|  |
| --- |
| **{COMMAND}** |
| **{SYSTEM NAME} {ACRONYM}** |
| **System Version: {VERSION}****eMASS# {EMASS#}****Confidentiality: {CONFIDENTIALITY}****Integrity: {INTEGRITY}****Availability: {AVAILABILITY}** |
| **Department of the {SERVICE}** |
| **{LOGO}** |
|  |
| **Security Planning****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)" 
2. DoD Instruction 8500.01, "Cybersecurity", as amended 
3. Committee on National Security Systems (CNSS) Instruction No. 1253, " Security Categorization and Control Selection for National Security Systems" 

**Table of Contents**

[**1.0** **OVERVIEW** 1](#_Toc453840740)

[**2.0** **SECURITY PLANNING POLICY AND PROCEDURES** 1](#_Toc453840741)

[**3.0** **SYSTEM SECURITY PLAN (SSP)** 2](#_Toc453840742)

[**4.0** **RULES OF BEHAVIOR** 3](#_Toc453840743)

[**5.0** **SECURITY CONCEPT OF OPERATIONS** 4](#_Toc453840744)

[**6.0** **INFORMATION SECURITY ARCHITECTURE** 4](#_Toc453840745)

[**7.0** **CENTRAL MANAGEMENT** 5](#_Toc453840746)

[**APPENDIX A – DETAILED COMPLIANCE MATRIX** 6](#_Toc453840747)

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

# **OVERVIEW**

The objective of security planning is to improve protection of information system resources. All federal systems have some level of sensitivity and require protection as part of good management practice. The protection of a system must be documented in a system security plan. The completion of system security plans is a requirement of the Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources,” Appendix III, “Security of Federal Automated Information Resources,” and” Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA).

The DoD has established an integrated enterprise-wide decision structure for cybersecurity risk management (the Risk Management Framework (RMF)) that includes cybersecurity requirements for DoD information technologies will be managed through the RMF consistent with the principals established in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37.

This plan ensures that {ACRONYM} follows the established guidelines and requirements for security planning. The formal System Security Plan is documented separately. The purpose of this document is to consolidate information and provide traceability to security control requirements.

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_–).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CNTL NO. | CONTROL NAME | PRIORITY | LOW | MOD | HIGH |
| [PL-1](#PL1) | Security Planning Policy and Procedures | P1 | PL-1 | PL-1 | PL-1 |
| [PL-2](#PL2) | System Security Plan | P1 | PL-2 | PL-2 (3) | PL-2 (3) |
| PL-3 | System Security Plan Update | Not Selected | Not Selected | Not Selected | Not Selected |
| [PL-4](#PL4) | Rules of Behavior | P2 | PL-4 | PL-4 (1) | PL-4 (1) |
| PL-5 | Privacy Impact Assessment | Not Selected | Not Selected | Not Selected | Not Selected |
| PL-6 | Security-Related Activity Planning | Not Selected | Not Selected | Not Selected | Not Selected |
| [PL-7](#PL7) | Security Concept of Operations | P0 | Not Selected | Not Selected | Not Selected |
| [PL-8](#PL8) | Information Security Architecture | P1 | Not Selected | PL-8 | PL-8 |
| [PL-9](#PL9) | Central Management | P0 | Not Selected | Not Selected | Not Selected |

Table 1 - SP-800-53v4 Compliance Matrix

# **2.0 SECURITY PLANNING POLICY AND PROCEDURES**

{ACRONYM} is automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01, “Risk Management Framework (RMF) for DoD Information Technology (IT)”. DoDI 8510.01 meets the requirements for a security planning policy. DoD has defined the roles as organizational personnel with planning responsibilities or information security responsibilities.

The RMF has the following characteristics:

* Promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes;
* Encourages the use of automation to provide senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions;
* Integrates information security into the enterprise architecture and system development life cycle;
* Provides emphasis on the selection, implementation, assessment, and monitoring of security controls, and the authorization of information systems;
* Links risk management processes at the information system level to risk management processes at the organization level through a risk executive (function); and
* Establishes responsibility and accountability for security controls deployed within organizational information systems and inherited by those systems (i.e., common controls).

