|  |
| --- |
| **{COMMAND}** |
| **{SYSTEM NAME} {ACRONYM}** |
| **System Version: {VERSION}**  **eMASS# {EMASS#}**  **Confidentiality: {CONFIDENTIALITY}**  **Integrity: {INTEGRITY}**  **Availability: {AVAILABILITY}** |
| **Department of the {SERVICE}** |
| **{LOGO}** |
|  |
| **System and Services Acquisition Plan**  **Document Version: 1.0.0**  **{DATE}** |
| Prepared by: {ORGANIZATION}  **DISTRIBUTION IS LIMITED TO U.S. GOVERNMENT AGENCIES AND THEIR CONTRACTORS.**  **OTHER REQUESTS FOR THIS DOCUMENT MUST BE REFERRED TO: {ORGANIZATION}** |

**Change Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Author | Changes Made / Section(s) |
| {DATE} | 1.0.0 | {ORGANIZATION} | Initial Document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Amplifying Guidance**

1. DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)" [PDF icon](http://dtic.mil/whs/directives/corres/pdf/851001_2014.pdf)
2. DoD Directive 5000.01, “The Defense Acquisition System” [PDF icon](http://dtic.mil/whs/directives/corres/pdf/500001p.pdf)
3. DoD Instruction 5000.02, “Operation of the Defense Acquisition System” [PDF icon](http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf)
4. DoD Instruction 8580.1, “Information Assurance (IA) in the Defense Acquisition System” [PDF icon](http://dtic.mil/whs/directives/corres/pdf/858001p.pdf)
5. NIST Special Publication 800-100, "Information Security Handbook: A Guide for Managers" [PDF icon](http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf)
6. NIST Special Publication 800-64 Revision 2, "Security Considerations in the System Development Life Cycle" [PDF icon](http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf)

**Table of Contents**

[**1.0** **OVERVIEW** 1](#_Toc461611746)

[**2.0** **SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES** 2](#_Toc461611747)

[**3.0** **ALLOCATION OF RESOURCES** 2](#_Toc461611748)

[**4.0** **SYSTEM DEVELOPMENT LIFE CYCLE** 2](#_Toc461611749)

[**5.0** **ACQUISITION PROCESS** 3](#_Toc461611750)

[**5.1** **Architecture Characteristics** 3](#_Toc461611751)

[**5.2** **Design Information** 3](#_Toc461611752)

[**5.3** **Contracts and Agreements** 4](#_Toc461611753)

[**6.0** **INFORMATION SYSTEM DOCUMENTATION** 5](#_Toc461611754)

[**7.0** **SECURITY ENGINEERING PRINCIPLES** 6](#_Toc461611755)

[**8.0** **EXTERNAL INFORMATION SYSTEM SERVICES** 7](#_Toc461611756)

[**9.0** **DEVELOPER CONFIGURATION MANAGEMENT** 8](#_Toc461611757)

[**10.0** **DEVELOPER SECURITY TESTING AND EVALUATION** 9](#_Toc461611758)

[**11.0** **SUPPLY CHAIN PROTECTION** 10](#_Toc461611759)

[**12.0** **DEVELOPMENT PROCESS, STANDARDS, AND TOOLS** 11](#_Toc461611760)

[**13.0** **COMPONENT AUTHENTICITY** 12](#_Toc461611761)

[**APPENDIX A – DETAILED COMPLIANCE MATRIX** 13](#_Toc461611762)

[**ENCLOSURE 1 – SYSTEM DEVELOPMENT LIFECYCLE** 95](#_Toc461611763)

[Table 1 - SP-800-53v4 Compliance Matrix 1](#_Toc447181008)

# **OVERVIEW**

The purpose of this System and Services Acquisition Plan is to manage the design, development, and maintenance of the {ACRONYM} security infrastructure, and to protect its information.

This document complies with the following requirements from NIST Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations". A detailed compliance matrix can be found in [Appendix A, “Detailed Compliance Matrix”](#_APPENDIX_I_–).

The following Assessment Procedures have not been allocated by NIST:

* SA-6 Software Usage Restrictions
* SA-7 User-Installed Software
* SA-13 Trustworthiness
* SA-14 Criticality Analysis
* SA-16 Developer-Provided Training
* SA-17 Developer Security Architecture and Design
* SA-18 Tamper Resistance and Detection

| CNTL NO. | CONTROL NAME | PRIORITY | LOW | MOD | HIGH |
| --- | --- | --- | --- | --- | --- |
| [SA-1](#SA1) | System and Services Acquisition Policy and Procedures | P1 | SA-1 | SA-1 | SA-1 |
| [SA-2](#SA2) | Allocation of Resources | P1 | SA-2 | SA-2 | SA-2 |
| [SA-3](#SA3) | System Development Life Cycle | P1 | SA-3 | SA-3 | SA-3 |
| [SA-4](#SA4) | Acquisition Process | P1 | SA-4 (10) | SA-4 (1) (2) (9) (10) | SA-4 (1) (2) (9) (10) |
| [SA-5](#SA5) | Information System Documentation | P2 | SA-5 | SA-5 | SA-5 |
| SA-6 | Software Usage Restrictions | Not Selected | Not Selected | Not Selected | Not Selected |
| SA-7 | User-Installed Software | Not Selected | Not Selected | Not Selected | Not Selected |
| [SA-8](#SA8) | Security Engineering Principles | P1 | Not Selected | SA-8 | SA-8 |
| [SA-9](#SA9) | External Information System Services | P1 | SA-9 | SA-9 (2) | SA-9 (2) |
| [SA-10](#SA10) | Developer Configuration Management | P1 | Not Selected | SA-10 | SA-10 |
| [SA-11](#SA11) | Developer Security Testing and Evaluation | P1 | Not Selected | SA-11 | SA-11 |
| [SA-12](#SA12) | Supply Chain Protection | P1 | Not Selected | Not Selected | SA-12 |
| [SA-13](#SA13) | Trustworthiness | P0 | Not Selected | Not Selected | Not Selected |
| [SA-14](#SA14) | Criticality Analysis | P0 | Not Selected | Not Selected | Not Selected |
| [SA-15](#SA15) | Development Process, Standards, and Tools | P2 | Not Selected | Not Selected | SA-15 |
| [SA-16](#SA16) | Developer-Provided Training | P2 | Not Selected | Not Selected | SA-16 |
| [SA-17](#SA17) | Developer Security Architecture and Design | P1 | Not Selected | Not Selected | SA-17 |
| [SA-18](#SA18) | Tamper Resistance and Detection | P0 | Not Selected | Not Selected | Not Selected |
| [SA-19](#SA19) | Component Authenticity | P0 | Not Selected | Not Selected | Not Selected |
| [SA-20](#SA20) | Customized Development of Critical Components | P0 | Not Selected | Not Selected | Not Selected |
| [SA-21](#SA21) | Developer Screening | P0 | Not Selected | Not Selected | Not Selected |
| [SA-22](#SA22) | Unsupported System Components | P0 | Not Selected | Not Selected | Not Selected |

Table 1 - SP-800-53v4 Compliance Matrix

# **SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES**

DoD Components are automatically compliant with this control because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1, which address system and services acquisition.

# **ALLOCATION OF RESOURCES**

Resource allocation for {ACRONYM} security includes funding for the initial system or information system service acquisition and funding for the sustainment of the system/service.

{ACRONYM} security requirements are documented in the Control Selection Form and Security Assessment Plan (SAP), which was created and approved during RMF Step 2 – Select Security Controls.

{ACRONYM} requires the following resources to implement and maintain cybersecurity requirements:

|  |  |
| --- | --- |
| Resource | Funded? |
| Project Manager | Choose an item. |
| System/Network Administrator | Choose an item. |
| Information System Security Officer | Choose an item. |
| Validator | Choose an item. |

Has {ACRONYM} identified and individual line item to support cybersecurity requirements?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

# **SYSTEM DEVELOPMENT LIFE CYCLE**

A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of information systems.

Does {ACRONYM} perform development activities?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If Yes, reference [Enclosure 1 “System Development Lifecycle”](#_Enclosure_1_–)

# **ACQUISITION PROCESS**

The acquisition process ensures that the technologies and architecture used by {ACRONYM} comply with DoD requirements.

{ACRONYM} will utilize the Incident Response Plan (IRP) to:

* respond to attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service
* document attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service
* record actions to obtain either unavailable or nonexistent documentation for information system, system component, or information system service

All {ACRONYM} components, or information system service documentation will be distributed to at a minimum, the ISSO, ISSM, and SCA.

All {ACRONYM} components, or information system service documentation will be stored and handled in accordance with the Physical and Environmental Protection Plan.

## **5.1 Architecture Characteristics**

The {ACRONYM} contains the following security characteristics:

Are DoD approved PKI tokens implemented for identify verification?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

Describe the PKI implementation, or lack thereof.

Does {ACRONYM} utilize commercially provided IA and IA-enabled IT products?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If Yes, have the products been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If No, do the products rely on FIPS-validated cryptographic modules?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

## **5.2 Design Information**

Design information provides the developer with the list of security controls that must be implemented for {ACRONYM}.

Does {ACRONYM} perform development activities?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If no, delete the following information.

If Yes, then within the {ACRONYM} Design Document, is the following information defined:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. | Design information that the developer of the information system, system component, or information system service is required to provide for the security controls to be employed? |  | No |  | Yes |
| 2. | Level of detail the design information of the security controls is required to be provided by the developer of the information system, system component, or information system services? |  | No |  | Yes |
| 3. | Level of detail the implementation information of the security controls is required to be provided by the developer of the information system, system component, or information system services? |  | No |  | Yes |

## **5.3 Contracts and Agreements**

Does {ACRONYM} perform development activities?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If no, delete the following information.

If Yes, then within the {ACRONYM} contracts/agreements, is the following information defined:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. | Identify the functions, ports, protocols, and services intended for organizational use? |  | No |  | Yes |
| 2. | Includes the security functional requirements, explicitly or by reference, in the acquisition contract? |  | No |  | Yes |
| 3. | Includes the security strength requirements, explicitly or by reference, in the acquisition contract? |  | No |  | Yes |
| 4. | Includes the security assurance requirements, explicitly or by reference, in the acquisition contract? |  | No |  | Yes |
| 5. | Includes the security-related documentation requirements, explicitly or by reference, in the acquisition contract? |  | No |  | Yes |
| 6. | Includes requirements for protecting security-related documentation, explicitly or by reference, in the acquisition contract? |  | No |  | Yes |
| 7. | Includes a description of the information system development environment and environment in which the system is intended to operate, explicitly or by reference, in the acquisition contract? |  | No |  | Yes |
| 8. | Includes acceptance criteria, explicitly or by reference, in the acquisition contract? |  | No |  | Yes |
| 9. | Requires that the developer provide administrator documentation for the information system, system component or information system service that describe secure configuration of the system, component, or service? |  | No |  | Yes |
| 10. | Requires that the developer provide administrator documentation for the information system, system component or information system service that describe secure installation of the system, component, or service? |  | No |  | Yes |
| 11. | Requires that the developer provide administrator documentation for the information system, system component or information system service that describe secure operation of the system, component, or service? |  | No |  | Yes |
| 12. | Requires that the developer provide administrator documentation for the information system, system component or information system service that describe effective use and maintenance of security functions/mechanisms? |  | No |  | Yes |
| 13. | Requires that the developer provide administrator documentation for the information system, system component or information system service that describe known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions? |  | No |  | Yes |
| 14. | Requires that the developer provide user documentation for the information system, system component or information system service that describes user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms? |  | No |  | Yes |
| 15. | Requires that the developer provide user documentation for the information system, system component or information system service that describes methods for user interaction which enables individuals to use the system, component, or service in a more secure manner? |  | No |  | Yes |
| 16. | Requires that the developer provide user documentation for the information system, system component or information system service that describes user responsibilities in maintaining the security of the system, component, or service? |  | No |  | Yes |
| 17. | Requires the developer of the information system, system component, or information system service to provide design information for the security controls to be employed that includes security-relevant external system interfaces, high-level design, low-level design, source code and/or hardware schematics and/or design/information |  | No |  | Yes |
| 18. | Requires the developer of the information system, system component, or information system service to provide implementation information for the security controls to be employed that includes security-relevant external system interfaces, high-level design, low-level design, source code and/or hardware schematics and/or implementation information |  | No |  | Yes |
|  |  |  |  |  |  |

# **INFORMATION SYSTEM DOCUMENTATION**

This section details the implementation and operation of security controls associated with {ACRONYM} components, and information system services.

SYSTEM NAME} will utilize the Incident Response Plan (IRP) to:

* respond to attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service
* document attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service
* record actions to obtain either unavailable or nonexistent documentation for information system, system component, or information system service

All {ACRONYM} components, or information system service documentation will be distributed to at a minimum, the ISSO, ISSM, and SCA.

All {ACRONYM} components, or information system service documentation will be stored and handled in accordance with the Physical and Environmental Protection Plan.

Does {ACRONYM} perform development activities?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If no, delete the following information.

If Yes, then within the {ACRONYM} contracts/agreements, is the following information defined:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. | Requires that the developer provide administrator documentation for the information system, system component or information system service that describe secure configuration of the system, component, or service? |  | No |  | Yes |
| 2. | Requires that the developer provide administrator documentation for the information system, system component or information system service that describe secure installation of the system, component, or service? |  | No |  | Yes |
| 3. | Requires that the developer provide administrator documentation for the information system, system component or information system service that describe secure operation of the system, component, or service? |  | No |  | Yes |
| 4. | Requires that the developer provide administrator documentation for the information system, system component or information system service that describe effective use and maintenance of security functions/mechanisms? |  | No |  | Yes |
| 5. | Requires that the developer provide administrator documentation for the information system, system component or information system service that describe known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions? |  | No |  | Yes |
| 6. | Requires that the developer provide user documentation for the information system, system component or information system service that describes user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms? |  | No |  | Yes |
| 7. | Requires that the developer provide user documentation for the information system, system component or information system service that describes methods for user interaction which enables individuals to use the system, component, or service in a more secure manner? |  | No |  | Yes |
| 8. | Requires that the developer provide user documentation for the information system, system component or information system service that describes user responsibilities in maintaining the security of the system, component, or service? |  | No |  | Yes |

# **SECURITY ENGINEERING PRINCIPLES**

Security engineering principles are primarily applied to new development information systems or systems undergoing major upgrades. For legacy systems, organizations apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems.

Security engineering principles include, developing layered protections; establishing sound security policy, architecture, and controls as the foundation for design; incorporating security requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that system developers are trained on how to build secure software; tailoring security controls to meet organizational and operational needs; 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; and reducing risk to acceptable levels, thus enabling informed risk management decisions,

Is {ACRONYM} a new development effort?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If no, delete the following information.

