Supply Chain Cybersecurity Resources Guide

Purpose

This Supply Chain Cybersecurity Resources Guide provides access to resources that can assist with security activities specific to supply chain and third-party vendor processes. The following resources are either publicly available through various organizations, or are available as links within this guide, as donated from members of the Multi-State Information Sharing & Analysis Center (MS-ISAC) and the MS-ISAC Metrics Workgroup.

Center for Internet Security® (CIS®) and Department of Homeland Security (DHS) Resources

CIS Technology Procurement Guide: *A Guide for Ensuring Security in Election Technology Procurements*

Resource Link: "A Guide for Ensuring Security in Election Technology Procurements"

Reference Note

While the above item is elections-focused, its principles can apply to any organization.

Description

CIS developed this guide with input from state and local government, federal government, academic, and commercial stakeholders. It provides model procurement language that election officials can use to communicate their security priorities, better understand vendor security procedures, and facilitate a more precise cybersecurity dialogue with the private sector. This guide includes best practices that election offices can use for planning, developing, and executing procurements.

Supplementary Resource

For election offices, this guide can be utilized alongside the CIS "Security Best Practices for Non-Voting Election Technology Guide," located on the following page: https://www.cisecurity.org/elections-resources/.

Supply Chain Guidance from DHS Cybersecurity & Infrastructure Security Agency (CISA)

Resource Link: DHS CISA Supply Chain Risk Management Website

Description

The above link directs to the "Information and Communications Technology (ICT) Supply Chain Risk Management" page within the DHS CISA website. The page includes resources specific to the ICT supply chain, focusing on the security of hardware, software, and managed services from third-party vendors, suppliers, service providers, and contractors.

External Dependencies Management Assessment from DHS CISA

Resource Link: DHS CISA "Cyber Resource Hub"

Description

The above link directs to resources from DHS CISA, including the "External Dependencies Management (EDM) Assessment." This assessment is interview-based and measures an organization's risk management within the Information and Communications Technology (ICT) Supply Chain.

Policy/Contract Templates

Security RFP and Contract Language Template

Resource Link: Security RFP & Contract Language Template

Description

This template was donated by an MS-ISAC member organization, and it provides language utilized as part of security RFP and security contracting processes. Text highlighted in yellow has specific security or framework phrasing that could be edited, depending on the specific organization.

Vendor Acquisition and Selection Policy Template

Resource Link: Vendor Acquisition & Selection Policy Template

Description

This policy document was donated by an MS-ISAC member organization. It provides a baseline to assess the information security risk of prospective vendors/third parties/supply chain, to reduce the likelihood of risk associated with non-performing or non-compliant vendors.

Monitoring Vendor Performance and Compliance Policy Template

Resource Link: Monitoring Vendor Performance & Compliance Policy Template

Description

This document was donated by an MS-ISAC member organization. It defines the monitoring of vendor performance to help provide assurance that any third-party provided service is operating effectively without exposing the entity to security or compliance risks. This policy should align with right-to-audit clauses in contracts, but it is the responsibility of the entity to perform and monitor their third-party vendor performance periodically.

Additional Policy Templates (Donated MS-ISAC Member Anonymized Policy Templates)

- Computer Security Threat Response PolicyCyber Incident Response Standard
- Identification and Authentication Policy
- Incident Response Policy
- Security Assessment and Authorization Policy
- Systems and Services Acquisition Policy

Training & Guidance

NIST Key Practices in Cyber Supply Chain Risk Management: Observations from Industry

Resource Link: "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry"

Description	This document was created by the National Institute of Standards and Technology (NIST) and is Publication "NISTIR 8276." It includes a high-level summary of practices instrumental to an effective cyber supply chain risk management program.
NIST Abstract	In today's highly connected world, all organizations rely on other organizations for critical products and services. However, today's world of globalization, while providing many benefits, has resulted in a world where organizations no longer fully control—and often do not have full visibility into—the supply ecosystems of the products that they make or the services that they deliver. With more and more businesses becoming digital, producing digital products and services, and moving their workloads to the cloud, the impact of a cybersecurity event today is greater than ever before and could include personal data loss, significant financial losses, compromise of safety, and even loss of life. Organizations can no longer protect themselves by simply securing their own infrastructures since their electronic perimeter is no longer meaningful; threat actors intentionally target the suppliers of more cyber-mature organizations to take advantage of the weakest link.

No-Cost Online Course: Federal Virtual Training Environment (FedVTE): *Cyber Supply Chain Risk Management*

Course Information	https://fedvte.usalearning.gov/coursecat_external.php
FedVTE Login and Registration Page	https://fedvte.usalearning.gov/
Description	This 2-hour online course is available to state, local, tribal, and territorial organizations at no cost. The course will show how to securely provision and govern a supply chain, as well as give guidance on recognizing potential dangers and identifying threats.