	Department of Human Services Online Directives Information System	Index: Revised: Next Review:	POL1915 01/05/2022 01/05/2024

System and Services Acquisition Policy

Policy

This policy establishes the Enterprise System and Services Acquisition Policy, for managing risks from third party products and services' providers, through the establishment of an effective third-party risk management program. The third-party risk assessment program helps DHS implement security best practices with regard to Systems and Services Acquisition.

References:

1. 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 4, January 2015
2. 45 CFR Parts 160 and 164 HIPAA General Administrative Requirements and Security and Privacy; Final Rule: Workforce Security
3. Georgia Technology Authority Enterprise Information Security Policy
4. Centers for Medicare & Medicaid Services, Volume II: Minimum Acceptable Risk Standards for Exchanges

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.

Responsibilities

DHS shall adopt the System and Services Acquisition principles established in NIST SP 800-53 "System and Services Acquisition," Control Family guidelines, as the official policy for this domain. The following subsections outline the System and Services Acquisition 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.

- **SA-1 System and Services Acquisition Policy and Procedures**
    1. Senior management, management, and all organization entities are required to coordinate and implement necessary controls for system and services acquisition of IT resources and information systems on the basis of business and security requirements.
    2. Periodic reviews of this policy shall be performed and documented at least within every **three years**, or when there is a **significant change**.
    3. Periodic review of access control procedures shall be performed at least **annually**.
- **SA-2 Allocation of Resources**:
    1. The resources required to provide security for the information system must be determined, documented, and allocated as part of the capital planning and investment control process.
    2. Security must be integrated into the Capital Planning and Investment Control process.
    3. A discrete line item for information security must be established in organizational programming and budgeting documentation.
- **SA-3 System Development Life Cycle**
  All DHS project/program lifecycle methodologies should be cross referenced with security lifecycle activities as described by the Office of Information Technology.
    1. The information system must be managed using a system development life cycle (SDLC) methodology that includes information security considerations.
    2. Information system security roles and responsibilities must be defined and documented throughout the SDLC. Additionally, the information security risk management process must be integrated into SDLC activities.
    3. Individuals having information security roles and responsibilities must be identified.
    4. Integrate the agency information security risk management process into SDLC activities.
- **SA-4 Acquisition Process:**
    1. Requirements and/or specifications must include the following, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.
        a) Security functional requirements
        b) Security strength requirements
        c) Security assurance requirements
        d) Security-related documentation requirements
        e) Requirements for protecting security-related documentation

f) Description of the information system development environment and environment in which the system is intended to operate

g) Acceptance criteria

2. Providers of defined external information systems are required identify the location of information systems that receive, process, store, or transmit agency data, with special emphasis on sensitive data to include, but is not limited to Federal Tax Information (FTI), Social Security Administration data, etc.

- **SA-5 Information System Documentation**
  1. Administrator documentation (i.e., whether published by a vendor/manufacturer or written in-house) for the information system and constituent components must be obtained, protected as required, and made available to authorized personnel. Administrator documentation must include information that describes:
     a) Secure configuration, installation, and operation of the system, component, or service.
     b) Effective use and maintenance of security functions/mechanisms.
     c) Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.
  2. User documentation (i.e., whether published by a vendor/manufacturer or written in-house) for the information system and constituent components must be obtained, protected as required, and made available to authorized personnel. User documentation must include information that describes:
     a) User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.
     b) Methods for user interaction, which enable individuals to use the system, component, or service in a more secure manner.
     c) User responsibilities in maintaining the security of the system, component, or service.
  3. When information system documentation is either unavailable or non- existent, the following actions must be taken:
     a) Document attempts to obtain such documentation.
     b) Recreate selected information system documentation if such documentation is essential to the effective implementation and/or operation of security controls.
  4. Protect documentation, as required by system classification requirements.
  5. Distribute documentation to designated agency officials.
- **SA-8 Security Engineering Principles**
  1. Information system security engineering principles must be applied in the specification, design, development, implementation, and modification of the information system.
  2. The application of security engineering principles must be integrated into the SDLC.
     a) Security engineering principles are primarily targeted at information systems under new development and information systems undergoing major upgrades.

b) For legacy information systems, security engineering principles must be applied to system upgrades and modifications, to the extent feasible, given the current states of the hardware, software, and firmware components within the system.

3. Security engineering principles must include, but are not limited to:
    a) Developing layered protections.
    b) Establishing sound security policy, architecture, and controls as the foundation for design.
    c) Incorporating security into the SDLC.
    d) Delineating physical and logical security boundaries.
    e) Ensuring system developers and integrators are trained on how to develop secure software.
    f) Tailoring security controls to meet organizational and operational needs.
    g) Reducing risk to acceptable levels, thus enabling informed risk management decisions.

- **SA-9 External Information System Services**
    1. Documents that solicit and implement external information system services must require that providers comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
    2. Documents that solicit and implement external information system services must:
        a) Identify specific drivers for soliciting the services.
            i. Examples include, but are not limited to applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
        b) Specify responsibilities for each security control or for specific activities within a control.
        c) Identify associated reporting requirements for each security control.
        d) Require the provider of external information system services to conform to the same security control and documentation requirements as would apply to the Agency's internal systems.
    3. The following documentation must be included in the procurement of external information system services:
        a) Government, service provider, and end user security roles and responsibilities.
        b) Any SLAs.
    4. Security control compliance by external service providers must be verified on an ongoing basis.
    5. **FOR SYSTEMS WHICH PROCESS FTI DATA ONLY:** Restrict the location of information systems that receive, process, store, or transmit FTI to areas within the United States territories, embassies, or military installations.

- **SA-10 Developer Configuration Management**
    1. Configuration management must be performed during information system design, development, implementation, and operation for:
        a) Contractual development and system integration.
        b) Internal development procedures.
    2. The configuration management process must address the following:
        a) Managing and controlling changes to the information system.
        b) Implementing only EPA-approved changes.
        c) Documenting approved changes to the information system.
        d) Tracking of security flaws and corrective or remediation actions
- **SA-11 Developer Security Testing and Evaluation**
    1. Testing requirements must be included in:
        a) Contractual documents for development and system integration.
        b) Internal development procedures.
    2. A Security Test and Evaluation Plan must be created and implemented for all information system development.
        a) The plan must be developed in consultation with associated security personnel, including security engineers.
        b) Using automated code analysis tools is a preferred testing methodology, has proved to be an efficient testing mechanism, and provides better assurance than manual code walk-throughs.
        c) Vulnerability scanning must be a component of the testing
            i. The information system and its configuration must be scanned prior to authorization and again immediately following deployment.
        d) When NIST-validated cryptographic modules are used, the following must be verified:
            i. The existence of a valid certificate for each module.
            ii. Conformance to the published security policy for each module employed.
        e) The plan must include requirements for retesting after significant changes occur.
    3. A verifiable flaw remediation process must be implemented to correct weaknesses and deficiencies identified during the security testing and evaluation process.
    4. Those controls not in place or not operating as intended, as determined by test results, must be remediated.
        a) The plan for remediation must be entered into and tracked in the DHS POA&M repository.
        b) The DHS POA&M repository must be used.

- **SA-22 Unsupported System Components**

  DHS shall replace information system components when support for the components is no longer available from the developer, vendor, or manufacturer.

History

None

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.