If yes,

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. | Do system requirements documents apply information system security engineering principles in the specification of the information system? |  | No |  | Yes |
| 2. | Do design documents apply information system security engineering principles in the design of the information system? |  | No |  | Yes |
| 3. | Do system development procedures (e.g. configuration management plans, code review procedures, and coding style guides) apply information system security engineering principles in the development of the information system? |  | No |  | Yes |
| 4. | Are changes made in accordance with the configuration management plan? |  | No |  | Yes |
| 5. | Does an audit trail of changes exist? |  | No |  | Yes |

# **EXTERNAL INFORMATION SYSTEM SERVICES**

External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems.

FISMA and OMB policy require that organizations using external service providers that are processing, storing, or transmitting federal information or operating information systems on behalf of the federal government ensure that such providers meet the same security requirements that federal agencies are required to meet.

Does {ACRONYM} acquire or outsource information security services?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If no, delete the following information.

If yes,

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. | Has an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services been performed? |  | No |  | Yes |
| 2. | Has the acquisition or outsourcing of dedicated information security services been approved by the DoD Component CIO or their delegate(s)? |  | No |  | Yes |
| 3. | Have the functions, ports, protocols, and other services required for the use of such services been identified? |  | No |  | Yes |
| 4. | Do external information system services comply with organization-specific information security requirements? |  | No |  | Yes |
| 5. | Do contracts/agreements require that providers of external information system services employ security controls defined in CNSSI 1253? |  | No |  | Yes |
| 6. | Does the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) clearly defined the government oversight to be conducted on external information system services and service providers? |  | No |  | Yes |
| 7. | Does the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) clearly established the government oversight to be conducted on external information system services and service providers? |  | No |  | Yes |
| 8. | Does the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) clearly defined the roles and responsibilities of all types of users of the external information system services? |  | No |  | Yes |
| 8. | Does the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) clearly established the roles and responsibilities of all types of users of the external information system services? |  | No |  | Yes |
| 10. | Are the processes, methods, and techniques defined in SA-9, CCI 3139 to monitor security control compliance by external service providers on an ongoing basis implemented? |  | No |  | Yes |
| 11. | Are the processes, methods, and techniques to employ to monitor security control compliance by external service providers on an ongoing basis implemented? |  | No |  | Yes |

# **DEVELOPER CONFIGURATION MANAGEMENT**

This section applies to internal information systems development and integration. The quality and completeness of the configuration management activities conducted by developers as evidence of applying effective security safeguards is considered. Safeguards include, for example, protecting from unauthorized modification or destruction, the master copies of all material used to generate security-relevant portions of the system hardware, software, and firmware.

Configuration items that are placed under configuration management (if existence/use is required by other security controls) include: the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and software/firmware source code with previous versions; and test fixtures and documentation.

Does {ACRONYM} perform system development?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If no, delete the following information.

If yes,

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. | Do contracts/agreements require that the developer of the information system, system component, or information system service enable integrity verification of software and firmware components? |  | No |  | Yes |
| 2. | Do contracts/agreements require the developer of the information system, system component, or information system service perform configuration management during system, component or service design, development, implementation and/or operation? |  | No |  | Yes |
| 3. | Do contracts/agreements require that the developer of the information system, system component, or information system service document the integrity of changes to configuration items under configuration management defined in SA-10, CCI 3159? |  | No |  | Yes |
| 4. | Do the contracts/agreements require that the developer of the information system, system component, or information system service manage the integrity of changes to configuration items under configuration management defined in SA-10, CCI 3159? |  | No |  | Yes |
| 5. | Do contracts/agreements require that the developer of the information system, system component, or information system service control the integrity of changes to configuration items under configuration management defined in SA-10, CCI 3159? |  | No |  | Yes |
| 6. | Is the documented configuration items ensure the organization being inspected/assessed defines the configuration items under configuration management that require the integrity of changes to be documented, managed and controlled? |  | No |  | Yes |
| 7. | Do contracts/agreements between the organization and the IS developer confirm the organization has established in its acquisition contracts/agreements the requirement that the IS developer implement only organization-approved changes to the system, component, or service throughout its life cycle? |  | No |  | Yes |
| 8. | Do contracts/agreements require that the developer of the information system, system component, or information system service document approved changes to the system, component, or service? |  | No |  | Yes |
| 8. | Do contracts/agreements require that the developer of the information system, system component, or information system service document the potential security impacts of approved changes to the system, component, or service? |  | No |  | Yes |
| 10. | Do contracts/agreements require that the developer of the information system, system component, or information system service track security flaws within the system, component, or service? |  | No |  | Yes |
| 11. | Do contracts/agreements require that the developer of the information system, system component, or information system service track flaw resolution within the system, component, or service? |  | No |  | Yes |
| 12. | Do contracts/agreements require that the developer of the information system, system component, or information system service report security flaws and flaw resolution within the system, component, or service findings to at a minimum, the ISSO and ISSM? |  | No |  | Yes |

# **DEVELOPER SECURITY TESTING AND EVALUATION**

Developmental security testing/evaluation occurs at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements.

Does {ACRONYM} perform system development?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If no, delete the following information.

If yes,

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. | Do contracts/agreements require that the developer of the information system, system component, or information system service create a security assessment plan? |  | No |  | Yes |
| 2. | Do contracts/agreements require that the developer of the information system, system component, or information system service implement a security assessment plan? |  | No |  | Yes |
| 3. | Do contracts/agreements require that the developer of the information system, system component, or information system service perform unit, integration, system, and/or regression testing/evaluation at depth and coverage defined in SA-11, CCI 3174? |  | No |  | Yes |
| 4. | Is the depth and coverage to perform unit, integration, system, and/or regression testing/evaluation defined? |  | No |  | Yes |
| 5. | Do contracts/agreements require that the developer of the information system, system component, or information system service produce evidence of the execution of the security assessment plan? |  | No |  | Yes |
| 6. | Do contracts/agreements require that the developer of the information system, system component, or information system service produce the results of the security testing/evaluation? |  | No |  | Yes |
| 7. | Do contracts/agreements require that the developer of the information system, system component, or information system service implement a verifiable flaw remediation process? |  | No |  | Yes |
| 8. | Do contracts/agreements require that the developer of the information system, system component, or information system service correct flaws identified during security testing/evaluation and provide evidence? |  | No |  | Yes |

# **SUPPLY CHAIN PROTECTION**

Information systems (including system components that compose those systems) need to be protected throughout the system development life cycle (i.e., during design, development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). Protection of organizational information systems is accomplished through threat awareness, by the identification, management, and reduction of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to respond to risk.

Is {ACRONYM} a “covered system” IAW DoDI 5200.44?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If no, delete the following information.

If yes,

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. | Has a criticality analysis to identify mission critical functions and critical components and reduced the vulnerability of such functions and components through secure system design been conducted? |  | No |  | Yes |
| 2. | Has a threat analysis of suppliers of critical components from the TSN focal point and managed access to and control of threat analysis products containing U.S. person information been performed? |  | No |  | Yes |
| 3. | Have TSN focal points for guidance on managing identified risk using DoD Components and Enterprise risk management resources been engaged? |  | No |  | Yes |
| 4. | Have TSN best practices, processes, techniques, and procurement tools prior to the acquisition of critical components or their integration into applicable systems, at any point in the system lifecycle been applied? |  | No |  | Yes |

# **DEVELOPMENT PROCESS, STANDARDS, AND TOOLS**

Development tools include, for example, programming languages and computer-aided design (CAD) systems. Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes enables accurate supply chain risk assessment and mitigation, and requires robust configuration control throughout the life cycle (including design, development, transport, delivery, integration, and maintenance) to track authorized changes and prevent unauthorized changes.

Does {ACRONYM} perform system development?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If no, delete the following information.

If yes,

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. | Do contracts/agreements require that the developer of the information system, system component, or information system service to follow a documented development process? |  | No |  | Yes |
| 2. | Do the documented process as well as the record of approvals approve the use of live data in development environments for the information system, system component, or information system service? |  | No |  | Yes |
| 3. | Do the documented process as well as the record of approvals approve the use of live data in test environments for the information system, system component, or information system service? |  | No |  | Yes |
| 4. | Is live data in development environments for the information system, system component, or information system service documented? |  | No |  | Yes |
| 5. | Is live data in test environments for the information system, system component, or information system service documented? |  | No |  | Yes |
| 6. | Is the use of live data in development environments for the information system, system component, or information system service controlled? |  | No |  | Yes |
| 7. | Is the use of live data in test environments for the information system, system component, or information system service controlled? |  | No |  | Yes |
| 8. | Do contracts/agreements require that the developer of the information system, system component, or information system service explicitly addresses security requirements? |  | No |  | Yes |
| 9. | Do contracts/agreements require that the developer of the information system, system component, or information system service identifies the standards used in the development process? |  | No |  | Yes |
| 10. | Do contracts/agreements require that the developer of the information system, system component, or information system service identifies the tools used in the development process? |  | No |  | Yes |
| 11. | Do contracts/agreements require that the developer of the information system, system component, or information system service documents the specific tool options and tool configurations used in the development process? |  | No |  | Yes |
| 12. | Do contracts/agreements require that the developer of the information system, system component, or information system service documents changes to the process and/or tools used in development? |  | No |  | Yes |
| 13. | Do contracts/agreements require that the developer of the information system, system component, or information system service document a process to manage changes to the process and/or tools used in development? |  | No |  | Yes |
| 14. | Do contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service document the integrity of changes to the process and/or tools used in development? |  | No |  | Yes |
| 15. | Is the development process reviewed before first use and annually thereafter to determine if the development process selected and employed can satisfy the security requirements defined in SA-15, CCI 3246 |  | No |  | Yes |
| 16. | Are development standards reviewed before first use and annually thereafter to determine if the development standards selected and employed can satisfy the security requirements defined in SA-15, CCI 3246? |  | No |  | Yes |
| 17. | Are development tools reviewed before first use and annually thereafter to determine if the development tools selected and employed can satisfy the security requirements defined in SA-15, CCI 3246? |  | No |  | Yes |
| 18. | Are development tool options/configurations reviewed before first use and annually thereafter to determine if the development tool options/configurations selected and employed can satisfy the security requirements defined in SA-15, CCI 3246? |  | No |  | Yes |
| 19. | Are the security requirements that must be satisfied by conducting a review of the development process, standards, tools, and tool options/configurations defined? |  | No |  | Yes |

# **COMPONENT AUTHENTICITY**

Anti-counterfeiting policy and procedures support tamper resistance and provide a level of protection against the introduction of malicious code.

{ACRONYM} follows DoDI 4140.67, "DoD Counterfeit Prevention Policy" as its documented anti-counterfeit policy, which implements the following:

* detect counterfeit components from entering the information system
* prevent counterfeit components from entering the information system
* report counterfeit information system components to source of counterfeit component, at a minimum, USCYBERCOM. And/or at a minimum, the ISSO, ISSM, and PM

# **APPENDIX A – DETAILED COMPLIANCE MATRIX**

The following table provides traceability between this document and the Assessment Procedures contained within NIST Special Publication 800-53A Revision 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations".

