim/final revision statuses.				

Authorized and Approved by:

Alan Greenberg, CISO

DocuSigned by:
Alan Greenberg
7062227F849B429...

7/8/2022 | 1:55 PM CDT

Print/Type
Title

Signature

Date

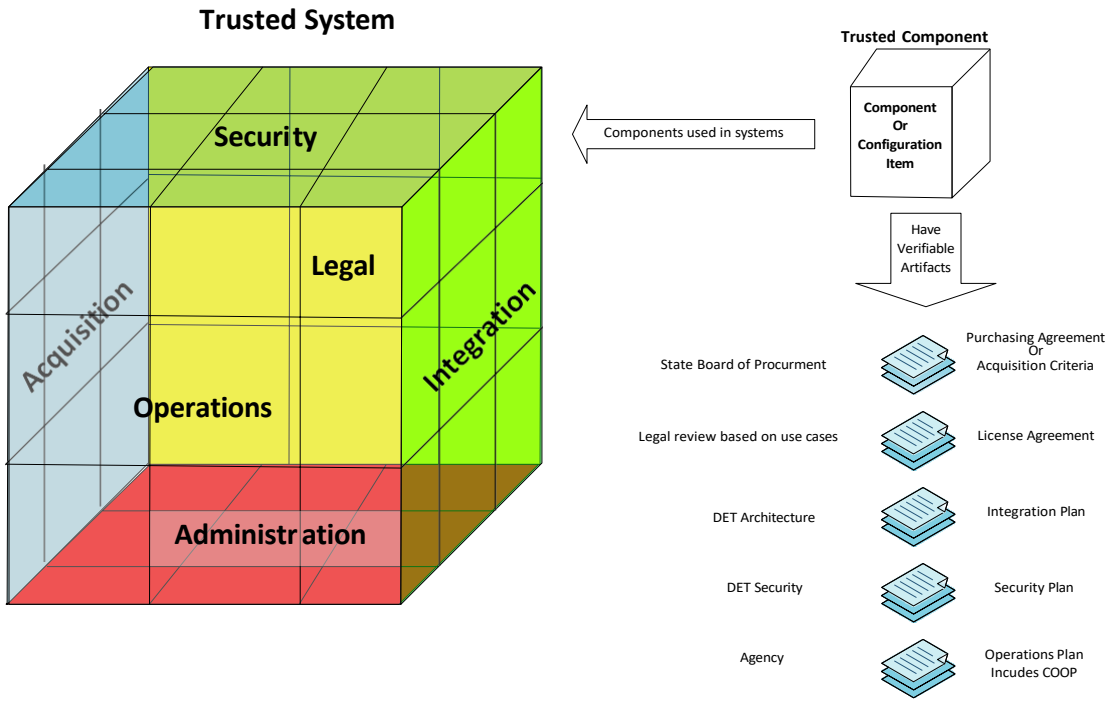
Appendix A

Additional information for Executive Branch agencies to consider regarding supply chain.

When looking at the supply chain we are talking about the ***acquisitions*** of components (Products and Services) that will be ***integrated*** together to develop systems that handle data.

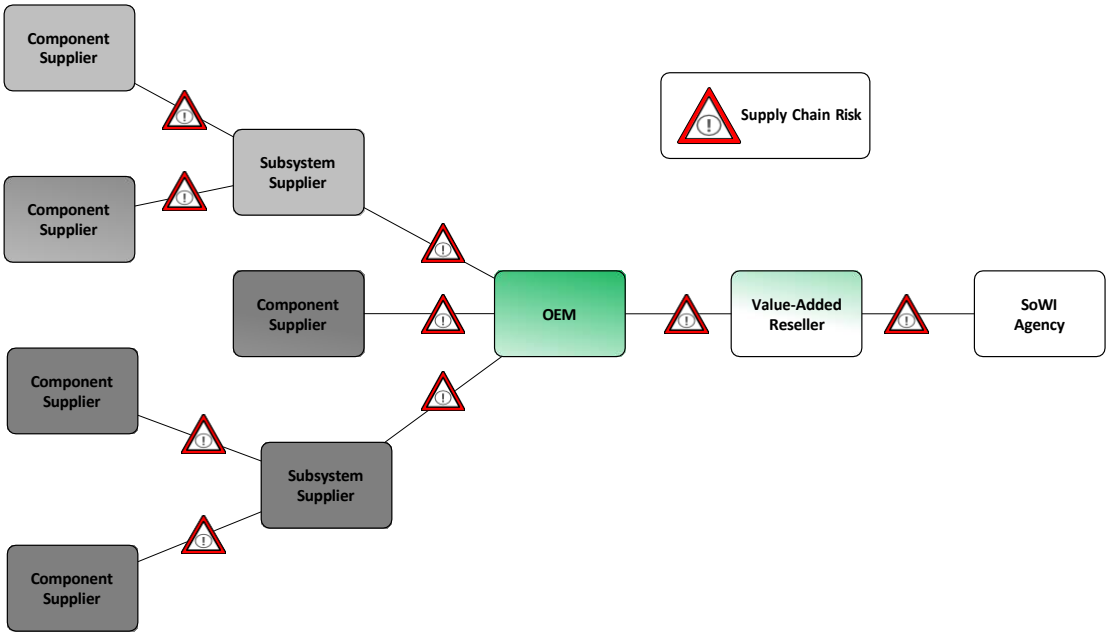
Not all controls are technical. Legal, Acquisition (Procurement), IT security, operations, and integration (compatibility) all have weight in the process. Trusted systems are made from trusted components. Each component must have verifiable artifacts that each area above defines as "Good". These would be used to "test" the components at every supplier to ensure trust throughout the entire system end to end.