# **3.0 SYSTEM SECURITY PLAN (SSP)**

The purpose of the SSP is to provide an overview of the security requirements of {ACRONYM} and describe the controls in place or planned for meeting those requirements. The SSP also delineates responsibilities and expected behavior of all individuals who access {ACRONYM}. The SSP should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for {ACRONYM}. The formal SSP for {ACRONYM} is documented separately. {ACRONYM} coordinates security-related activities affecting the information system with the following groups:

|  |  |
| --- | --- |
| Group | Role |
| Command Staff | Maintain cyber situational awareness for {ACRONYM} |
| Enterprise Architecture | Ensure compliance with {ACRONYM} architecture standards |
| Configuration Management | Maintain control of {ACRONYM} configuration |
| Incident Response | Focal point for {ACRONYM} incidents |
| External Approvers | Review and approve SSP |

Has an SSP been created for {ACRONYM}?

|  |
| --- |
|[ ]  No |
|[ ]  Yes |

If Yes, does the SSP contain a list of the individuals or groups with whom security-related activities are planned and coordinated?

|  |
| --- |
|[ ]  No |
|[ ]  Yes |

Within the {ACRONYM} SSP, is the following information defined:

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | Is the system architecture consistent with the organization's enterprise architecture? |[ ]  No |[ ]  Yes |
| 2. | Is the authorization boundary for the system defined? |[ ]  No |[ ]  Yes |
| 3. | Is the operational context of the information system in terms of missions and business processes defined? |[ ]  No |[ ]  Yes |
| 4. | Is the security categorization of the information system including supporting rationale defined? |[ ]  No |[ ]  Yes |
| 5. | Is the operational environment for the information system and relationships with or connections to other information systems defined? |[ ]  No |[ ]  Yes |
| 6. | Is an overview of the security requirements for the system defined? |[ ]  No |[ ]  Yes |
| 7. | Are any relevant overlays, if applicable, defined? |[ ]  No |[ ]  Yes |
| 8. | Are the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions defined? |[ ]  No |[ ]  Yes |
| 9. | Has security plan approval by the authorizing official or designated representative prior to plan implementation been obtained? |[ ]  No |[ ]  Yes |
| 10. | Have copies of the security plan been distributed, to at a minimum, the ISSO, ISSM and SCA |[ ]  No |[ ]  Yes |
| 11. | Has the security plan has been reviewed annually? |[ ]  No |[ ]  Yes |
| 12. | Is the security plan current? |[ ]  No |[ ]  Yes |

Is the security plan protected from unauthorized disclosure?

|  |
| --- |
|[ ]  No |
|[ ]  Yes |

If Yes, describe the controls in place.

|  |  |
| --- | --- |
|  | Click or tap here to enter text. |

Is the security plan protected from unauthorized modification?

|  |
| --- |
|[ ]  No |
|[ ]  Yes |

If Yes, describe the controls in place.

|  |  |
| --- | --- |
|  | Click or tap here to enter text. |

# **4.0 RULES OF BEHAVIOR**

{ACRONYM} utilizes DD Form 2875 (System Access Authorization Agreement (SAAR)) as the methodology to request and grant access to {ACRONYM}.

The SAAR contains the following information:

* Explicit restrictions on the use of social media/networking sites IAW DoDI 8550.01
* Explicit restrictions on posting organizational information on public websites IAW DoDI 8550.01

The SAAR has clearly defined and established rules describing {ACRONYM} user responsibilities and expected behavior with regard to information and information system usage.

SAARs are stored with the ISSM and {ACRONYM} documentation. The SAAR is shared with required parties via email. The SAARs are reviewed annually. In the event the SAAR is revised or updated, the end user must read and resign the form.

# **5.0 SECURITY CONCEPT OF OPERATIONS**

The Security Concept of Operations for {ACRONYM} is contained within its System Security Plan (SSP). The {ACRONYM} SSP is reviewed annually as confirmed by the Change Record contained within the SSP.

# **6.0 INFORMATION SECURITY ARCHITECTURE**

The information security architecture for {ACRONYM} is a unified security design that addresses the RMF requirements.

Has a system architecture been created for {ACRONYM}?

|  |
| --- |
|[ ]  No |
|[ ]  Yes |

If Yes, within the Security Architecture contained in the SSP is the following information defined:

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | Does the security architecture use a defense-in-depth approach that allocates security safeguards? |[ ]  No |[ ]  Yes |
| 2. | Does the security architecture use a defense-in-depth approach that allocates security safeguards to architectural layers? |[ ]  No |[ ]  Yes |
| 3. | Are security safeguards allocated to organization-defined locations defined? |[ ]  No |[ ]  Yes |
| 4. | Are security safeguards allocated to organization-defined architectural layers defined? |[ ]  No |[ ]  Yes |
| 5. | Does the SSP define the locations to which it allocates organization-defined security safeguards in the security architecture? |[ ]  No |[ ]  Yes |
| 6. | Does the SSP define the architectural layers to which it allocates organization-defined security safeguards in the security architecture? |[ ]  No |[ ]  Yes |
| 7. | Does the security architecture use a defense-in-depth approach that ensures that the allocated security safeguards operate in a coordinated and mutually reinforcing manner? |[ ]  No |[ ]  Yes |
| 8. | Are different suppliers used to procure security safeguards and allocated to locations and architectural layers? |[ ]  No |[ ]  Yes |
| 9. | Has an information security architecture for the information system been developed? |[ ]  No |[ ]  Yes |
| 10. | Is the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information defined? |[ ]  No |[ ]  Yes |
| 11. | Is how the information security architecture is integrated into and supports the enterprise architecture defined? |[ ]  No |[ ]  Yes |
| 12. | Does the information security architecture for the information system describe any information security assumptions about, and dependencies on, external services? |[ ]  No |[ ]  Yes |
| 13. | Is the information security architecture updated annually to reflect updates in the enterprise architecture? |[ ]  No |[ ]  Yes |
| 14. | Does the SSP include planned information security architecture changes? |[ ]  No |[ ]  Yes |
| 15. | Does the SSP include planned information security architecture changes in the security CONOPS? |[ ]  No |[ ]  Yes |
| 16. | Are planned information security architecture changes in organizational procurements/acquisitions documented? |[ ]  No |[ ]  Yes |

# **7.0 CENTRAL MANAGEMENT**

{ACRONYM} is automatically compliant with this requirement because they are covered at the DoD level. DoDI 8500.01, DoDI 8510.01, and CNSSI 1253 meet the DoD requirements for centrally managing security controls and related processes.