| **Control Number** | **Assessment Number** | **CCI** | **Confidentiality** | **Integrity** | **Availability** | **Assessment Procedures** | **Reference** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| SA-1 | SA-1 (a) | CCI-003089 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles as all personnel. | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-1 | SA-1 (a) | CCI-003090 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles as all personnel. | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-1 | SA-1 (a) (1) | CCI-000602 | High Moderate Low | High Moderate Low | High Moderate Low | DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures.   DoD Components are automatically compliant with this control because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1. | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-1 | SA-1 (a) (1) | CCI-000603 | High Moderate Low | High Moderate Low | High Moderate Low | DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures.   DoD Components are automatically compliant with this control because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1. | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-1 | SA-1 (a) (2) | CCI-000605 | High Moderate Low | High Moderate Low | High Moderate Low | DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures.   DoD Components are automatically compliant with this control because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1. | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-1 | SA-1 (a) (2) | CCI-000606 | High Moderate Low | High Moderate Low | High Moderate Low | DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures.   DoD Components are automatically compliant with this control because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1. | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-1 | SA-1 (b) (1) | CCI-000601 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as every 5 years. | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-1 | SA-1 (b) (1) | CCI-000604 | High Moderate Low | High Moderate Low | High Moderate Low | DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures.   DoD Components are automatically compliant with this control because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1. | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-1 | SA-1 (b) (2) | CCI-001646 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-1 | SA-1 (b) (2) | CCI-000607 | High Moderate Low | High Moderate Low | High Moderate Low | DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures.   DoD Components are automatically compliant with this control because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1. | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-10 (1) | SA-10 (1) | CCI-000698 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service enable integrity verification of software and firmware components. | [Section 9](#_DEVELOPER_CONFIGURATION_MANAGEMENT) |
| SA-10 (2) | SA-10 (2) | CCI-000700 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the Configuration Control Board (CCB) charter to determine if the organization, in the absence of a dedicated software developer configuration management team, has established an alternate configuration management process that is staffed with key organizational personnel. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-10 (3) | SA-10 (3) | CCI-003165 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service enable integrity verification of hardware components. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-10 (4) | SA-10 (4) | CCI-003166 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service employ tools for comparing newly generated versions of security-relevant hardware descriptions with previous versions. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-10 (4) | SA-10 (4) | CCI-003167 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service employ tools for comparing newly generated versions of software/firmware source code with previous versions. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-10 (4) | SA-10 (4) | CCI-003168 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service employ tools for comparing newly generated versions of object code with previous versions. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-10 (5) | SA-10 (5) | CCI-003169 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service maintain the integrity of the mapping between the master build data (hardware drawings and software/firmware code) describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-10 (6) | SA-10 (6) | CCI-003170 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-10 | SA-10 (a) | CCI-003155 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires the developer of the information system, system component, or information system service perform configuration management during system, component or service design, development, implementation and/or operation. | [Section 9](#_DEVELOPER_CONFIGURATION_MANAGEMENT) |
| SA-10 | SA-10 (b) | CCI-003156 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service document the integrity of changes to configuration items under configuration management defined in SA-10, CCI 3159. | [Section 9](#_DEVELOPER_CONFIGURATION_MANAGEMENT) |
| SA-10 | SA-10 (b) | CCI-003157 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service manage the integrity of changes to configuration items under configuration management defined in SA-10, CCI 3159. | [Section 9](#_DEVELOPER_CONFIGURATION_MANAGEMENT) |
| SA-10 | SA-10 (b) | CCI-003158 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service control the integrity of changes to configuration items under configuration management defined in SA-10, CCI 3159. | [Section 9](#_DEVELOPER_CONFIGURATION_MANAGEMENT) |
| SA-10 | SA-10 (b) | CCI-003159 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented configuration items to ensure the organization being inspected/assessed defines the configuration items under configuration management that require the integrity of changes to be documented, managed and controlled.   DoD has determined the configuration items are not appropriate to define at the Enterprise level. | [Section 9](#_DEVELOPER_CONFIGURATION_MANAGEMENT) |
| SA-10 | SA-10 (c) | CCI-000692 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines contracts/agreements between the organization and the IS developer to confirm the organization has established in its acquisition contracts/agreements the requirement that the IS developer implement only organization-approved changes to the system, component, or service throughout its life cycle. | [Section 9](#_DEVELOPER_CONFIGURATION_MANAGEMENT) |
| SA-10 | SA-10 (d) | CCI-000694 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service document approved changes to the system, component, or service. | [Section 9](#_DEVELOPER_CONFIGURATION_MANAGEMENT) |
| SA-10 | SA-10 (d) | CCI-003160 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service document the potential security impacts of approved changes to the system, component, or service. | [Section 9](#_DEVELOPER_CONFIGURATION_MANAGEMENT) |
| SA-10 | SA-10 (e ) | CCI-003161 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service track security flaws within the system, component, or service. | [Section 9](#_DEVELOPER_CONFIGURATION_MANAGEMENT) |
| SA-10 | SA-10 (e) | CCI-003162 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service track flaw resolution within the system, component, or service. | [Section 9](#_DEVELOPER_CONFIGURATION_MANAGEMENT) |
| SA-10 | SA-10 (e) | CCI-003163 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service report security flaws and flaw resolution within the system, component, or service findings to at a minimum, the ISSO and ISSM.    DoD has defined the personnel as at a minimum, the ISSO and ISSM. | [Section 9](#_DEVELOPER_CONFIGURATION_MANAGEMENT) |
| SA-10 | SA-10 (e) | CCI-003164 |  | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel as at a minimum, the ISSO and ISSM. | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-11 (1) | SA-11 (1) | CCI-003179 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service employ static code analysis tools to identify common flaws. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-11 (1) | SA-11 (1) | CCI-003180 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service document the results of static code analysis. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-11 (2) | SA-11 (2) | CCI-003181 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service perform threat and vulnerability analysis. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-11 (2) | SA-11 (2) | CCI-003182 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service perform testing/evaluation of the as-built system, component, or service subsequent to threat and vulnerability analysis. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-11 (3) | SA-11 (3) (a) | CCI-003183 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that an independent agent satisfying independence criteria defined in SA-11 (3), CCI 3185 verify the correct implementation of the developer security assessment plan. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-11 (3) | SA-11 (3) (a) | CCI-003184 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that an independent agent satisfying independence criteria defined in SA-11 (3), CCI 3185 verify the evidence produced during security testing/evaluation. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-11 (3) | SA-11 (3) (a) | CCI-003185 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented independence criteria to ensure the organization being inspected/assessed defines the independence criteria the independent agent must satisfy prior to verifying the correct implementation of the developer security assessment plan and the evidence produced during security testing/evaluation.   DoD has determined the independence criteria is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-11 (3) | SA-11 (3) (b) | CCI-003186 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the record of information provided to ensure the organization being inspected/assessed provides the independent agent with sufficient information and access/authority to complete the verification process. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-11 (4) | SA-11 (4) | CCI-003187 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service perform a manual code review of specific code defined in SA-11 (4), CCI 3188 using processes, procedures, and/or techniques defined in SA-11 (4), CCI 3189. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-11 (4) | SA-11 (4) | CCI-003188 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented specific code to ensure the organization being inspected/assessed defines the specific code that requires the developer of the information system, system component, or information system service to perform a manual code review against using organization-defined process, procedures, and/or techniques.   DoD has determined the specific code is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-11 (4) | SA-11 (4) | CCI-003189 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented processes, procedures, and/or techniques to ensure the organization being inspected/assessed defines the processes, procedures, and/or techniques to be used by the developer of the information system, system component, or information system service to perform a manual code review of organization-defined specific code.   DoD has determined the processes, procedures, and/or techniques are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-11 (5) | SA-11 (5) | CCI-003190 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service perform penetration testing at a breadth/depth defined in SA-11 (5), CCI 3191 and with constraints defined in SA-11 (5), CCI 3192. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-11 (5) | SA-11 (5) | CCI-003191 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented breadth/depth to ensure the organization being inspected/assessed defines the breadth/depth the developer of the information system, system component, or information system service is required to perform penetration testing.   DoD has determined the constraints are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-11 (5) | SA-11 (5) | CCI-003192 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented constraints to ensure the organization being inspected/assessed defines the constraints on penetration testing performed by developer of the information system, system component, or information system service.   DoD has determined the constraints are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-11 (6) | SA-11 (6) | CCI-003193 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service perform and document attack surface reviews. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-11 (7) | SA-11 (7) | CCI-003194 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service verify that the scope of security testing/evaluation provides complete coverage of required security controls at the depth of testing/evaluation defined in SA-11 (7), CCI 3195. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-11 (7) | SA-11 (7) | CCI-003195 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented depth of testing/evaluation to ensure the organization being inspected/assessed defines the depth of testing/evaluation to which the developer of the information system, system component, or information system service is required to verify that the scope of security testing/evaluation provides complete coverage of the required security controls.   DoD has determined the depth of testing/evaluation is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-11 (8) | SA-11 (8) | CCI-003196 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service employ dynamic code analysis tools to identify common flaws. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-11 (8) | SA-11 (8) | CCI-003197 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service document the results of the dynamic code analysis. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-11 | SA-11 (a) | CCI-003171 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service create a security assessment plan. | [Section 10](#_DEVELOPER_SECURITY_TESTING) |
| SA-11 | SA-11 (a) | CCI-003172 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service implement a security assessment plan. | [Section 10](#_DEVELOPER_SECURITY_TESTING) |
| SA-11 | SA-11 (b) | CCI-003173 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service perform unit, integration, system, and/or regression testing/evaluation at depth and coverage defined in SA-11, CCI 3174. | [Section 10](#_DEVELOPER_SECURITY_TESTING) |
| SA-11 | SA-11 (b) | CCI-003174 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the documented depth and coverage to ensure the organization being inspected/assessed defines the depth and coverage to perform unit, integration, system, and/or regression testing/evaluation.   DoD has determined the depth and coverage are not appropriate to define at the Enterprise level. | [Section 10](#_DEVELOPER_SECURITY_TESTING) |
| SA-11 | SA-11 (c) | CCI-003175 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service produce evidence of the execution of the security assessment plan. | [Section 10](#_DEVELOPER_SECURITY_TESTING) |
| SA-11 | SA-11 (c) | CCI-003176 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service produce the results of the security testing/evaluation. | [Section 10](#_DEVELOPER_SECURITY_TESTING) |
| SA-11 | SA-11 (d) | CCI-003177 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service implement a verifiable flaw remediation process. | [Section 10](#_DEVELOPER_SECURITY_TESTING) |
| SA-11 | SA-11 (e) | CCI-003178 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service correct flaws identified during security testing/evaluation and provide evidence. | [Section 10](#_DEVELOPER_SECURITY_TESTING) |
| SA-12 | SA-12 | CCI-000723 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the Security Plan for the system to determine whether the system is a “covered system” IAW DoDI 5200.44.   If it is a covered system, the organization conducting the inspection/assessment obtains and examines documentation of compliance with DoDI 5200.44, to ensure the organization being inspected/assessed has: 1. Conducted a criticality analysis to identify mission critical functions and critical components and reduced the vulnerability of such functions and components through secure system design; 2. Requested threat analysis of suppliers of critical components from the TSN focal point and managed access to and control of threat analysis products containing U.S. person information; 3. Engaged TSN focal points for guidance on managing identified risk using DoD Components and Enterprise risk management resources; and 4. Applied TSN best practices, processes, techniques, and procurement tools prior to the acquisition of critical components or their integration into applicable systems, at any point in the system lifecycle. Such tools and practices include contract requirements and the SCRM key practices Guide. | [Section 11](#_SUPPLY_CHAIN_PROTECTION) |
| SA-12 | SA-12 | CCI-000722 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the requirements to protect against supply chain threats in DoDI 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)." | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-12 (1) | SA-12 (1) | CCI-003198 | High | High | High | The organization conducting the inspection/assessment obtains and examines documentation tracing the strategies, tools, and methods implemented to the organization-defined strategies, tools, and methods to ensure that the tailored acquisition strategies, contract tools, and procurement methods identified in SA-12 (1), CCI 3199 have been implemented. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-12 (1) | SA-12 (1) | CCI-003199 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documentation containing the tailored acquisition strategies, contract tools, and procurement methods to ensure they have been defined IAW DoDI 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)."  DoD has determined the tailored acquisition strategies, contract tools, and procurement methods are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-12 (10) | SA-12 (10) | CCI-003212 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the record of information system validation to ensure the organization being inspected/assessed employs security safeguards defined in SA-12 (10), CCI 3213 to validate that the information system or system component received is genuine and has not been altered.   DoD has determined the security safeguards are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-12 (10) | SA-12 (10) | CCI-003213 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure they have been defined IAW DoDI 5200.44.  DoD has determined the security safeguards are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-12 (11) | SA-12 (11) | CCI-003214 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented processes to ensure the organization being inspected/assessed employs organizational analysis, independent third-party analysis, organizational penetration testing and/or independent third-party penetration testing of supply chain elements, processes and actors defined in SA-12 (11), CCI 3215 associated with the information system, system component, or information system service. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-12 (11) | SA-12 (11) | CCI-003215 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented supply chain elements, processes, and actors to ensure the organization being inspected/assessed defines the supply chain elements, processes, and actors associated with the information system, system component, or information system service for organizational analysis, independent third-party analysis, organizational penetration testing and/or independent third-party penetration testing IAW DoDI 5200.44.   DoD has determined the elements, processes, and actions are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-12 (12) | SA-12 (12) | CCI-003216 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented inter-organizational agreements to ensure the organization being inspected/assessed establishes inter-organizational agreements with entities involved in the supply chain for the information system, system component, or information system service. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-12 (12) | SA-12 (12) | CCI-003217 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented inter-organizational procedures to ensure the organization being inspected/assessed establishes inter-organizational procedures with entities involved in the supply chain for the information system, system component, or information system service. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-12 (13) | SA-12 (13) | CCI-003218 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed employs security safeguards defined by SA-12 (13), CCI 3219 to ensure an adequate supply of critical information system components defined in SA-12 (13), CCI 3220. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-12 (13) | SA-12 (13) | CCI-003219 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed defines the security safeguards to be employed to ensure an adequate supply of organization-defined critical information system components.  DoD has determined the security safeguards are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-12 (13) | SA-12 (13) | CCI-003220 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented critical information system components to ensure the organization being inspected/assessed defines the critical information system components for which organization-defined security safeguards are employed to ensure adequate supply.   DoD has determined the critical information system components are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-12 (14) | SA-12 (14) | CCI-003223 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented elements, processes, and actors to ensure the organization being inspected/assessed defines the supply chain elements, processes, and actors for the information system, system component, or information system service to establish and retain unique identification IAW DoDI 5200.44.   DoD has determined the elements, processes, and actors are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-12 (14) | SA-12 (14) | CCI-003221 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented unique identification of supply chain elements, processes, and actors to ensure the organization being inspected/assessed establishes unique identification of supply chain elements, processes, and actors defined in SA-12 (14), CCI 3223 for the information system, system component, or information system service. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-12 (14) | SA-12 (14) | CCI-003222 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines previous versions of the identification of supply chain elements, processes, and actors documented IAW SA-12 (14), CCI 3221 to ensure the organization being inspected/assessed retains unique identification of supply chain elements, processes, and actors. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-12 (15) | SA-12 (15) | CCI-003224 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed establishes a process to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-12 (2) | SA-12 (2) | CCI-003200 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of supplier review to ensure the organization being inspected/assessed documents and implements a process to conduct a supplier review prior to entering into a contractual agreement to acquire the information system, system component, or information system service. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-12 (5) | SA-12 (5) | CCI-003201 | High | High | High | The organization conducting the inspection/assessment obtains and examines the record of security safeguards supplied to ensure the organization being inspected/assessed employs security safeguards defined in SA-12 (5), CCI 3202 to limit harm from potential adversaries identifying and targeting the organizational supply chain. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-12 (5) | SA-12 (5) | CCI-003202 | High | High | High | The conducting the inspection/assessment obtains and examines the documented security safeguards to ensure they have been defined IAW DoDI 5200.44.  DoD has determined the security safeguards are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-12 (7) | SA-12 (7) | CCI-003203 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines documented assessment(s) that were conducted by the organization prior to selection, acceptance, or update to ensure that the organization being inspected/assessed is assessing information systems, system components, or information system services prior to selection, acceptance, or update. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-12 (8) | SA-12 (8) | CCI-003205 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process IAW DoDI 5200.44 to use all-source intelligence analysis of suppliers and potential suppliers of the information system, system component, or information system service. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-12 (9) | SA-12 (9) | CCI-003210 | High | High | High | The organization being inspected/assessed obtains and examines the documented OPSEC safeguards to ensure they have been defined IAW DoDD 5205.02E, DoD Manual 5205.02, and DoDI 5200.44.   DoD has determined the OPSEC safeguards are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-12 (9) | SA-12 (9) | CCI-003206 | High | High | High | The organization conducting the inspection/assessment obtains and examines any applicable artifacts showing the use of OPSEC safeguards to ensure the organization being inspected/assessed implements OPSEC safeguards defined in SA-12 (9), CCI 3206 to protect supply chain-related information for the information system, system component, or information system service.   DoD has determined the OPSEC safeguards are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-13 | SA-13 (a) | CCI-003225 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed documents within its security plan the trustworthiness required in the information system, information system component, or information system service defined in SA-13, CCI 3226 supporting its critical mission’s/business functions. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-13 | SA-13 (a) | CCI-003226 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system, information system component, or information system service to ensure the organization being inspected/assessed defines the information system, information system component, or information system service supporting its critical mission’s/business functions in which the trustworthiness must be described.    DoD has determined the information system, information system component, or information system service is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-13 | SA-13 (b) | CCI-003227 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed implements an assurance overlay defined in SA-13, CCI 3228 to achieve trustworthiness required to support its critical mission’s/business functions. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-13 | SA-13 (b) | CCI-003228 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented assurance overlay to ensure the organization being inspected/assessed defines an assurance overlay to be implemented to achieve trustworthiness required to support its critical mission’s/business functions.   DoD has determined the assurance overlay is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-14 | SA-14 | CCI-003229 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed identifies critical information system components by performing a criticality analysis for information systems, information system components, or information system services IAW DoDI 5200.44. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-14 | SA-14 | CCI-003230 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented information system functions to ensure the organization being inspected/assessed identifies critical information system functions by performing a criticality analysis for information systems, information system components, or information system services IAW DoDI 5200.44. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-14 | SA-14 | CCI-003231 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented information systems, information system components, or information system services to ensure they have been defined IAW DoDI 5200.44.  DoD has determined the information systems, information system components, or information system services are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-14 | SA-14 | CCI-003232 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented decision points to ensure they have been defined IAW DoDI 5200.44 and DoDI 5000.2.   DoD has determined the decision points are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 | SA-15 | CCI-003233 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service to follow a documented development process. | [Section 12](#_DEVELOPMENT_PROCESS,_STANDARDS,) |