The Goal of supply chain management is to build and maintain trusted systems. This is illustrated in the below diagrams.

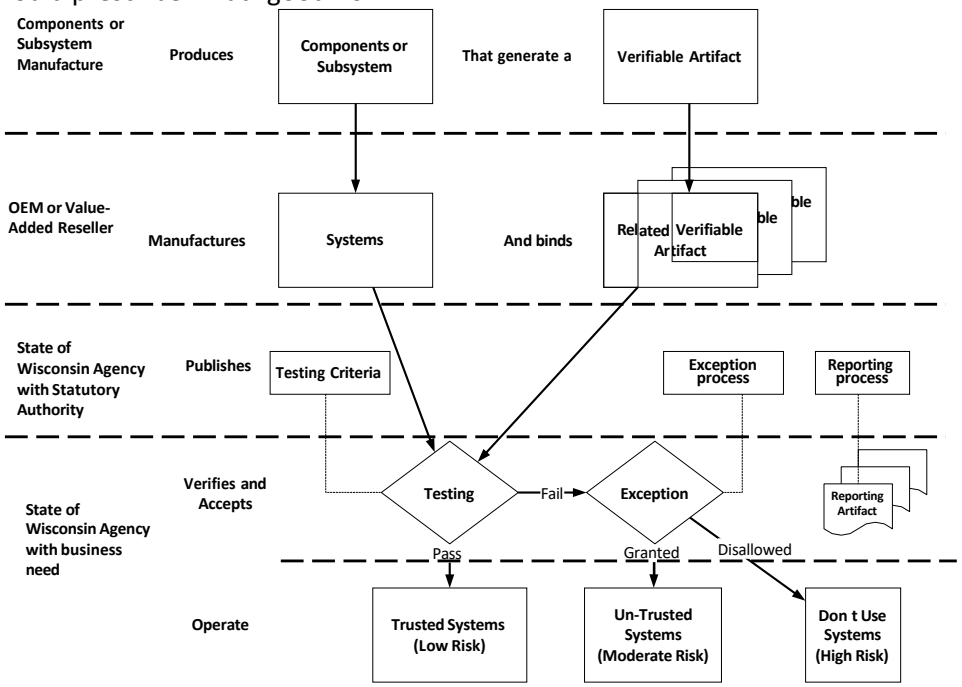


Where there are gaps (exceptions) in verifiable artifacts, a procedure will need to be defined on how these are handled.

Here is a typical supply chain:



Testing criteria should prescribe what “good” is



It is recommended that all components and services use the NIST Official Common Platform Enumeration (CPE) Dictionary or CPE naming format for identification of components and services across the enterprise and in any artifacts generated. This would be used to populate the Technology Reference Model (TRM) at both the Enterprise and Agency levels as well as to enable continuous testing against the National Vulnerability Database

by the enterprise and agency security programs.

As agencies test their systems, some will be found to be a Moderate or High risk. These will always require a Plan of Actions and Milestones (POAM) to move them into Low Risk.

It should also be noted that a components or systems often have a published lifetime, so annual testing (as per policy) at a minimum will need to be a documented part of the operations in their program management plan. Here is an example for a Cloud Service that integrates with DET services: