Department of Transformation and Shared Services
State Cybersecurity Office

Standard Title: System and Services Acquisition Standard
Standard Version: 1.0
Effective Date: 12/19/2022

---

1. Purpose

The purpose of this Standard is to ensure that Information Technology (IT) resources and information systems are acquired with security requirements to meet the mission and business objectives of the Arkansas DIS and are in compliance with IT security policies, standards, and procedures

2. Applicability

This standard covers all systems developed by, or on behalf of the Arkansas Division of Information Systems (DIS). This includes all development, test, quality assurance, production and other ad hoc systems.

Notations of specific control items (e.g., CJIS, FTI, PCI) only pertain to the systems that are required to comply with such regulations.

3. Definitions

Refer to the DIS Regulatory Definitions document.

4. Standard

4.1 Allocation of Resources SA-2 (NIST Moderate Control)

DIS, in coordination with the information system owner, shall:

a. Determine information security requirements for the information system or information system service in mission/business process planning.
b. Determine, document, and allocate the resources required to protect the information system or information system service as part of its capital planning and investment control process.
c. Establish a discrete line item for information security in organizational programming and budgeting documentation.

4.2 System Development Life Cycle SA-3 (NIST Moderate Control)

DIS shall acquire, develop, and manage systems using a System Development Life Cycle (SDLC) that incorporates information security and privacy considerations including:

a. Identify qualified individuals having information security and privacy roles and responsibilities that are involved in creating the SDLC. This may include the CIO, CISO, business owners, system administrators, security architects, security engineers, security analysts, etc. These personnel will ensure that the system life cycle activities meet the security and privacy requirements for the organization.
b. Define and document information security and privacy roles and responsibilities throughout the SDLC in the Regulatory_Settings spreadsheet.
c. Integrate the agency information security and privacy risk management process into SDLC activities.
d. A business case justification of custom system development projects shall be required. When proposing the development of custom software, a strong business case shall include the following:
    1. Support the rationale for not enhancing current systems;
    2. Demonstrate the inadequacies of packaged solutions; and
    3. Justify the creation of custom software.
e. The organization shall implement a change management program which enables system engineers, architects, and security analysts to expediently perform their necessary business functions, yet maintain a controlled, secure, and functioning environment. Examples of this program include multi-tiered deployments (Dev, Test, Quality Assurance (QA), Production), which are capable of backing-up and rolling-back changes which are unsuccessful. Change control requirements are provided in the Configuration Management Policy
f. DIS will plan for End-of-Life (EoL) and End-of-Support dates (EoS) for systems and services. This will ensure that systems and services can receive security patches and updates throughout the system development lifecycle, and that the organization is prepared to discontinue the system or service once no longer supported, or when security cannot be ensured.

4.3 Acquisition Process SA-4 (NIST Moderate Control)

Security functional requirements are a part of the hardware, software, or firmware acquisition process. Agencies shall be capable of acquiring necessary solutions in an expedient manner. The following shall be done:

a. Security and privacy functional requirements shall include security capabilities, security functions, and security mechanisms.
b. Strength of mechanism requirements based on security categorization, e.g., Low or Moderate, associated with such capabilities, functions, and mechanisms shall include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass.
c. Security and privacy assurance requirements shall include the following:
d. Controls needed to satisfy the security and privacy requirements.
    1. Development processes, procedures, practices, and methodologies.
    2. Evidence from development and assessment activities providing grounds for confidence that the required security and/or privacy functionality has been implemented and the required security strength has been achieved.
e. Security and privacy documentation requirements.
f. Requirements for protecting security and privacy documentation.
g. Description of the information system development environment and environment in which the system is intended to operate.
h. Acceptance criteria requirements for assessing the ability of a system component, software, or system to perform its intended function.
i. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management.
j. Proposed vendor hardware design shall comply with information security and other State policies and standard security and technical specifications, such as the following:
    1. Vendors shall configure the system with adequate capacity to fulfil the functional requirements stated in the agency's design document.
    2. Vendor shall configure hardware security controls to adequately protect data. (Optionally, the vendor may assist the agency with the configuration of software security controls to provide adequate data protection on the vendor's hardware.)
k. Systems under consideration for acquisition shall be interoperable with the peripherals and systems currently in use.
l. To mitigate risks of exploitation of covert channels, third-party applications shall be obtained from reputable sources.
m. Non-security functional and technical requirements shall be a part of the hardware, software, or firmware acquisition process.
n. DIS shall follow State procurement policies when acquiring hardware to ensure that the purchase meets specified functional needs. Agencies shall include specific requirements for performance, reliability, cost, capacity,