| SA-15 (1) | SA-15 (1) (a) | CCI-003247 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service define quality metrics at the beginning of the development process. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-15 (1) | SA-15 (1) (b) | CCI-003248 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service provide evidence of meeting the quality metrics in accordance with the frequency defined in SA-15 (1), CCI 3249, at a minimum, program review milestones IAW DoD Memorandum "Document Streamlining - Program Protection Plan (PPP)" and/or upon delivery.  DoD has defined the program review milestones as at a minimum, program review milestones IAW DoD Memorandum "Document Streamlining - Program Protection Plan (PPP)." | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-15 (1) | SA-15 (1) (b) | CCI-003249 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented frequency to ensure the organization being inspected/assessed defines the frequency that is required by the developer of the information system, system component, or information system service to provide evidence of meeting the quality metrics.   DoD has determined the frequency is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-15 (1) | SA-15 (1) (b) | CCI-003250 | blank | blank | blank | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.  DoD has defined the program review milestones as at a minimum, program review milestones IAW DoD Memorandum "Document Streamlining - Program Protection Plan (PPP)." | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-15 (10) | SA-15 (10) | CCI-003289 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service provide an incident response plan. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-15 (11) | SA-15 (11) | CCI-003290 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service be released or delivered together with the corresponding evidence supporting the final security review. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-15 (2) | SA-15 (2) | CCI-003251 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service select a security tracking tool for use during the development process. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-15 (2) | SA-15 (2) | CCI-003252 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service employ a security tracking tool for use during the development process. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-15 (3) | SA-15 (3) | CCI-003253 | High | High | High | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service perform a criticality analysis at the breadth/depth IAW DoDI 5200.44. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (3) | SA-15 (3) | CCI-003254 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented breadth/depth to ensure the organization being inspected/assessed defines the breadth/depth the developer of the information system, system component, or information system service is required to perform a criticality analysis IAW DoDI 5200.44.  DoD has determined the breadth/depth are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (3) | SA-15 (3) | CCI-003255 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented decision points to ensure the organization being inspected/assessed defines decision points in the system development life cycle the developer of the information system, system component, or information system service is required to perform a criticality analysis IAW DoDI 5200.44 and DoDI 5000.2.  DoD has determined the decision points are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (4) | SA-15 (4) | CCI-003256 | High | High | High | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developers perform threat modeling for the information system at the breadth/depth defined in SA-15 (4), CCI 3258. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (4) | SA-15 (4) | CCI-003257 | High | High | High | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developers perform a vulnerability analysis for the information system at the breadth/depth defined in SA-15 (4), CCI 3259. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (4) | SA-15 (4) | CCI-003258 | High | High | High | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developers perform threat modeling for the information system at the breadth/depth defined in SA-15 (4), CCI 3258. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (4) | SA-15 (4) | CCI-003259 | High | High | High | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developers perform a vulnerability analysis for the information system at the breadth/depth defined in SA-15 (4), CCI 3259. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (4) | SA-15 (4) (a) | CCI-003260 | High | High | High | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed documents within their contracts/agreements, their requirement that the developer's threat modeling include the use of information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels defined in SA-15 (4), CCI 3262. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (4) | SA-15 (4) (a) | CCI-003261 | High | High | High | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed documents within their contracts/agreements, their requirement that the developer's vulnerability analysis include the use of information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels defined in SA-15 (4), CCI 3263. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (4) | SA-15 (4) (a) | CCI-003262 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented information to ensure the organization being inspected/assessed defines information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels to be used to perform threat modeling for the information system by the developer.   DoD has determined the information is not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (4) | SA-15 (4) (a) | CCI-003263 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented information to ensure the organization being inspected/assessed defines information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels to be used to perform a vulnerability analysis for the information system by the developer.     DoD has determined the information is not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (4) | SA-15 (4) (b) | CCI-003264 | High | High | High | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the threat modeling performed by the developers employ the tools and methods defined in SA-15 (4), CCI 3266. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (4) | SA-15 (4) (b) | CCI-003265 | High | High | High | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the vulnerability analysis performed by the developers employ the tools and methods defined in SA-15 (4), CCI 3267. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (4) | SA-15 (4) (b) | CCI-003266 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented tools and methods to ensure the organization being inspected/assessed defines tools and methods to be employed to perform threat modeling for the information system by the developer.   DoD has determined the tools and methods are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (4) | SA-15 (4) (b) | CCI-003267 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented tools and methods to ensure the organization being inspected/assessed defines tools and methods to be employed to perform a vulnerability analysis for the information system by the developer.   DoD has determined the tools and methods are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (4) | SA-15 (4) (c) | CCI-003268 | High | High | High | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developers performing threat modeling for the information system produces evidence that meet the acceptance criteria defined in SA-15 (4), CCI 3270. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (4) | SA-15 (4) (c) | CCI-003269 | High | High | High | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the vulnerability analysis performed by the developers performing vulnerability analysis for the information system produces evidence that meet the acceptance criteria defined in SA-15 (4), CCI 3271. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (4) | SA-15 (4) (c) | CCI-003270 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented acceptance criteria to ensure the organization being inspected/assessed defines the acceptance criteria that must be met when threat modeling of the information system is performed by the developer.   DoD has determined the acceptance criteria is not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (4) | SA-15 (4) (c) | CCI-003271 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented acceptance criteria to ensure the organization being inspected/assessed defines the acceptance criteria that must be met when vulnerability analysis of the information system is performed by the developer.   DoD has determined the acceptance criteria is not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (5) | SA-15 (5) | CCI-003272 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service reduce attack surfaces to thresholds defined in SA-15 (5), CCI 3273. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-15 (5) | SA-15 (5) | CCI-003273 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented thresholds to ensure the organization being inspected/assessed defines the thresholds that the developer of the information system, system component, or information system service is required to reduce attack surfaces.   DoD has determined the thresholds are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-15 (6) | SA-15 (6) | CCI-003274 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service implement an explicit process to continuously improve the development process. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-15 (7) | SA-15 (7) (a) | CCI-003275 |  | High |  | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service perform an automated vulnerability analysis using the tools defined in SA-15 (7), CCI 3276. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (7) | SA-15 (7) (a) | CCI-003276 |  | High |  | The organization conducting the inspection/assessment obtains and examines the documented tools to ensure the organization being inspected/assessed defines the tools the developer of the information system, system component, or information system services uses to perform an automated vulnerability analysis.   DoD has determined the tools are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (7) | SA-15 (7) (b) | CCI-003277 |  | High |  | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service determine the exploitation potential for discovered vulnerabilities. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (7) | SA-15 (7) (c) | CCI-003278 |  | High |  | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service determine potential risk mitigations for delivered vulnerabilities. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (7) | SA-15 (7) (d) | CCI-003279 |  | High |  | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service deliver the outputs of the tools and results of the vulnerability analysis to the ISSO, ISSM, and PM.   DoD has defined the personnel or roles as the ISSO, ISSM, and PM. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-15 (7) | SA-15 (7) (d) | CCI-003280 |  | High |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles as the ISSO, ISSM, and PM. | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-15 (8) | SA-15 (8) | CCI-003281 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service use threat modeling from similar systems, components, or services to inform the current development process. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-15 (8) | SA-15 (8) | CCI-003282 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service use vulnerability analysis from similar systems, components, or services to inform the current development process. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-15 (9) | SA-15 (9) | CCI-003283 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of approvals to ensure the organization being inspected/assessed approves the use of live data in development environments for the information system, system component, or information system service. | [Section 12](#_DEVELOPMENT_PROCESS,_STANDARDS,) |
| SA-15 (9) | SA-15 (9) | CCI-003284 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of approvals to ensure the organization being inspected/assessed approves the use of live data in test environments for the information system, system component, or information system service. | [Section 12](#_DEVELOPMENT_PROCESS,_STANDARDS,) |
| SA-15 (9) | SA-15 (9) | CCI-003285 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the documented use of live data in test environments to ensure the organization being inspected/assessed documents the use of live data in development environments for the information system, system component, or information system service. | [Section 12](#_DEVELOPMENT_PROCESS,_STANDARDS,) |
| SA-15 (9) | SA-15 (9) | CCI-003286 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the documented use of live data in test environments to ensure the organization being inspected/assessed documents the use of live data in test environments for the information system, system component, or information system service. | [Section 12](#_DEVELOPMENT_PROCESS,_STANDARDS,) |
| SA-15 (9) | SA-15 (9) | CCI-003287 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed controls the use of live data in development environments for the information system, system component, or information system service. | [Section 12](#_DEVELOPMENT_PROCESS,_STANDARDS,) |
| SA-15 (9) | SA-15 (9) | CCI-003288 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed controls the use of live data in test environments for the information system, system component, or information system service. | [Section 12](#_DEVELOPMENT_PROCESS,_STANDARDS,) |
| SA-15 | SA-15 (a) (1) | CCI-003234 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service explicitly addresses security requirements. | [Section 12](#_DEVELOPMENT_PROCESS,_STANDARDS,) |
| SA-15 | SA-15 (a) (2) | CCI-003235 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service identifies the standards used in the development process. | [Section 12](#_DEVELOPMENT_PROCESS,_STANDARDS,) |
| SA-15 | SA-15 (a) (2) | CCI-003236 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service identifies the tools used in the development process. | [Section 12](#_DEVELOPMENT_PROCESS,_STANDARDS,) |
| SA-15 | SA-15 (a) (3) | CCI-003237 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service documents the specific tool options and tool configurations used in the development process. | [Section 12](#_DEVELOPMENT_PROCESS,_STANDARDS,) |
| SA-15 | SA-15 (a) (4) | CCI-003238 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service documents changes to the process and/or tools used in development. | [Section 12](#_DEVELOPMENT_PROCESS,_STANDARDS,) |
| SA-15 | SA-15 (a) (4) | CCI-003239 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service document a process to manage changes to the process and/or tools used in development. | [Section 12](#_DEVELOPMENT_PROCESS,_STANDARDS,) |
| SA-15 | SA-15 (a) (4) | CCI-003240 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service document the integrity of changes to the process and/or tools used in development. | [Section 12](#_DEVELOPMENT_PROCESS,_STANDARDS,) |
| SA-15 | SA-15 (b) | CCI-003241 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews the development process before first use and annually thereafter to determine if the development process selected and employed can satisfy the security requirements defined in SA-15, CCI 3246.   DoD has defined the frequency as before first use and annually thereafter. | [Section 12](#_DEVELOPMENT_PROCESS,_STANDARDS,) |
| SA-15 | SA-15 (b) | CCI-003242 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews the development standards before first use and annually thereafter to determine if the development standards selected and employed can satisfy the security requirements defined in SA-15, CCI 3246.   DoD has defined the frequency as before first use and annually thereafter. | [Section 12](#_DEVELOPMENT_PROCESS,_STANDARDS,) |
| SA-15 | SA-15 (b) | CCI-003243 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews the development tools before first use and annually thereafter to determine if the development tools selected and employed can satisfy the security requirements defined in SA-15, CCI 3246.   DoD has defined the frequency as before first use and annually thereafter. | [Section 12](#_DEVELOPMENT_PROCESS,_STANDARDS,) |
| SA-15 | SA-15 (b) | CCI-003244 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews the development tool options/configurations before first use and annually thereafter to determine if the development tool options/configurations selected and employed can satisfy the security requirements defined in SA-15, CCI 3246.   DoD has defined the frequency as before first use and annually thereafter. | [Section 12](#_DEVELOPMENT_PROCESS,_STANDARDS,) |
| SA-15 | SA-15 (b) | CCI-003246 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented security requirements to ensure the organization being inspected/assessed defines the security requirements that must be satisfied by conducting a review of the development process, standards, tools, and tool options/configurations.   DoD has determined the security requirements are not appropriate to define at the Enterprise level. | [Section 12](#_DEVELOPMENT_PROCESS,_STANDARDS,) |
| SA-15 | SA-15 (b) | CCI-003245 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as before first use and annually thereafter. | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-16 | SA-16 | CCI-003292 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented training to ensure the organization being inspected/assessed defines the training the developer of the information system, system component, or information system service is required to provide on the correct use and operation of the implemented security functions, controls, and/or mechanisms.   DoD has determined the training is not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-16 | SA-16 | CCI-003291 | High | High | High | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service provide training defined in SA-16, CCI 3292 on the correct use and operation of the implemented security functions, controls, and/or mechanisms. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-17 | SA-17 | CCI-003293 | High | High | High | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service produce a design specification and security architecture. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-17 (1) | SA-17 (1) (a) | CCI-003298 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service produce, as an integral part of the development process, a formal policy model describing the elements of organizational security policy defined in SA-17 (1), CCI 3299 to be enforced. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (1) | SA-17 (1) (a) | CCI-003299 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented elements to ensure the organization being inspected/assessed defines the elements of organization security policy to be described in the formal policy model for enforcement on the information system, system component, or information system service.   DoD has determined the elements are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (1) | SA-17 (1) (b) | CCI-003300 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational security policy when implemented. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (2) | SA-17 (2) (a) | CCI-003301 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service define security-relevant software. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (2) | SA-17 (2) (a) | CCI-003303 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service define security-relevant software. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (2) | SA-17 (2) (a) | CCI-003304 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service define security-relevant firmware. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (2) | SA-17 (2) (a) | CCI-003305 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service provide a rationale that the definition for security-relevant hardware is complete. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (2) | SA-17 (2) (b) | CCI-003306 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service provide a rationale that the definition for security-relevant software is complete. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (2) | SA-17 (2) (b) | CCI-003307 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service provide a rationale that the definition for security-relevant firmware is complete. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (3) | SA-17 (3) (a) | CCI-003308 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant hardware in terms of exceptions, error messages, and effects. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (3) | SA-17 (3) (a) | CCI-003309 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant software in terms of exceptions, error messages, and effects. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (3) | SA-17 (3) (a) | CCI-003310 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant firmware in terms of exceptions, error messages, and effects. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (3) | SA-17 (3) (b) | CCI-003311 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service show via proof to the extent feasible with additional informal demonstration as necessary, that the formal top-level specification is consistent with the formal policy model. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (3) | SA-17 (3) (c) | CCI-003312 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (3) | SA-17 (3) (c) | CCI-003313 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant software. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (3) | SA-17 (3) (c) | CCI-003314 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant firmware. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (3) | SA-17 (3) (d) | CCI-003315 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service show that the formal top-level specification is an accurate description of the implemented security-relevant hardware. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (3) | SA-17 (3) (d) | CCI-003316 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service show that the formal top-level specification is an accurate description of the implemented security-relevant software. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (3) | SA-17 (3) (d) | CCI-003317 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service show that the formal top-level specification is an accurate description of the implemented security-relevant firmware. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (3) | SA-17 (3) (e) | CCI-003318 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service describe the security-relevant firmware mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant hardware. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (3) | SA-17 (3) (e) | CCI-003319 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service describe the security-relevant software mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant software. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (3) | SA-17 (3) (e) | CCI-003320 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service describe the security-relevant firmware mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant firmware. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (4) | SA-17 (4) (a) | CCI-003321 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant hardware in terms of exceptions, error messages, and effects. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (4) | SA-17 (4) (a) | CCI-003322 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant firmware in terms of exceptions, error messages, and effects. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (4) | SA-17 (4) (a) | CCI-003323 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant firmware in terms of exceptions, error messages, and effects. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (4) | SA-17 (4) (b) | CCI-003324 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service show via informal demonstration or convincing argument with formal methods as feasible that the descriptive top-level specification is consistent with the formal policy model. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (4) | SA-17 (4) (c) | CCI-003325 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (4) | SA-17 (4) (c) | CCI-003326 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant software. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (4) | SA-17 (4) (c) | CCI-003327 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant firmware. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (4) | SA-17 (4) (d) | CCI-003328 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant hardware. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (4) | SA-17 (4) (d) | CCI-003329 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant software. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (4) | SA-17 (4) (d) | CCI-003330 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant firmware. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (4) | SA-17 (4) (e) | CCI-003331 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service describe the security-relevant hardware mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant hardware. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (4) | SA-17 (4) (e) | CCI-003332 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service describe the security-relevant software mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant software. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (4) | SA-17 (4) (e) | CCI-003333 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service describe the security-relevant firmware mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant firmware. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (5) | SA-17 (5) (a) | CCI-003334 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service design and structure the security-relevant hardware to use a complete, conceptually simple protection mechanism with precisely defined semantics. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (5) | SA-17 (5) (a) | CCI-003335 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service design and structure the security-relevant software to use a complete, conceptually simple protection mechanism with precisely defined semantics. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (5) | SA-17 (5) (a) | CCI-003336 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service design and structure the security-relevant firmware to use a complete, conceptually simple protection mechanism with precisely defined semantics. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (5) | SA-17 (5) (b) | CCI-003337 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service internally structure the security-relevant hardware with specific regard for the complete, conceptually simple protection mechanism with precisely defined semantics. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (5) | SA-17 (5) (b) | CCI-003338 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service internally structure the security-relevant software with specific regard for the complete, conceptually simple protection mechanism with precisely defined semantics. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (5) | SA-17 (5) (b) | CCI-003339 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service internally structure the security-relevant firmware with specific regard for the complete, conceptually simple protection mechanism with precisely defined semantics. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (6) | SA-17 (6) | CCI-003340 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service structure security-relevant hardware to facilitate testing. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (6) | SA-17 (6) | CCI-003341 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service structure security-relevant software to facilitate testing. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (6) | SA-17 (6) | CCI-003342 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service structure security-relevant firmware to facilitate testing. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (7) | SA-17 (7) | CCI-003343 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service structure security-relevant hardware to facilitate controlling access with least privilege. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (7) | SA-17 (7) | CCI-003344 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service structure security-relevant software to facilitate controlling access with least privilege. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 (7) | SA-17 (7) | CCI-003345 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service structure security-relevant firmware to facilitate controlling access with least privilege. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-17 | SA-17 (a) | CCI-003294 | High | High | High | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer produce a design specification and security architecture that is consistent with and supportive of the organization's security architecture which is established within and is interrogated part of the organization's enterprise architecture. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-17 | SA-17 (b) | CCI-003295 | High | High | High | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer produce a design specification and security architecture that accurately and completely describes the required security functionality. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-17 | SA-17 (b) | CCI-003296 | High | High | High | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer produce a design specification and security architecture that accurately and completely describes the allocation of security controls among physical and logical components. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-17 | SA-17 (c) | CCI-003297 | High | High | High | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer produce a design specification and security architecture that expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-18 | SA-18 | CCI-003346 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented tamper protection program to ensure the organization being inspected/assessed implements a tamper protection program for the information system, system component, or information system service. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-18 (1) | SA-18 (1) | CCI-003347 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed employs anti-tamper technologies and techniques during multiple phases in the system development life cycle including design. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-18 (1) | SA-18 (1) | CCI-003348 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed employs anti-tamper technologies and techniques during multiple phases in the system development life cycle including development. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-18 (1) | SA-18 (1) | CCI-003349 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed employs anti-tamper technologies and techniques during multiple phases in the system development life cycle including integration. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-18 (1) | SA-18 (1) | CCI-003350 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed employs anti-tamper technologies and techniques during multiple phases in the system development life cycle including operations. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-18 (1) | SA-18 (1) | CCI-003351 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed employs anti-tamper technologies and techniques during multiple phases in the system development life cycle including maintenance. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-18 (2) | SA-18 (2) | CCI-003352 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of inspections to ensure the organization being inspected/assessed inspects information systems, system components, or devices defined in SA-18 (2), CCI 3353 at random, at a frequency defined in SA-18 (2), CCI 3354, and/or upon indications of need for inspection defined in SA-18 (2), CCI 3355 to detect tampering. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-18 (2) | SA-18 (2) | CCI-003353 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information systems, system components, or devices to ensure the organization being inspected/assessed defines the information systems, system components, or devices to inspect at random, at organization-defined frequency, and/or upon organization-defined indications of need for inspection to detect tampering.   DoD has determined the information systems, system components, or devices are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-18 (2) | SA-18 (2) | CCI-003354 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented frequency to ensure the organization being inspected/assessed defines the frequency to inspect organization-defined information systems, system, components, or devices to detect tampering.   DoD has determined the frequency is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-18 (2) | SA-18 (2) | CCI-003355 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented indications to ensure the organization being inspected/assessed defines indications of need for inspection to detect tampering during inspections of organization-defined information systems, system components, or devices.   DoD has determined the indications are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-19 (1) | SA-19 (1) | CCI-003367 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process, the list of personnel responsible for detecting counterfeit information system components, as well as the record of training to ensure the organization being inspected/assessed trains personnel or roles defined in SA-19 (1), CCI 3368 to detect counterfeit information system components (including hardware, software, and firmware). | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-19 (1) | SA-19 (1) | CCI-003368 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines the personnel or roles to be trained to detect counterfeit information system components (including hardware, software, and firmware).     DoD has determined the personnel or roles are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-19 (2) | SA-19 (2) | CCI-003369 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed maintains configuration control l over information system components defined in SA-19 (2), CCI 3370 awaiting service/repair. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-19 (2) | SA-19 (2) | CCI-003370 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed defines the information system components awaiting service/repair in which configuration control must be maintained.   DoD has determined the information system components are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-19 (2) | SA-19 (2) | CCI-003371 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed maintains configuration control over serviced/repaired components awaiting return to service. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-19 (3) | SA-19 (3) | CCI-003391 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of disposal to ensure the organization being inspected/assessed disposes of information system components using techniques and methods defined IAW DoD Manual 5200.01.      DoD has defined the techniques and methods as defined IAW DoD Manual 5200.01. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-19 (3) | SA-19 (3) | CCI-003390 | blank | blank | blank | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the techniques and methods as defined IAW DoD Manual 5200.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-19 (4) | SA-19 (4) | CCI-003388 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented frequency to ensure the organization being inspected/assessed defines the frequency to scan for counterfeit information system components.   DoD has determined the frequency is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-19 (4) | SA-19 (4) | CCI-003389 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of scans to ensure the organization being inspected/assessed scans for counterfeit information system components in accordance with the frequency defined in SA-19 (4), CCI 3388. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-19 | SA-19 (a) | CCI-003356 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented anti-counterfeit policy to ensure the organization being inspected/assessed develops an anti-counterfeit policy that include the means to detect counterfeit components from entering the information system. | [Section 13](#_COMPONENT_AUTHENTICITY) |
| SA-19 | SA-19 (a) | CCI-003357 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented anti-counterfeit policy to ensure the organization being inspected/assessed develops an anti-counterfeit policy that include the means to prevent counterfeit components from entering the information system. | [Section 13](#_COMPONENT_AUTHENTICITY) |
| SA-19 | SA-19 (a) | CCI-003358 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented anti-counterfeit procedures to ensure the organization being inspected/assessed develops anti-counterfeit procedures that include the means to detect counterfeit components from entering the information system. | [Section 13](#_COMPONENT_AUTHENTICITY) |
| SA-19 | SA-19 (a) | CCI-003359 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented anti-counterfeit procedures to ensure the organization being inspected/assessed develops anti-counterfeit procedures that include the means to prevent counterfeit components from entering the information system. | [Section 13](#_COMPONENT_AUTHENTICITY) |
| SA-19 | SA-19 (a) | CCI-003360 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the policy defined in SA-19, CCIs 3356 and any artifacts applicable to counterfeit components to ensure the organization being inspected/assessed implements the policy defined in SA-19, CCIs 3356 that include the means to detect counterfeit components from entering the information system. | [Section 13](#_COMPONENT_AUTHENTICITY) |
| SA-19 | SA-19 (a) | CCI-003361 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the policy defined in SA-19, CCIs 3357 and any artifacts applicable to counterfeit components to ensure the organization being inspected/assessed implements the policy defined in SA-19, CCIs 3357 that include the means to detect counterfeit components from entering the information system. | [Section 13](#_COMPONENT_AUTHENTICITY) |
| SA-19 | SA-19 (a) | CCI-003362 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the procedures defined in SA-19, CCIs 3358 and any artifacts applicable to counterfeit components to ensure the organization being inspected/assessed implements the procedures defined in SA-19, CCIs 3358 that include the means to detect counterfeit components from entering the information system. | [Section 13](#_COMPONENT_AUTHENTICITY) |
| SA-19 | SA-19 (a) | CCI-003363 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the procedures defined in SA-19, CCIs 3359 and any artifacts applicable to counterfeit components to ensure the organization being inspected/assessed implements the procedures defined in SA-19, CCIs 3359 that include the means to prevent counterfeit components from entering the information system. | [Section 13](#_COMPONENT_AUTHENTICITY) |
| SA-19 | SA-19 (b) | CCI-003364 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reporting to ensure the organization being inspected/assessed reports counterfeit information system components to source of counterfeit component, at a minimum, USCYBERCOM. And/or at a minimum, the ISSO, ISSM, and PM. | [Section 13](#_COMPONENT_AUTHENTICITY) |
| SA-19 | SA-19 (b) | CCI-003365 |  | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the external reporting organizations as at a minimum, USCYBERCOM | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-19 | SA-19 (b) | CCI-003366 |  | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM, and PM. | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-2 | SA-2 (a) | CCI-003091 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented information security requirements to ensure the organization being inspected/assessed determines information security requirements for the information system or information system service in mission/business process planning. | [Section 3](#_ALLOCATION_OF_RESOURCES) |
| SA-2 | SA-2 (b) | CCI-000610 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the planning, programming, and budget documentation to ensure the organization being inspected/assessed has determined the resources required for cybersecurity requirements to protect the information system or information system service. | [Section 3](#_ALLOCATION_OF_RESOURCES) |
| SA-2 | SA-2 (b) | CCI-000611 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the planning, programming, and budget documentation to ensure the organization being inspected/assessed has documented the resources required for cybersecurity requirements to protect the information system or information system service. | [Section 3](#_ALLOCATION_OF_RESOURCES) |
| SA-2 | SA-2 (b) | CCI-000612 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the planning, programming, and budget documentation to ensure the organization being inspected/assessed has allocated the resources required for cybersecurity requirements to protect the information system or information system service. | [Section 3](#_ALLOCATION_OF_RESOURCES) |
| SA-2 | SA-2 (c) | CCI-000613 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the planning, programming, and budget documentation to ensure the organization being inspected/assessed has identified and established an individual line item for cybersecurity requirements to protect the information system. | [Section 3](#_ALLOCATION_OF_RESOURCES) |
| SA-2 | SA-2 (c) | CCI-000614 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the planning, programming, and budget documentation to ensure the organization being inspected/assessed has identified and established an individual line item for cybersecurity requirements to protect the information system. | [Section 3](#_ALLOCATION_OF_RESOURCES) |
| SA-20 | SA-20 | CCI-003386 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented critical information system components to ensure the organization being inspected/assessed defines the critical information system components to re-implement or custom develop.     DoD has determined the critical information system components are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-20 | SA-20 | CCI-003387 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines hardware and software lists to ensure that no commercial off-the-shelf components are used as critical information system components defined in SA-20, CCI 3386. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-21 | SA-21 | CCI-003384 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system, system component, or information system service to ensure the organization being inspected/assessed defines the information system, system component, or information system service which require the information system developer to have appropriate access authorizations and satisfy additional personnel screening criteria.    DoD has determined the information system, system component, or information system service is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-21 (1) | SA-21 (1) | CCI-003377 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented actions to ensure the organization being inspected/assessed defines the actions the developer of the information system, system component, or information system service must take to ensure the required screening criteria are satisfied.   DoD has determined the actions are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-21 (1) | SA-21 (1) | CCI-003378 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented actions to ensure the organization being inspected/assessed defines the actions the developer of the information system, system component, or information system service must take to ensure the required access authorizations are satisfied.   DoD has determined the actions are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-21 (1) | SA-21 (1) | CCI-003379 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of information system, system component, or information system service take actions defined in SA-21 (1), CCI 3377 to ensure the required screening criteria are satisfied. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-21 (1) | SA-21 (1) | CCI-003380 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of information system, system component, or information system service take actions defined in SA-21 (1), CCI 3378 to ensure the required access authorizations are satisfied. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-21 | SA-21 (a) | CCI-003383 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented official government duties to ensure the organization being inspected/assessed defines the official government duties to be assigned to the developer of organization-defined information system, system component, or information system service.   DoD has determined the official government duties are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-21 | SA-21 (a) | CCI-003385 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of information system, system component, or information system service defined in SA-21, CCI 3384 have appropriate access authorizations as determined by assigned official government duties defined in SA-21, CCI 3383. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-21 | SA-21 (b) | CCI-003382 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of information system, system component, or information system service defined in SA-21, CCI 3384 satisfy additional personnel screening criteria defined in SA-21, CCI 3381. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-21 | SA-21 (b) | CCI-003381 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented additional personnel screening criteria to ensure the organization being inspected/assessed defines additional personnel screening criteria that must be satisfied by the developer of organization-defined information system, system component, or information system service.   DoD has determined the additional personnel screening criteria is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-22 (1) | SA-22 (1) | CCI-003372 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented support to ensure the organization being inspected/assessed defines the support from external providers to be provided for unsupported information system components.   DoD has determined the support from external providers is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-22 (1) | SA-22 (1) | CCI-003373 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed provides in-house support and/or support from external providers defined in SA-22 (1), CCI 3372 for unsupported information system components. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-22 | SA-22 (a) | CCI-003376 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented process as well as the hardware and software lists to ensure the organization being inspected/assessed replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-22 | SA-22 (b) | CCI-003374 | High | High | High | The organization conducting the inspection/assessment obtains and examines the hardware and software lists as well as the documented approvals to ensure the organization being inspected/assessed documents approval for the continued use of unsupported system components required to satisfy mission/business needs. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-22 | SA-22 (b) | CCI-003375 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented justification as well as the hardware and software lists to ensure the organization being inspected/assessed provides justification for the continued use of unsupported system components required to satisfy mission/business needs. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-3 | SA-3 (a) | CCI-003092 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented system development life cycle to ensure the organization being inspected/assessed defines a system development life cycle that is used to manage the information system.    DoD has determined the system development life cycle is not appropriate to define at the Enterprise level. | [Section 4](#_SYSTEM_DEVELOPMENT_LIFE) |
| SA-3 | SA-3 (a) | CCI-000615 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process and artifacts of the system development life cycle process to ensure the organization being inspected/assessed manages the information system using the system development life cycle defined in SA-3, CCI 3092 that incorporates information security considerations IAW DoDI 8580.1. | [Section 4](#_SYSTEM_DEVELOPMENT_LIFE) |
