Office of Information Technology

1920 Supply Chain Risk Management Policy

2025-10-20

Table of Contents

	Department of Human Services **Online Directives Information System**	**Index:**	**POL1920**
		Revised:	**06/02/2025**
		Next Review:	**06/02/2027**

Subject: DHS Information Security Policies

Policy

This policy establishes the Supply Chain Risk Management Policy, for managing risk by identifying, assessing, and mitigating threats, vulnerabilities, and disruptions to the DHS supply chain from beginning to end to ensure mission effectiveness. The Supply Chain Risk Management Policy and associated plans, augment DHS mission, by proactively identifying threats and vulnerabilities, which can result in consequences (impact).

Authority

1. United States Department of Commerce National Institute for Standards and Technology (NIST)
2. United States Internal Revenue Service
3. United States Department of Health & Human Services – Administration of Children and Families (ACF), Office of Child Support Services (OCSS)
4. United States Department of Health & Human Services - Centers for Medicare & Medicaid Services (CMS)
5. Georgia Technology Authority
6. Social Security Administration
7. Federal Bureau Investigation (Criminal Justice Information Services)

References

- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, Revision 5, September 2020
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-100 “Information Security Handbook: A Guide for Managers” March 2007
- Federal Information Security Management Act of 2002 (FISMA)
- Georgia Technology Authority Enterprise Information Security Policy
- United States Internal Revenue Service, IRS Publication 1075 Tax Information Security Guidelines For Federal, State and Local Agencies Safeguards for Protecting Federal Tax Returns and Return Information
- Centers for Medicare & Medicaid Services, Volume II: Minimum Acceptable Risk Standards for Exchanges
- Social Security Administration (“SSA”) Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration (“TSSR”)
- Criminal Justice Information Services Security Policy
- ACF/OCSS - Security Agreement

Applicability

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by DHS. Any information not specifically identified as the property of other parties, that is transmitted or stored on DHS IT resources (including e-mail, messages and files) is the property of DHS. All users (DHS employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

Definitions

Controlled Unclassified Information (CUI)

Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

Responsibilities

a. DHS shall adopt the Supply Chain principles established in NIST SP 800-161 "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," Control Family guidelines, as the official policy for this domain. The following subsections outline the Supply Chain standards that constitute DHS policy. Each DHS Business System is then bound to this policy, and shall develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented.

SR-1 Supply Chain Risk Management Policy and Procedures

a. Develop, document, and disseminate to designated agency personnel:
   A. All organizational level supply chain risk management policy that:
      1. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      2. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   B. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;

b. Designate an **agency official** to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and

c. Review and update the current supply chain risk management:
   A. Policy **every one (1) years (or if there is a significant change)**; and
   B. Procedures **every one (1) year (or if there is a significant change)**.

SR-2: Supply Chain Risk Management Plan

a. 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: Information systems that process, store, or transmit CUI.

b. Review and update the supply chain risk management plan at least every one (1) year or as required, to address threat, organizational or environmental changes; and

c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

SR-2 (1) *Establish SCRM Team:*

Establish a supply chain risk management team consisting of agency-defined personnel to lead and support the following SCRM activities: provide expertise in acquisition processes, legal practices, vulnerabilities, threats, and attack vectors, as well as an understanding of the technical aspects and dependencies of systems.

SR-3: Supply Chain Controls and Processes

a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of systems that access, process, store, or transmit CUI in coordination with agency-defined supply chain personnel;

b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain related events: Agency-defined Supply Chain Risk Controls and controls identified in Pub 1075; and

c. Document the selected and implemented supply chain processes and controls in security and privacy plans; supply chain risk management plan; Agency System Security Plan.

SR-3 (2) *Limitation of Harm:*

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

SR-3 (3) *Sub-Tier Flow Down:*

Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subs.

SR-6: Supplier Assessments and Reviews

Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide at a minimum annually.

SR-8: Notification Agreements

Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the notification of supply chain compromises, results of assessments or audits, and organization information.

SR-10: Inspection of Systems and Components

Inspect the following systems or system components at agency-defined frequency, upon delivery to detect tampering: hardware /software components that access, process, store, or transmit CUI.

SR-11: Component Authenticity

a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and

b. Report counterfeit system components to source of counterfeit component; agency-defined personnel or roles.

SR-11 (1) *Anti-Counterfeit Training:*

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

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

Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: hardware used to receive, access, process, store, transmit or protect CUI.

SR-12: Component Disposal

Dispose of organization-defined data, documentation, tools, or system components using the techniques and methods in accordance with the most current NIST SP 800-88, Guidelines for Media Sanitization.

History

Date	Change	User	Version

Evaluation

The Office of Information Technology (OIT), upon recommendation of the DHS Chief Information Security Officer (CISO), evaluates this policy annually by:

1. Comparing its content and intent to evolving regulatory compliance standards imposed upon the Agency, such as, IRS 1075, NIST 800-53, and CMS MARS-E.
2. Addressing any deficiencies or gaps discovered during periodic audits conducted by Georgia DOAA or other regulatory bodies, such as, IRS, CMS, SSA, FBI, etc.