security, support, and compatibility in Requests for Proposals (RFPs) to properly evaluate quotes.

o. DIS must ensure vendor compliance with Statewide security policies.

p. New system purchases shall meet, at a minimum, current operational specifications and have scalability to accommodate for growth projected by the agency.

4.4 Acquisition Process | Functional Properties of Controls SA-4(1) (NIST Moderate Control)

Developer(s) of the system, system component, or information system service shall provide a description of the functional properties of the security controls to be employed. Functional properties of security controls describe the functionality (e.g., security capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.

4.5 Acquisition Process | Design and Implementation Information for Controls SA-4(2) (NIST Moderate Control)

Developer(s) of a system, system component, or information system service shall provide design and implementation information for the security controls to be employed that includes the following: security-relevant external system interfaces, high-level design, source code, or hardware schematics

4.6 Acquisition Process | Functions, Ports, Protocols, and Services in Use SA-4(9) (NIST Moderate Control)

Developer(s) of a system, system component, or information system service shall identify the functions, ports, protocols, and services intended for use.

4.7 System Documentation SA-5 (NIST Moderate Control)

DIS must obtain, develop, or document administrator and user documentation for the system, system component, or system service. Such documentation shall be distributed to designated agency officials that describes the following:

a. Secure configuration, installation, and operation of the system, component, or service.

b. Effective use and maintenance of security and privacy functions/mechanisms.

c. Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.

d. User-accessible security and privacy functions/mechanisms and how to effectively use those functions/mechanisms.

e. Methods for user interaction, which enable individuals to use the system, component, or service in a more secure manner and protect individual privacy.
f. What responsibilities the end user has in maintaining the security and privacy of the individuals.
g. The following shall also be done:
    a. Ensure each new or updated system includes supporting system documentation and technical specifications of information technology hardware, whether the system is developed or updated by in-house staff or by a third-party vendor.
    b. Create, manage, and secure system documentation libraries or data stores that are always available to only authorized personnel.
    c. Ensure that system documentation is readily available to support the staff responsible for operating, securing, and maintaining new and updated systems.
    d. Control system documentation to ensure that it is current and available for purposes such as auditing, troubleshooting and staff turnover.
    e. All documentation of operational procedures must be approved by management and reviewed for accuracy and relevancy according to the Regulatory_Settings spreadsheet.

4.8 Security and Privacy Engineering Principles SA-8 (NIST Moderate Control)

DIS shall apply information system security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components. Security and Privacy engineering principles shall be primarily applied to new development information systems or systems undergoing major upgrades. For legacy systems, organizations shall apply security engineering principles to system upgrades and modifications to the extent that it is technically configurable, given the current state of hardware, software, and firmware within those systems.

a. Security and Privacy engineering principles shall include:
    1. Developing layered protections.
    2. Establishing sound security and privacy policy, architecture, and controls as the foundation for design.
    3. Incorporating security and privacy requirements into the SDLC.
    4. Delineating physical and logical security boundaries.
    5. Ensuring that system developers are trained on how to build secure software.

6. Tailoring security and privacy controls to meet organizational and operational needs.
7. Performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk.
8. Reducing risk to acceptable levels, thus enabling informed risk management decisions.

b. NIST SP 800-160, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems shall be used as guidance on engineering principles for information system security.