| SA-3 | SA-3 (b) | CCI-000616 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the information system security roles and responsibilities to ensure the organization being inspected/assessed defines and documents information system security roles and responsibilities throughout the system development life cycle IAW DoDI 8580.1. | [Section 4](#_SYSTEM_DEVELOPMENT_LIFE) |
| SA-3 | SA-3 (c) | CCI-000618 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented individuals having information system security roles and responsibilities to ensure the organization being inspected/assessed identifies individuals having information system security roles and responsibilities. | [Section 4](#_SYSTEM_DEVELOPMENT_LIFE) |
| SA-3 | SA-3 (d) | CCI-003093 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed integrates the organizational information security risk management process into system development life cycle activities. | [Section 4](#_SYSTEM_DEVELOPMENT_LIFE) |
| SA-4 (1) | SA-4 (1) | CCI-000623 | High Moderate | High Moderate | High Moderate | DoDI 8510.01 system categorization meets the DoD requirement for providing a description of the functional properties of the security controls to be employed.    DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8510.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-4 (10) | SA-4 (10) | CCI-003116 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure DoD approved PKI tokens are implemented for identify verification. | [Section 5](#_ACQUISITION_PROCESS) |
| SA-4 (2) | SA-4 (2) | CCI-003101 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires the developer of the information system, system component, or information system service to provide design information for the security controls to be employed that includes security-relevant external system interfaces, high-level design, low-level design, source code and/or hardware schematics and/or design/information defined in SA-4 (2), CCI 3103 at the level of detail defined in SA-4 (2), CCI 3105. | [Section 5](#_ACQUISITION_PROCESS) |
| SA-4 (2) | SA-4 (2) | CCI-003102 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires the developer of the information system, system component, or information system service to provide implementation information for the security controls to be employed that includes security-relevant external system interfaces, high-level design, low-level design, source code and/or hardware schematics and/or implementation information defined in SA-4 (2), CCI 3104 at the level of detail defined in SA-4 (2), CCI 3106. | [Section 5](#_ACQUISITION_PROCESS) |
| SA-4 (2) | SA-4 (2) | CCI-003103 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the documented design information to ensure the organization being inspected/assessed defines the design information that the developer of the information system, system component, or information system service is required to provide for the security controls to be employed.   DoD has determined the design information is not appropriate to define at the Enterprise level. | [Section 5](#_ACQUISITION_PROCESS) |
| SA-4 (2) | SA-4 (2) | CCI-003104 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the documented implementation information to ensure the organization being inspected/assessed defines the implementation information that the developer of the information system, system component, or information system service is required to provide for the security controls to be employed.   DoD has determined the implementation information is not appropriate to define at the Enterprise level. | [Section 5](#_ACQUISITION_PROCESS) |
| SA-4 (2) | SA-4 (2) | CCI-003105 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the documented level of detail to ensure the organization being inspected/assessed defines the level of detail the design information of the security controls is required to be provided by the developer of the information system, system component, or information system services.   DoD has determined the level of detail is not appropriate to define at the Enterprise level. | [Section 5](#_ACQUISITION_PROCESS) |
| SA-4 (2) | SA-4 (2) | CCI-003106 | High Moderate | High Moderate | High Moderate | The organization conducting the inspection/assessment obtains and examines the documented level of detail to ensure the organization being inspected/assessed defines the level of detail the implementation information of the security controls is required to be provided by the developer of the information system, system component, or information system services.   DoD has determined the level of detail is not appropriate to define at the Enterprise level. | [Section 5](#_ACQUISITION_PROCESS) |
| SA-4 (3) | SA-4 (3) | CCI-003107 |  | High |  | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires the developer of the information system, system component, or information system service to demonstrate the use of a system development life cycle that includes the state-of-the-practice system/security engineering methods, software development methods, testing/evaluation/validation techniques, and quality control processes defined in SA-4 (3), CCI 3108. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-4 (3) | SA-4 (3) | CCI-003108 |  | High |  | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed defines the state-of-the-practice system/security engineering methods, software development methods, testing/evaluation/validation techniques, and quality control processes that the developer of the information system, system component, or information system service needs to include when demonstrating the use of a system development life cycle. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-4 (5) | SA-4 (5) (a) | CCI-003109 |  | High |  | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires he developer of the information system, system component, or information system service to deliver the system, component, or service with security configurations identified by the applicable requirements from DoDI 8510.01 and STIGs/SRGs.   DoD has defined the security configurations as security configurations identified by the applicable requirements from DoDI 8510.01 and STIGs/SRGs. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-4 (5) | SA-4 (5) (a) | CCI-003110 |  | High |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the security configurations as security configurations identified by the applicable requirements from DoDI 8510.01 and STIGs/SRGs. | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-4 (5) | SA-4 (5) (b) | CCI-003111 |  | High |  | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires the developer of the information system, system component, or information system service to use the applicable requirements from DoDI 8510.01 and STIGs/SRGs as the default for any subsequent system, component, or service reinstallation or upgrade.   DoD has defined the security configurations as security configurations identified by the applicable requirements from DoDI 8510.01 and STIGs/SRGs. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-4 (6) | SA-4 (6) (a) | CCI-000631 | blank | blank | blank | The organization conducting the inspection/assessment examines and verifies identified encryption technologies in use by the organization being inspected/assessed are NSA-approved. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-4 (6) | SA-4 (6) (b) | CCI-000633 | blank | blank | blank | The organization conducting the inspection/assessment examines and verifies identified encryption technologies in use by the organization being inspected/assessed are NSA-approved. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-4 (7) | SA-4 (7) (a) | CCI-000634 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the hardware and software lists to ensure the organization being inspected/assessed, when using commercially provided IA and IA-enabled IT products uses only products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists. | [Section 5](#_ACQUISITION_PROCESS) |
| SA-4 (7) | SA-4 (7) (b) | CCI-000635 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the hardware and software lists to ensure the organization being inspected/assessed, when using commercially provided IA or IA enabled IT products for which there is no NIAP-approved protection profile, relies on FIPS-validated cryptographic modules. | [Section 5](#_ACQUISITION_PROCESS) |
| SA-4 (8) | SA-4 (8) | CCI-003112 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service produce a plan for the continuous monitoring of security control effectiveness that contains the level of detail defined in SA-4 (8), CCI 3113. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-4 (8) | SA-4 (8) | CCI-003113 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented level of detail to ensure the organization being inspected/assessed defines the level of detail to be contained in the plan for the continuous monitoring of security control effectiveness that the developer of the information system, system component, or information system services is required to produce.   DoD has determined the level of detail is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| SA-4 (9) | SA-4 (9) | CCI-003114 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use. | [Section 5](#_ACQUISITION_PROCESS) |
| SA-4 | SA-4 (a) | CCI-003094 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed includes the security functional requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs including DoDI 8580.1. | [Section 5](#_ACQUISITION_PROCESS) |
| SA-4 | SA-4 (b) | CCI-003095 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed includes the security strength requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs including DoDI 8580.1. | [Section 5](#_ACQUISITION_PROCESS) |
| SA-4 | SA-4 (c) | CCI-003096 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed includes the security assurance requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs including DoDI 8580.1. | [Section 5](#_ACQUISITION_PROCESS) |
| SA-4 | SA-4 (d) | CCI-003097 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed includes the security-related documentation requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs. | [Section 5](#_ACQUISITION_PROCESS) |
| SA-4 | SA-4 (e) | CCI-003098 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed includes requirements for protecting security-related documentation, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs. | [Section 5](#_ACQUISITION_PROCESS) |
| SA-4 | SA-4 (f) | CCI-003099 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed includes a description of the information system development environment and environment in which the system is intended to operate, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs. | [Section 5](#_ACQUISITION_PROCESS) |
| SA-4 | SA-4 (g) | CCI-003100 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed includes acceptance criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs. | [Section 5](#_ACQUISITION_PROCESS) |
| SA-5 | SA-5 (a) (1) | CCI-003124 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide administrator documentation for the information system, system component or information system service that describe secure configuration of the system, component, or service. | [Section 6](#_INFORMATION_SYSTEM_DOCUMENTATION) |
| SA-5 | SA-5 (a) (1) | CCI-003125 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide administrator documentation for the information system, system component or information system service that describe secure installation of the system, component, or service. | [Section 6](#_INFORMATION_SYSTEM_DOCUMENTATION) |
| SA-5 | SA-5 (a) (1) | CCI-003126 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide administrator documentation for the information system, system component or information system service that describe secure operation of the system, component, or service. | [Section 6](#_INFORMATION_SYSTEM_DOCUMENTATION) |
| SA-5 | SA-5 (a) (2) | CCI-003127 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide administrator documentation for the information system, system component or information system service that describe effective use and maintenance of security functions/mechanisms. | [Section 6](#_INFORMATION_SYSTEM_DOCUMENTATION) |
| SA-5 | SA-5 (a) (3) | CCI-003128 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide administrator documentation for the information system, system component or information system service that describe known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions. | [Section 6](#_INFORMATION_SYSTEM_DOCUMENTATION) |
| SA-5 | SA-5 (b) (1) | CCI-003129 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide user documentation for the information system, system component or information system service that describes user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms. | [Section 6](#_INFORMATION_SYSTEM_DOCUMENTATION) |
| SA-5 | SA-5 (b) (2) | CCI-003130 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide user documentation for the information system, system component or information system service that describes methods for user interaction which enables individuals to use the system, component, or service in a more secure manner. | [Section 6](#_INFORMATION_SYSTEM_DOCUMENTATION) |
| SA-5 | SA-5 (b) (3) | CCI-003131 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide user documentation for the information system, system component or information system service that describes user responsibilities in maintaining the security of the system, component, or service. | [Section 6](#_INFORMATION_SYSTEM_DOCUMENTATION) |
| SA-5 | SA-5 (c) | CCI-003133 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting inspection/assessment obtains and examines the documented actions to ensure the organization being inspected/assessed defines action to be taken in response to attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service.  DoD has determined the actions are not appropriate to define at the Enterprise level. | [Section 6](#_INFORMATION_SYSTEM_DOCUMENTATION) |
| SA-5 | SA-5 (c) | CCI-000642 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented attempts to ensure the organization being inspected/assessed documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent. | [Section 6](#_INFORMATION_SYSTEM_DOCUMENTATION) |
| SA-5 | SA-5 (c) | CCI-003132 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the record of actions taken to ensure the organization being inspected/assessed takes actions defined in SA-5, CCI 3133 in response to attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service.  DoD has determined the actions are not appropriate to define at the Enterprise level. | [Section 6](#_INFORMATION_SYSTEM_DOCUMENTATION) |
| SA-5 | SA-5 (d) | CCI-003134 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented processes to ensure the organization being inspected/assessed stores and handles information system, system component, or information system service documentation as required, in accordance with the risk management strategy. | [Section 6](#_INFORMATION_SYSTEM_DOCUMENTATION) |
| SA-5 | SA-5 (e) | CCI-003135 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the information system, system component, or information system service documentation via the organization's information sharing capability to ensure the organization being inspected/assessed distributes information system, system component, or information system service documentation to at a minimum, the ISSO, ISSM, and SCA.   DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM, and SCA. | [Section 6](#_INFORMATION_SYSTEM_DOCUMENTATION) |
| SA-5 | SA-5 (e) | CCI-003136 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM, and SCA. | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-8 | SA-8 | CCI-000664 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the system requirements documents to ensure that the organization being inspected/assessed applies information system security engineering principles in the specification of the information system. | [Section 7](#_SECURITY_ENGINEERING_PRINCIPLES) |
| SA-8 | SA-8 | CCI-000665 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the design documents to ensure that the organization being inspected/assessed applies information system security engineering principles in the design of the information system. | [Section 7](#_SECURITY_ENGINEERING_PRINCIPLES) |
| SA-8 | SA-8 | CCI-000666 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the system development procedures (e.g. configuration management plans, code review procedures, and coding style guides) to ensure that the organization being inspected/assessed applies information system security engineering principles in the development of the information system. | [Section 7](#_SECURITY_ENGINEERING_PRINCIPLES) |
| SA-8 | SA-8 | CCI-000667 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the audit trail artifacts that were created during the implementation of SA-8, CCI 000666 to ensure that the organization being inspected/assessed applies information system security engineering principles in the implementation of the information system and that changes are made IAW the configuration management plan (CM-9, CCI 001790). | [Section 7](#_SECURITY_ENGINEERING_PRINCIPLES) |
| SA-8 | SA-8 | CCI-000668 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the audit trail artifacts that were created during the modification of SA-8, CCI 000666 to ensure that the organization being inspected/assessed applies information system security engineering principles in the modification of the information system and that changes are made IAW the configuration management plan (CM-9, CCI 001790). | [Section 7](#_SECURITY_ENGINEERING_PRINCIPLES) |
| SA-9 (1) | SA-9 (1) (a) | CCI-003140 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines a list of acquired or outsourced information security services and the record of risk assessment to ensure the organization being inspected/assessed conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services. | [Section 8](#_EXTERNAL_INFORMATION_SYSTEM) |
| SA-9 (1) | SA-9 (1) (b) | CCI-003141 |  | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines a list of acquired or outsourced information security services as well as the record of approvals to ensure the organization being inspected/assessed ensures that the acquisition or outsourcing of dedicated information security services is approved by the DoD Component CIO or their delegate(s).   DoD has defined the personnel or roles the DoD Component CIO or their delegate(s). | [Section 8](#_EXTERNAL_INFORMATION_SYSTEM) |
| SA-9 (1) | SA-9 (1) (b) | CCI-003142 |  | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles the DoD Component CIO or their delegate(s). | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-9 (2) | SA-9 (2) | CCI-003143 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that providers of all external information system services identify the functions, ports, protocols, and other services required for the use of such services.   DoD has defined the external information system services as all external information system services. | [Section 8](#_EXTERNAL_INFORMATION_SYSTEM) |
| SA-9 (2) | SA-9 (2) | CCI-003144 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the external information system services as all external information system services. | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-9 (3) | SA-9 (3) | CCI-003145 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines a list of trust relationships with external service providers to ensure those relationships are established based on security requirements, properties, factors, or conditions defining acceptable trust relationship defined in SA-9 (3), CCI 3148. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-9 (3) | SA-9 (3) | CCI-003146 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the list of trust relationship with external service providers to ensure it is documented. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-9 (3) | SA-9 (3) | CCI-003147 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines a list of trust relationships with external service providers to ensure those relationships are maintained based on security requirements, properties, factors, or conditions defining acceptable trust relationship defined in SA-9 (3), CCI 3148. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-9 (3) | SA-9 (3) | CCI-003148 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented security requirements, properties, factors, or conditions to ensure the organization being inspected/assessed defines security requirements, properties, factors, or conditions defining acceptable trust relationships with external service providers.   DoD has determined the security requirements, properties, factors, or conditions are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-9 (4) | SA-9 (4) | CCI-003149 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines a list of external service providers as well as records of safeguard review to ensure the organization being inspected/assessed employs the security safeguards defined in SA-9 (4), CCI 3150 to ensure that the interests of all external service providers from whom services are solicited are consistent with and reflect organizational interests.   DoD has defined the external service providers as all external service providers from whom services are solicited. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-9 (4) | SA-9 (4) | CCI-003150 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed  defines security safeguards to employ to ensure that the interests of organization-defined external service providers are consistent with and reflect organizational interests. DoD has determined the security safeguards are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-9 (4) | SA-9 (4) | CCI-003151 | blank | blank | blank | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the external service providers as all external service providers from whom services are solicited. | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-9 (5) | SA-9 (5) | CCI-003152 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines a list of locations of information processing, information/data, and/or information system services to ensure the organization being inspected/assessed restricts the location of information processing, information/data, and/or information system services to locations defined in SA-9 (5), CCI 3153 based on requirements or conditions defined in SA-9 (5), CCI 3154. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-9 (5) | SA-9 (5) | CCI-003153 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented locations to ensure the organization being inspected/assessed defines the locations to restrict information processing, information/data, and/or information system services based on organization-defined requirements or conditions.   DoD has determined the location is not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-9 (5) | SA-9 (5) | CCI-003154 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented requirements or conditions to ensure the organization being inspected/assessed defines the requirements or conditions on which to base restricting the location of information processing, information/data, and/or information system services to organization-defined locations.   DoD has determined the requirements or conditions are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| SA-9 | SA-9 (a) | CCI-000669 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that providers of external information system services comply with any organization-specific information security requirements. | [Section 8](#_EXTERNAL_INFORMATION_SYSTEM) |
| SA-9 | SA-9 (a) | CCI-000670 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that providers of external information system services employ security controls defined in CNSSI 1253.   DoD has defined the security controls as security controls defined by CNSSI 1253. | [Section 8](#_EXTERNAL_INFORMATION_SYSTEM) |
| SA-9 | SA-9 (a) | CCI-003137 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the security controls as security controls defined by CNSSI 1253. | Automatically compliant with this CCI because they are covered at the DoD level |
| SA-9 | SA-9 (b) | CCI-000671 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) to confirm the organization has clearly defined the government oversight to be conducted on external information system services and service providers. | [Section 8](#_EXTERNAL_INFORMATION_SYSTEM) |
| SA-9 | SA-9 (b) | CCI-000672 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) to confirm the organization has clearly established the government oversight to be conducted on external information system services and service providers. | [Section 8](#_EXTERNAL_INFORMATION_SYSTEM) |
| SA-9 | SA-9 (b) | CCI-000673 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) to confirm the organization has clearly defined the roles and responsibilities of all types of users of the external information system services. | [Section 8](#_EXTERNAL_INFORMATION_SYSTEM) |
| SA-9 | SA-9 (b) | CCI-000674 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) to confirm the organization has clearly established the roles and responsibilities of all types of users of the external information system services. | [Section 8](#_EXTERNAL_INFORMATION_SYSTEM) |
| SA-9 | SA-9 (c) | CCI-003138 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the records of monitoring to ensure the organization being inspected/assessed implements the processes, methods, and techniques defined in SA-9, CCI 3139 to monitor security control compliance by external service providers on an ongoing basis. | [Section 8](#_EXTERNAL_INFORMATION_SYSTEM) |
| SA-9 | SA-9 (c) | CCI-003139 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented processes, methods, and techniques to ensure the organization being inspected/assessed defines processes, methods, and techniques to employ to monitor security control compliance by external service providers on an ongoing basis. | [Section 8](#_EXTERNAL_INFORMATION_SYSTEM) |

