MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

MS-ISAC Working Group
**Metrics**

# 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 Working Group.

## 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 at 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.

### Establish Basic Cyber Hygiene Through a Managed Service Provider

**Resource Link**

"Establish Basic Cyber Hygiene Through a Managed Service Provider"

**Description**

Small and medium enterprises often face the need to outsource their information technology infrastructure and services. Managed Service Providers (MSPs) offer the ideal solution of providing the services at an affordable cost and allow enterprises to focus on other aspects of their operations. Despite the convenience, relying on a third party for all of an organization's technology needs can leave an organization feeling uncertain, vulnerable, or provide a false sense of security. This paper provides an overview of the CIS Critical Security Controls® (CIS Controls®) and provides small and medium enterprises with a guideline questionnaire to ensure their basic cyber hygiene needs are met by their managed service provider.

### Managing Cybersecurity Supply Chain Risks in Election Technology: A Guide for Election Technology Providers

**Resource Link**

"Managing Cybersecurity Supply Chain Risks in Election Technology"

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

**Description**

The primary objective of this document is to provide election technology providers a mitigation approach for cybersecurity-based supply chain risks based on a risk assessment conducted by CIS. This document is intended to assist election technology providers in identifying the most significant cybersecurity supply chain risks for their products and choosing appropriate risk mitigation approaches or those risks.

## 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

### No-Cost Online Courses: Federal Virtual Training Environment (FedVTE)

**FedVTE Login and Registration** https://fedvte.usalearning.gov/

**Description** The Federal Virtual Training Environment (FedVTE) provides FREE online cybersecurity training to federal, state, local, tribal, and territorial government employees, federal contractors, US military veterans and the public. Managed by DHS, FedVTE contains more than 800 hours of training on topics such as ethical hacking and surveillance, risk management, and malware analysis.

### NIST Special Publication NIST SP 800-161r1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

**Resource Link** https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

**Description** Organizations are concerned about the risks associated with products and services that may potentially contain malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the supply chain. These risks are associated with an enterprise's decreased visibility into and understanding of how the technology they acquire is developed, integrated, and deployed or the processes, procedures, standards, and practices used to ensure the security, resilience, reliability, safety, integrity, and quality of the products and services. This publication provides guidance to organizations on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of their organizations. The publication integrates cybersecurity supply chain risk management (C-SCRM) into risk management activities by applying a multilevel, C-SCRM-specific approach, including guidance on the development of C-SCRM strategy implementation plans, C-SCRM policies, C-SCRM plans, and risk assessments for products and services.