4.9 External System Services SA-9 (NIST Moderate Control)

DIS shall require that third parties and providers of external system services comply with statewide information security and privacy requirements. Agencies shall employ controls as follows:

a. Define and document how external information system comply with statewide information security and privacy controls to include user roles and responsibilities and compliance auditing and reporting requirements. Agencies must ensure vendor compliance with Statewide security policies and obtain a Vendor Readiness Assessment Report (VRAR) from the vendor prior to contract approval.
b. Monitor security and privacy control compliance by external service providers on an ongoing basis.
c. Restrict the location of information systems that receive, process, store, or transmit state and federal data to areas within the (CMS, CJIS, FTI Control):
    1. US States,
    2. US Territories.
d. Restrict the location of help desk services supporting systems or applications with regulated data to areas within the (FTI Only Control):
    a. US States,
    b. US Territories.
e. Agencies that outsource their information processing must ensure that the service provider demonstrates compliance with state standards and procedures, and industry quality standards.
f. Outsourcing agreements shall include the following:
    1. The agency's course of action and remedy if the vendor's security and privacy controls are inadequate such that the confidentiality, integrity, or availability of the agency's data cannot be assured.

2. The vendor's ability to provide an acceptable level of processing and information security during contingencies or disasters.
3. The vendor's ability to provide processing in the event of failure(s).

g. To support service delivery, the outsourcing agreements shall contain, or incorporate by reference, all the relevant security and privacy requirements necessary to ensure compliance with the statewide information security standards, the agency's record retention schedules, its security policies, and its business continuity requirements.
h. Services, outputs, and products provided by third parties shall be reviewed and checked according to the Regulatory Settings spreadsheet and in accordance with state statutes.
i. To monitor third party deliverables, agencies shall do the following:
    1. Monitor third party service performance to ensure service levels meet contract requirements.
    2. Review reports provided by third parties and arrange regular meetings as required by contract(s).
    3. Resolve and manage any identified problem areas.
j. Contracts with vendors providing offsite hosting or cloud services that will host Confidential or Sensitive data must require the vendor to provide the State a third-party risk assessment report (e.g., Service Organization Control {SOC} 2 Type II, International Organization for Standardization {ISO} 27001, Federal Risk and Authorization Management Program {FedRAMP} Moderate, State Risk and Authorization Management Program {StateRAMP} Moderate, or HITRUST CSF {Common Security Framework}) before contract award and according to the Regulatory_Settings spreadsheet thereafter.
k. Any changes to services provided by a third party must be approved by the agency prior to implementation.
l. DIS shall develop a process for engaging service providers and maintain a list of all service providers who store or share confidential data.
m. DIS shall ensure that the service-level agreement (SLA) includes requirements for regular monitoring, review, and auditing of the service levels and security requirements as well as incident response and reporting requirements. The SLA shall state how the service provider is responsible for data stored or shared with the provider.
n. DIS shall perform the monitoring, review, and auditing of services to monitor adherence to the SLA and identify new vulnerabilities that may present unreasonable risk. Agencies shall enforce compliance with the SLA and must be proactive with third parties to mitigate risk to a reasonable level.

o. Changes to an SLA and services provided shall be controlled through formal change management.
p. DIS must prohibit the use of non-agency-owned information systems, system components, or devices that receive, process, store, or transmit Highly Restricted data, including federal tax information (FTI), unless explicitly approved by the IRS Office of Safeguards.

4.10 External System Services | Identification of Functions, Ports, Protocols, and Services SA-9(2) (NIST Moderate Control)

Providers of external system services shall identify the functions, ports, protocols, and other services required for the use of such services. Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be particularly useful when the need arises to understand the trade-offs involved in restricting certain functions/services or blocking certain ports/protocols.

4.11 Developer Configuration Management SA-10 (NIST Moderate Control)

System developers shall create and implement a configuration management plan that does the following:

a. Performs configuration management during system design, development; implementation, operation and/or disposal for the following:
    1. Internal system development and system integration of commercial software.
    2. External system development and system integration.
b. Documents, manages, and controls changes to the system or configuration items, and the potential security and privacy impacts
c. Implements only agency approved changes to the system,
d. Documents approved changes to the system,
e. Tracks security flaws and flaw resolution within the system,
f. Organizations shall mitigate risks of exploitation of covert channels by protecting the source code in custom developed applications.

4.12 Developer Testing and Evaluation SA-11 (NIST Moderate Control)

System developers shall test for software faults that pose a security risk at all post-design stages of the system development life cycle prior to putting an application into production. The following shall be done:

a. Develop and implement a security and privacy assessment plan.
    1. Develop and implement a plan that supports ongoing security and privacy assessments. Testing requirements must be defined and documented for both system development and system integration

activities. The plan must include requirements for retesting after significant changes occur.

2. Perform security testing/evaluation.
    - Restricted or Highly Restricted data shall not be used for testing purposes.
    - Organizations may permit the use of production data during the testing of new systems or system changes only when no other alternative allows for the validation of the functions and when permitted by other regulations and policies. Data anonymization or data masking tools shall be used if available.
    - If production data is used for testing, the same level of security controls required for a production system shall be used.
3. Produce evidence of the execution of the security and privacy assessment plan and the results of the security testing/evaluation
4. Implement a verifiable flaw remediation process
5. Correct flaws identified during security testing/evaluation

b. Teach and encourage software fault-reporting procedures through security training and awareness programs.
c. Designate a quality control team that consistently checks for faults and that is responsible for reporting them to software support.
d. Use a formal recording system for the following:
    1. Tracks faults from initial reporting through to resolution.
    2. Monitors the status of reported faults and confirms that satisfactory resolutions have been achieved.
    3. Provides reports and metrics for system development and software support management.
    4. Software faults shall be prioritized and addressed promptly to minimize the exposure resulting from the security vulnerability
e. While faults are being tracked through to resolution, research shall also be conducted to ensure no security controls have been compromised and resolution activities have been appropriately authorized.
f. Perform unit, integration, and system regression testing/evaluation:
    1. Require that information system developers/integrators perform a vulnerability assessment to document vulnerabilities, exploitation potential, and risk mitigations.
    2. Appropriate testing and assessment activities shall be performed after vulnerability mitigation plans have been executed to verify and validate that the vulnerabilities have been successfully addressed.

3. To maintain the integrity of information technology systems, software shall be evaluated and certified for functionality in a test environment before it is used in an operational/production environment.
4. Test data and accounts shall be removed from an application or system prior to being deployed into a production environment if the application or system does not have a dedicated testing environment.
5. Qualified personnel must certify that the upgrade or change has passed acceptance testing.
6. A rollback plan must be established in the event the upgrade or change has unacceptable ramifications.

g. The following issues and controls shall be included when developing acceptance criteria and acceptance test plans:
    1. Capacity requirements - both for performance and for the computer hardware needed.
    2. Error response - recovery and restart procedures and contingency plans.
    3. Routine operating procedures - prepared and tested according to defined policies.
    4. Security controls - agreed to and put in place.
    5. Manual procedures - effective and available where technically configurable and appropriate.
    6. Business continuity - meets the requirements defined in the business continuity plan.
    7. Impact on production environment - able to demonstrate that installation of new system will not adversely affect current production systems (particularly at peak processing times).
    8. Training - of operators, administrators, and users of the new or updated system.
    9. Logs - logs of results shall be kept for a defined period once testing is completed.
h. Implement a verifiable flaw remediation process to correct security weaknesses and deficiencies identified during the security testing and evaluation process.
i. Controls that have been determined to be either absent or not operating as intended during security testing/evaluation must be remediated.

4.13 Developer Testing and Evaluation | Static Code Analysis SA-11(1) CJIS Only

DIS shall identify applications, services and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

DIS, or the vendor where applicable, shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes. The policy shall include the following:

a. Testing of appropriate patches before installation
b. Rollback capabilities when installing patches, updates, etc.
c. Automatic updates without individual user intervention.
d. Centralized patch management.