# **ENCLOSURE 1 – SYSTEM DEVELOPMENT LIFECYCLE**

**1.0 OVERVIEW**

Information system security processes and activities provide valuable input into managing IT systems and their development, enabling risk identification, planning and mitigation. A risk management approach involves continually balancing the protection of agency information and assets with the cost of security controls and mitigation strategies throughout the complete information system development life cycle.

The System Development Life Cycle (SDLC) is the overall process of developing, implementing, and retiring information systems through a multistep process from initiation, analysis, design, implementation, and maintenance to disposal. There are many different SDLC models and methodologies, but each generally consists of a series of defined steps or phases. This guide incorporates security into the linear sequential model of SDLC, which includes five phases: initiation, development/acquisition, implementation/assessment, operations/maintenance, and disposal.

**2.0 ROLES AND RESPONSIBILITIES**

Many participants have a role in information system development. A list of key roles is provided below:

| Role | Responsibility |
| --- | --- |
| Chief Information Officer (CIO) | The CIO is responsible for the organization’s information system planning, budgeting, investment, performance, and acquisition. As such, the CIO provides advice and assistance to senior organization personnel in acquiring the most efficient and effective information system to fit the organization’s enterprise architecture. |
| Configuration Management (CM) Manager | The CM manager is responsible for managing the effects of changes or differences in configurations on an information system or network. Thus, the CM manager assists in streamlining change management processes and prevents changes that could detrimentally affect the security posture of a system before they happen. |
| Information System Security Officer | The Information System Security Officer is responsible for ensuring the security of an information system throughout its life cycle. |
| Program Manager / Official (Information Owner) | This person represents business and programmatic interests in the information system during the SDLC process. The program manager plays an essential role in security and is, ideally, intimately aware of functional system requirements. |
| Software Developer | The developer is responsible for programmatic coding regarding applications, software, and Internet/intranet sites, including “secure coding,” as well as coordinating and working with the Configuration Management (CM) manager to identify, resolve, and implement controls and other CM issues. |
| System Owner | The system owner is responsible for the procurement, development, integration, modification, operation, and maintenance of an information system. |

**3.0 INCORPORATING SECURITY INTO THE SDLC**

This section describes a number of phases that will help integrate information security into the SDLC. Security considerations are identified in each SDLC phase, thus advancing the business application and security requirements together to ensure a balanced approach during development. Each phase includes a minimum set of security tasks needed to effectively incorporate security in the system development process.

* Initiation - During the initiation phase, the need for a system is expressed and the purpose of the system is documented.
* Development/Acquisition - During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed.
* Implementation/Assessment - After system acceptance testing, the system is installed or fielded.
* Operation/Maintenance - During this phase, the system performs its work. The system is almost always modified by the addition of hardware and software and by numerous other events.
* Disposal - Activities conducted during this phase ensure the orderly termination of the system, safeguarding vital system information, and migrating data processed by the system to a new system, or preserving it in accordance with applicable records management regulations and policies.

**3.1 Initiation Phase**

During this first phase of the development life cycle, security considerations are key to diligent and early integration, thereby ensuring that threats, requirements, and potential constraints in functionality and integration are considered. Key security activities for this phase include:

* Initial delineation of business requirements in terms of confidentiality, integrity, and availability;
* Determination of information categorization and identification of known special handling requirements to transmit, store, or create information such as personally identifiable information; and
* Determination of any privacy requirements.

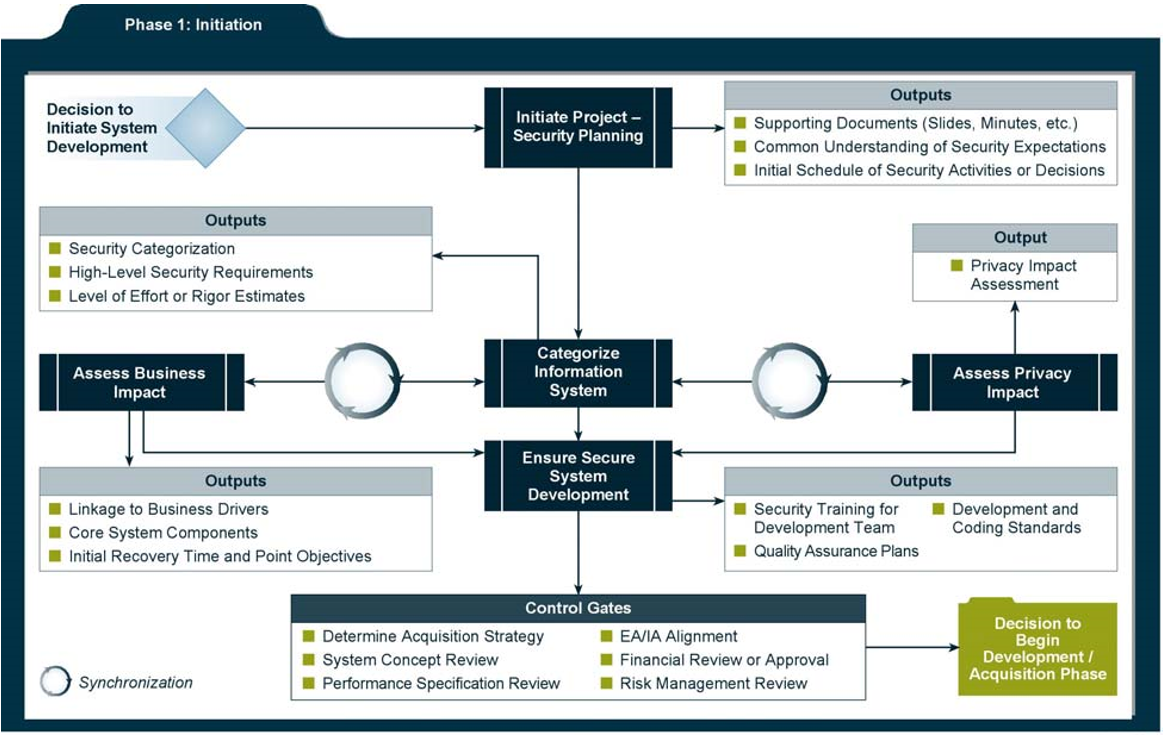


Figure 1 - Initiation

**3.1.1 Initiate Security Planning**

Security planning in the initiation phase should include preparations for the entire system life cycle, including the identification of key security milestones and deliverables, and tools and technologies.

{ACRONYM} has identified the following key security roles for the system development activities:

| Role | Name | Phone Number | Email |
| --- | --- | --- | --- |
| Information System Security Officer |  |  |  |
| Software Developer |  |  |  |
| System Owner |  |  |  |

{ACRONYM} security requirements have been defined in the RMF Control Selection Form and Security Assessment Plan.

**3.1.2 Categorize the Information System**

{ACRONYM} has completed RMF Step 1 – System Categorization.

**3.1.3 Assess Business Impact**

{ACRONYM} has completed the Business Impact Assessment (BIA), which is located in the Contingency Plan.

**3.1.4 Assess Privacy Impact**

{ACRONYM} has completed the Privacy Impact Assessment (PIA), which is located as an artifact in eMASS.

**3.1.5 Secure Information System Development Processes**

Primary responsibility for application security, during early phases, lies in the hands of the {ACRONYM} development team who has the most in-depth understanding of the detailed workings of the application and ability to identify security defects in functional behavior and business process logic. {ACRONYM} has implemented the following:

|  |  |
| --- | --- |
| Requirement | Response |
| Standards and Processes | Click or tap here to enter text. |
| Security Training for Development Team | Click or tap here to enter text. |
| Quality Management | Click or tap here to enter text. |
| Secure Environment | Click or tap here to enter text. |
| Secure Code Practices and Repositories | Click or tap here to enter text. |

**3.2 Development/Acquisition Phase**

This section addresses security considerations unique to the second SDLC phase. Key security activities for this phase include:

* Conduct the risk assessment and use the results to supplement the baseline security controls
* Analyze security requirements
* Perform functional and security testing
* Prepare initial documents for system certification and accreditation
* Design security architecture

Although this section presents the information security components in a sequential top-down manner, the order of completion is not necessarily fixed.

