Compliance Component

DEFINITION

Name	Supply Chain Risk Management Plan
Description	Supply chain risk management plans are strategies to determine responses to various issues that could arise in the supply chain if they were to occur
Rationale	The dependence on products, systems, and services from external providers, as well as the nature of the relationships with those providers, present an increasing level of risk to the State. Threat actions that may increase security or privacy risks include unauthorized production, the insertion or use of counterfeits, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development practices in the supply chain.
Benefits	- Planning ahead can help mitigate risk if there were to be an incident in the supply chain. - Helps protect against issues that may arise with third party vendors. - Keep better track of procurement

ASSOCIATED ARCHITECTURE LEVELS

Specify the Domain Name	Security
Specify the Discipline Name	Management
Specify the Technology Area Name	Supply Chain Risk Management

COMPLIANCE COMPONENT TYPE

Document the Compliance Component Type	
Component Sub-type	

COMPLIANCE DETAIL

State the Guideline, Standard or Legislation	Supply chain risks can be endemic or systemic within a system element or component, a system, or the State in general. Where feasible, the agency shall: - 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 Agency systems, system components or system services. - Review and update the supply chain risk management plan as required, to address threat, organizational, or environmental changes. - Protect the supply chain risk management plan from unauthorized disclosure and modification. - Establish a supply chain risk management team consisting of information technology, security, privacy, legal, and procurement personnel who lead and support acquisition and procurement activities.

	Managing supply chain risk is a complex, multifaceted undertaking that requires a coordinated effort to build trust relationships and communicate with internal and external stakeholders. Supply chain risk management (SCRM) activities include:
	 • Identifying and assessing risks • Determining appropriate risk response actions • Developing SCRM plans to document response actions • Monitoring performance against plans The SCRM plan (at the system-level) is implementation specific, providing policy implementation, requirements, constraints, and implications.
Document Source Reference #	NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations,* SR-2 – *Supply Chain Risk Management Plan* (Sep. 2020)

Compliance Sources			
Name		*Website*	[Security and Privacy Controls for Information Systems and Organizations (nist.gov)](nist.gov)
Contact Information			
Name		*Website*	
Contact Information			
Name		*Website*	
Contact Information			

KEYWORDS	
List Keywords	Supply Chain Risk Management, Plan, Third-Party Vendor

COMPONENT CLASSIFICATION				
Provide the Classification	☐ *Emerging*	☒ *Current*	☐ *Twilight*	☐ *Sunset*
Sunset Date				

CURRENT STATUS				
Provide the Current Status	☐ *In Development*	☐ *Under Review*	☒ *Approved*	☐ *Rejected*

AUDIT TRAIL			
Creation Date	08/21/2024	*Date Approved / Rejected*	10/03/2024
Reason for Rejection			
Last Date Reviewed	10/03/2024	*Last Date Updated*	10/03/2024
Reason for Update	Vitality		