4.14 Development Process, Standards and Tools SA-15 (NIST Moderate Control)

DIS requires all developers of the system, system component or system service to follow a documented development process that:

a. Explicitly addresses security and privacy requirements.
b. Identifies the standards and tools used in the development process.
c. Documents the specific tool options and tool configurations used in the development process.
d. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development

DIS will review the development process, standards, tool options, and tool configurations as referenced in the Regulatory_Settings spreadsheet, to ensure the process, standards, tools, tool options and tool configurations selected and employed can satisfy the security and privacy requirements implemented by DIS.

4.15 Development Process, Standards and Tools | Critical Analysis SA-15(3) (NIST Moderate Control)

DIS requires the developer of the information system, system components, or information system service to perform a criticality analysis at (breadth/depth and at (decision points in lifecycle).

4.16 Developer-provider Training SA-16 (PCI Only Control)

DIS will maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.

Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgment does not have to include the exact wording provided in this requirement.

4.17 Developer Security and Privacy Architecture and Design SA-17 (PCI Only Control)

DIS will require the developer of the system, system component or system service to produce, design specification and security architecture that:

a. Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:
    1. In accordance with PCI DSS (secure authentication and logging)
    2. Based on industry standards and/or best practices.
    3. Incorporating information security throughout the software-development life cycle.
b. Remove development, test and/or custom application accounts, user ID's, and passwords before applications become active or are released to customers.
c. Review custom code prior to release to production or customers to identify and potential coding vulnerability (using either manual or automated processes) to include at least the following:
    1. Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code review techniques and secure coding practices.
    2. Code reviews ensure code is developed according to secure coding guidelines.
    3. Appropriate corrections are implemented prior to release.
    4. Code-review results are reviewed and approved by management prior to release.
d. Follow change control processes and procedures for all changes to system components. The processes must include the following:
    1. Separate development/test environments from production environments and enforce the separation with access controls.
    2. Separation of duties between development/test and production environments.
    3. Production data (live PANs) are not used for testing or development.
    4. Removal of test data and accounts from system components before the system becomes active or goes into production.
e. Change control process must include the following:
    1. Documentation of impact.

2. Documented change approval by authorized parties.
3. Functionality testing to verify that the change does not adversely impact the security of the system.
4. Back-out procedures.

f. Upon completion of significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.
g. Address common coding vulnerabilities in software-development processes as follows:
    1. Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities.
    2. Develop applications based on secure coding guidelines

4.18 Developer Screening SA-21 (PCI Only Control)

DIS ensures that developers of systems, system components, or system services:

a. Have appropriate access authorizations as determined by defined duties.
b. Satisfy any additional personnel screening criteria required by the position.

4.19 Unsupported System Components SA-22 (NIST Moderate Control)

DIS must replace devices (e.g., servers, workstations, laptops, network devices, IoT devices, printers, applications) when support for such is no longer available from the developer, vendor, or manufacturer. Support includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components includes when vendors no longer provide security or other critical software patches or product updates, which can result in an opportunity for adversaries to exploit weaknesses in the installed components. In instances where components cannot be replaced, DIS will execute the Exception Request Procedure, implement alternative solutions for support (e.g., in-house support), and enforce appropriate mitigating controls.

5. Authority

Refer to the DIS Regulatory Definitions document.

6. Compliance

This control shall take effect upon publication. Compliance is expected with all DIS controls. Employees not following this DIS control are subject to the standard DIS disciplinary procedures.

If compliance with this control is not feasible or technically possible, or if deviation from this control is necessary to support a business function, applicable entities shall request an exception through the DIS Exception Request Procedure.

7. Related Documentation

System and Services Acquisition Procedures
Policy_SA_System and Services Acquisition
SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings

8. Revision History

This standard shall be subject to review according to the Regulatory Settings spreadsheet to ensure relevancy.

Date	Description of Change	Reviewer
12/16/2022	Moved from Draft to Final	Greggari Tucker, Deputy Chief Information Security
12/19/2024	Annual Review. Update of "Related Documentation".	Raymond Girdler, State IT Security Specialist