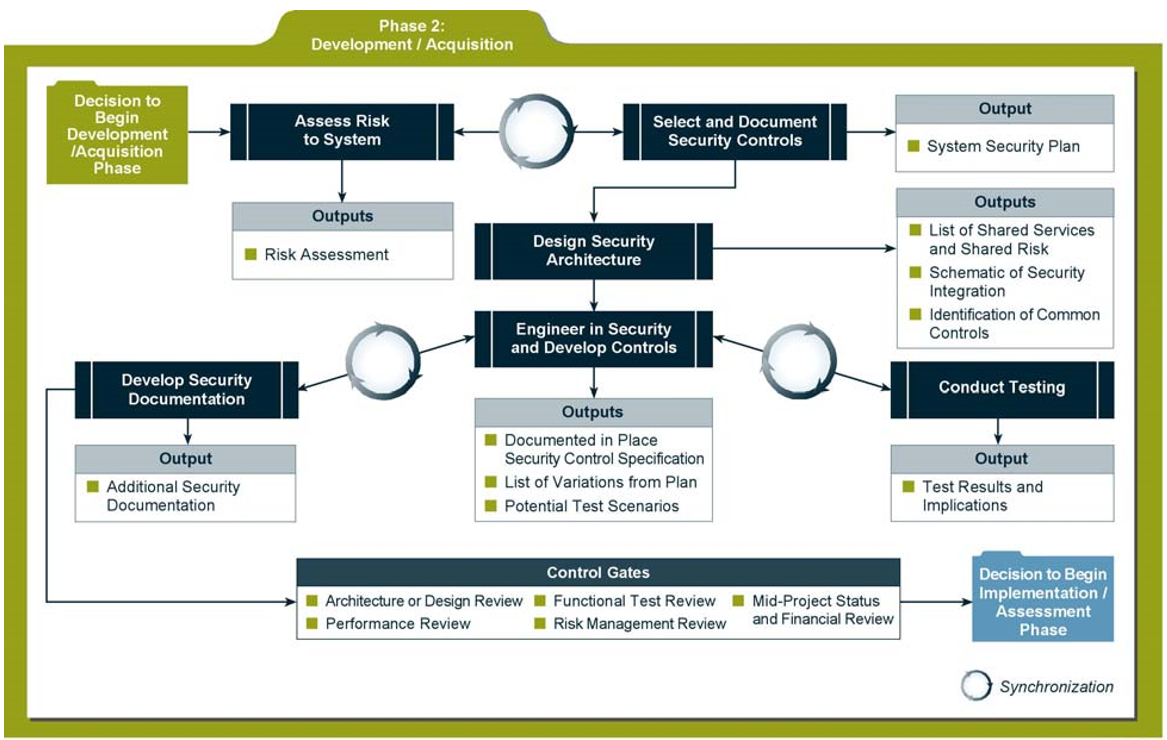


Figure 2 - Development/Acquisition

**3.2.1 Assess Risk to System**

{ACRONYM} has completed the Risk Assessment Report (RAR) in accordance with NIST SP 800-30, Risk Management Guide for Information Technology Systems.

**3.2.2 Select and Document Security Controls**

{ACRONYM} security controls have been identified in the RMF Control Selection Form.

**3.2.3 Design Security Architecture**

The {ACRONYM} security design considers services obtained externally, planned system interconnections, and the different orientations of system users. The following diagram depicts the {ACRONYM} security design:

**INSERT DIAGRAM**

**3.2.4 Engineer in Security and Develop Controls**

During this stage, security controls are implemented and become part of the system rather than applied at completion. {ACRONYM} has implemented security controls during RMF Step 3 – Implement Security Controls.

**3.2.5 Develop Security Documentation**

{ACRONYM} has developed the following documents, which are available as artifacts in eMASS:

* Configuration Management Plan
* Contingency Plan (including a Business Impact Assessment)
* Continuous Monitoring Plan
* Security Awareness, Training and Education Plan
* Incident Response Plan
* Privacy Impact Assessment (PIA)

**3.2.5 Conduct Testing (Developmental, Functional and Security)**

The objective of the test and evaluation process is to validate that the developed system complies with the functional and security requirements. {ACRONYM} initial security testing has been completed during RMF Step 3 – Implement Security Controls.

**3.3 Implementation / Assessment Phase**

During this phase, {ACRONYM} will be installed and evaluated in the organization’s operational environment. Key security activities for this phase include:

* Integrate the information system into its environment
* Plan and conduct system certification activities in synchronization with testing of security controls
* Complete system accreditation activities

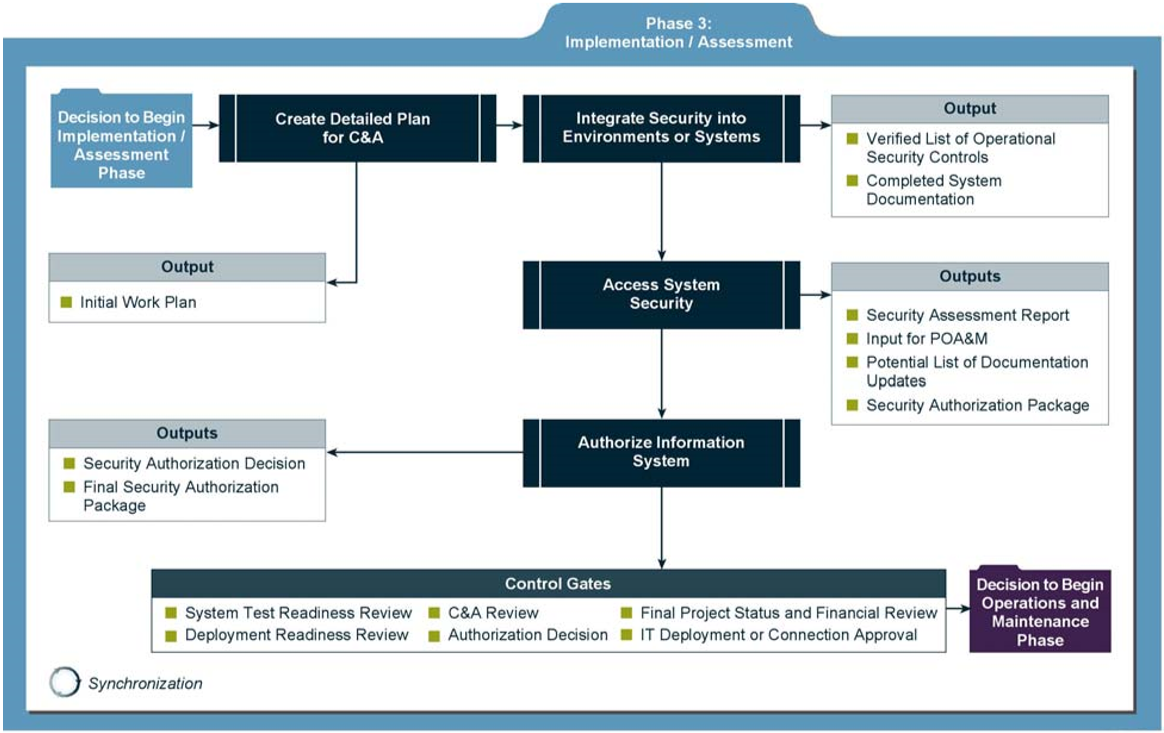


Figure 3 - Implementation/Assessment

**3.3.1 Create a Detailed Plan for C&A**

{ACRONYM} completed the Security Assessment Plan, which details the testing schedule during RMF Step 2 – Select Security Controls.

**3.3.2 Integrate Security**

System integration occurs at the operational site when the information system is to be deployed for operation. Integration and acceptance testing occur after information system delivery and installation. Security control settings are enabled in accordance with manufacturers’ instructions, available security implementation guidance, and documented security specification.

**3.3.3 Assess System Security**

Systems being developed or undergoing software, hardware, and/or communication modification(s) must be formally assessed prior to being granted formal accreditation. The objective of the security assessment process is to validate that the system complies with the functional and security requirements and will operate within an acceptable level of residual security risk.

{ACRONYM} completed the Security Assessment Report (SAR), which details the testing results during RMF Step 4 – Assess Security Controls. During this process, the {ACRONYM} Plan of Action and Milestones (POA&M) was created within eMASS.

**3.4 Operations and Maintenance Phase**

In this phase, {ACRONYM} is in place and operating, enhancements and/or modifications to {ACRONYM} are developed and tested, and hardware and/or software is added or replaced. {ACRONYM} is monitored for continued performance in accordance with security requirements and needed system modifications are incorporated. Key security activities for this phase include:

* Conduct an operational readiness review
* Manage the configuration of the system
* Institute processes and procedures for assured operations and continuous monitoring of the information system’s security controls
* Perform reauthorization as required

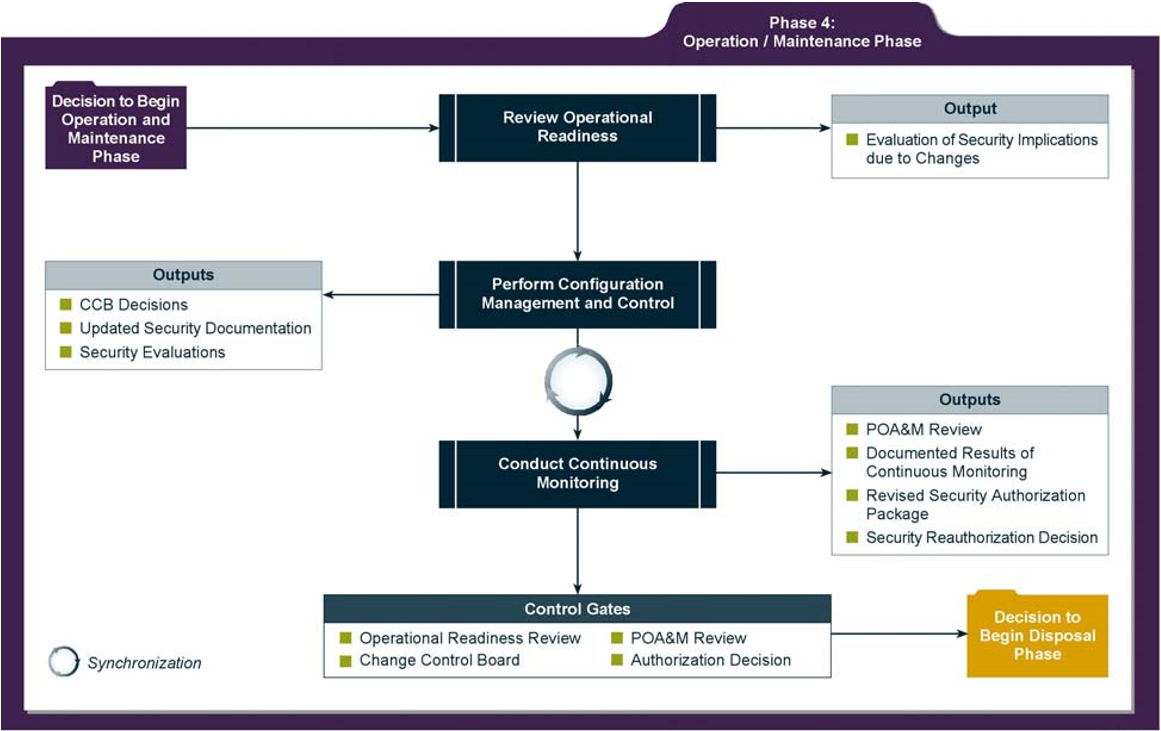


Figure 4 - Operations and Maintenance

**3.4.1 Review Operational Readiness**

The System Administrator and ISSO will confirm to System Owner that {ACRONYM} is operating normally and compliant with security requirements. Any change to security controls will be updated in the security documentation.

**3.4.2 Perform Configuration Management and Control**

Configuration management and control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for {ACRONYM} and subsequently for controlling and maintaining an accurate inventory of any changes to {ACRONYM}.

{ACRONYM} has developed a Configuration Management Plan, which is available as an artifact in eMASS.

**3.4.3 Conduct Continuous Monitoring**

The objective of continuous monitoring is to determine if the security controls in {ACRONYM} continue to be effective over time in light of the inevitable changes that occur in {ACRONYM} as well as the environment in which the {ACRONYM} operates.

{ACRONYM} has developed a Continuous Monitoring Strategy, which is available as an artifact in eMASS.

**3.5 Disposal Phase**

The disposal activities ensure the orderly termination of {ACRONYM} and preserve the vital information about {ACRONYM} so that some or all of the information may be reactivated in the future, if necessary. Particular emphasis will be given to proper preservation of the data processed by {ACRONYM} so that the data is effectively migrated to another system or archived in accordance with applicable records management regulations and policies for potential future access. Key security activities for this phase include:

* Build and Execute a Disposal/Transition Plan
* Archive of critical information
* Sanitization of media
* Disposal of hardware and software

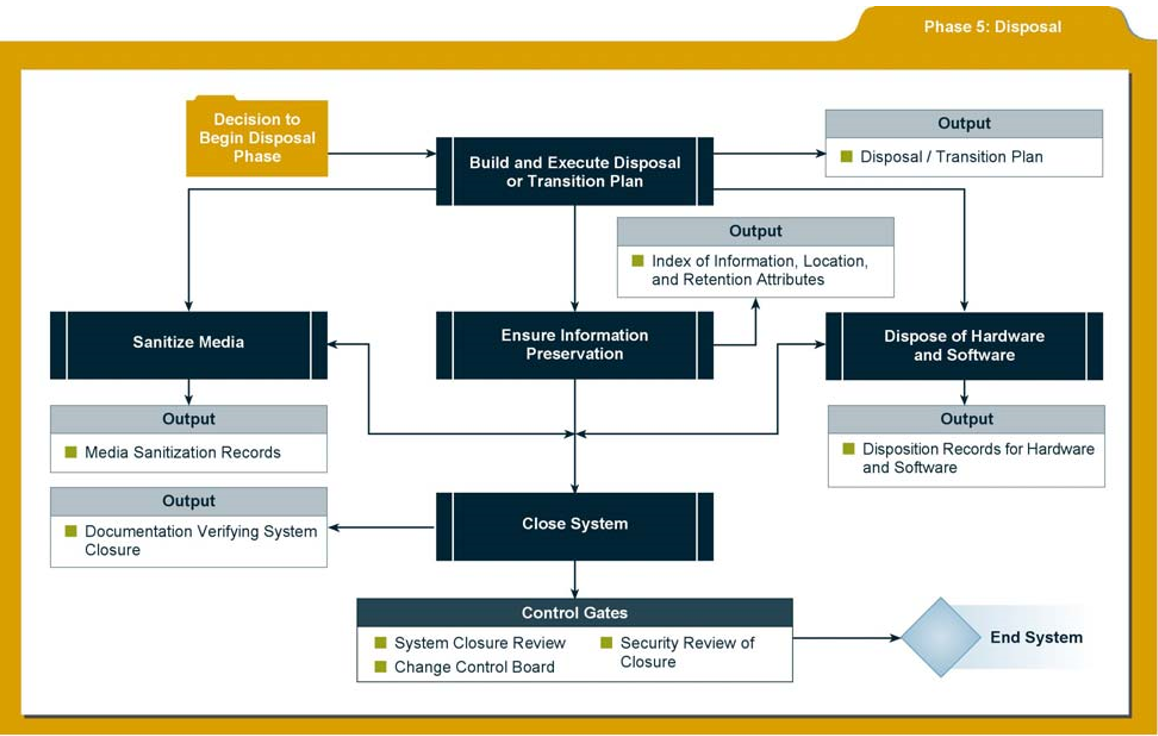


Figure 5 – Disposal

**3.5.1 Build and Execute a Disposal/Transition Plan**

This plan will account for the disposal / transition status for all critical components, services, and information. This plan will identify necessary steps, decisions, and milestones needed to properly close down, transition, or migrate {ACRONYM}.