# **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 |
| --- | --- | --- | --- | --- | --- | --- | --- |
| PL-1 | PL-1 (a) | CCI-003047 | HighModerateLow | HighModerateLow | HighModerateLow | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as Organizational personnel with planning responsibilities or information security responsibilities. | Automatically compliant with this CCI because they are covered at the DoD level |
| PL-1 | PL-1 (a) | CCI-003048 | HighModerateLow | HighModerateLow | HighModerateLow | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as Organizational personnel with planning responsibilities or information security responsibilities. | Automatically compliant with this CCI because they are covered at the DoD level |
| PL-1 | PL-1 (a) (1) | CCI-000563 | HighModerateLow | HighModerateLow | HighModerateLow | DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| PL-1 | PL-1 (a) (1) | CCI-000564 | HighModerateLow | HighModerateLow | HighModerateLow | DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01.DoD has defined the roles as organizational personnel with planning responsibilities or information security responsibilities. | Automatically compliant with this CCI because they are covered at the DoD level |
| PL-1 | PL-1 (a) (2) | CCI-000566 | HighModerateLow | HighModerateLow | HighModerateLow | DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| PL-1 | PL-1 (b) (1) | CCI-001636 | HighModerateLow | HighModerateLow | HighModerateLow | 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 reviewed annually - updated as appropriate but at least within 10 years of date of issuance. | Automatically compliant with this CCI because they are covered at the DoD level |
| PL-1 | PL-1 (b) (1) | CCI-001637 | HighModerateLow | HighModerateLow | HighModerateLow | DoDI 8510.01 meets the requirements for a security planning policy. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01.DoD has defined the frequency as every 5 years. | Automatically compliant with this CCI because they are covered at the DoD level |
| PL-1 | PL-1 (b) (2) | CCI-001638 | HighModerateLow | HighModerateLow | HighModerateLow | 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 reviewed annually - updated as appropriate. | Automatically compliant with this CCI because they are covered at the DoD level |
| PL-1 | PL-1 (b) (2) | CCI-000568 | HighModerateLow | HighModerateLow | HighModerateLow | DoDI 8510.01 meets the requirements for a security planning policy. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01.DoD has defined the frequency as reviewed annually - updated as appropriate. | Automatically compliant with this CCI because they are covered at the DoD level |
| PL-1 | PL-1 (b) (2) | CCI-000567 | HighModerateLow | HighModerateLow | HighModerateLow | DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01.DoD has defined the roles as organizational personnel with planning responsibilities or information security responsibilities. | Automatically compliant with this CCI because they are covered at the DoD level |
| PL-2 (3) | PL-2 (3) | CCI-003065 | HighModerate | HighModerate | HighModerate | The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed plans and coordinates of security-related activities affecting the information system with individuals or groups defined in PL-2 (3), CCI 3067 before conducting such activities in order to reduce the impact on other organizational entities. | Section 3 |
| PL-2 (3) | PL-2 (3) | CCI-003067 | HighModerate | HighModerate | HighModerate | The organization conducting the inspection/assessment obtains and examines the documented individuals or groups to ensure the organization being inspected/assessed defines the individuals or groups with whom security-related activities are planned and coordinated. DoD has determined the individuals or groups are not appropriate to define at the Enterprise level. | Section 3 |
| PL-2 | PL-2 (a) | CCI-003049 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the documented security plan to ensure the organization being inspected/assessed develops a security plan for the information system. | eMASS SSP |
| PL-2 | PL-2 (a) (1) | CCI-003050 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the security plan and the enterprise architecture to ensure the organization's security plan for the information system is consistent with the organization's enterprise architecture. | [Section 3](#_3.0_SYSTEM_SECURITY)eMASS SSP |
| PL-2 | PL-2 (a) (2) | CCI-003051 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed explicitly defines within the security plan the authorization boundary for the system. | [Section 3](#_3.0_SYSTEM_SECURITY)eMASS SSP |
| PL-2 | PL-2 (a) (3) | CCI-003052 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed describes within the security plan the operational context of the information system in terms of missions and business processes. | [Section 3](#_3.0_SYSTEM_SECURITY)eMASS SSP |
| PL-2 | PL-2 (a) (4) | CCI-003053 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed defines within the security plan the security categorization of the information system including supporting rationale. | [Section 3](#_3.0_SYSTEM_SECURITY)eMASS SSP |
| PL-2 | PL-2 (a) (5) | CCI-003054 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed describes within the security plan the operational environment for the information system and relationships with or connections to other information systems. | [Section 3](#_3.0_SYSTEM_SECURITY)eMASS SSP |
| PL-2 | PL-2 (a) (6) | CCI-003055 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed their security plan for the information system provides an overview of the security requirements for the system | [Section 3](#_3.0_SYSTEM_SECURITY)eMASS SSP |
| PL-2 | PL-2 (a) (7) | CCI-003056 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed identifies within the security plan any relevant overlays, if applicable. | [Section 3](#_3.0_SYSTEM_SECURITY)eMASS SSP |
| PL-2 | PL-2 (a) (8) | CCI-003057 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed describes within the security plan the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions. | [Section 3](#_3.0_SYSTEM_SECURITY)eMASS SSP |
| PL-2 | PL-2 (a) (9) | CCI-000571 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the security plan approval to ensure the organization being inspected/assessed obtains security plan approval by the authorizing official or designated representative prior to plan implementation. | [Section 3](#_3.0_SYSTEM_SECURITY)eMASS SSP |
| PL-2 | PL-2 (b) | CCI-003061 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment examines the organization's information sharing portal to ensure at a minimum, the ISSO, ISSM and SCA have been provided changes to the security plan. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA. | [Section 3](#_3.0_SYSTEM_SECURITY)eMASS SSP |
| PL-2 | PL-2 (b) | CCI-003059 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the security plan via the organization's information sharing portal to ensure the organization being inspected/assessed distributes copies of the security plan to at a minimum, the ISSO, ISSM and SCA via the organization's information sharing portal. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA. | [Section 3](#_3.0_SYSTEM_SECURITY)eMASS SSP |
| PL-2 | PL-2 (b) | CCI-003060 | HighModerateLow | HighModerateLow | HighModerateLow | 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 |
| PL-2 | PL-2 (b) | CCI-003062 | HighModerateLow | HighModerateLow | HighModerateLow | 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 |
| PL-2 | PL-2 (c ) | CCI-000573 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the audit records of security plan reviews to verify the security plan has been reviewed annually. DoD has defined the frequency as annually. | [Section 3](#_3.0_SYSTEM_SECURITY)eMASS SSP |
| PL-2 | PL-2 (c ) | CCI-000572 | HighModerateLow | HighModerateLow | HighModerateLow | 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 |
| PL-2 | PL-2 (d) | CCI-000574 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the audit records of security plan updates to verify the security plan is current. The purpose of the reviews is to validate the organization is updating the Information System (IS) security plan to address changes to the IS, its environment of operation, or problems identified during plan implementation or security control assessments. | [Section 3](#_3.0_SYSTEM_SECURITY)eMASS SSP |
| PL-2 | PL-2 (e ) | CCI-003063 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects the security plan from unauthorized disclosure. | [Section 3](#_3.0_SYSTEM_SECURITY) |
| PL-2 | PL-2 (e ) | CCI-003064 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects the security plan from unauthorized modification. | [Section 3](#_3.0_SYSTEM_SECURITY) |
| PL-4 (1) | PL-4 (1) | CCI-000594 | HighModerate |   |   | The organization conducting the inspection/assessment obtains and examines the rules of behavior to ensure the organization being inspected/assessed includes explicit restrictions on the use of social media/networking sites IAW DoDI 8550.01. | [Section 4](#_4.0_RULES_OF) |
| PL-4 (1) | PL-4 (1) | CCI-000595 | HighModerate |   |   | The organization conducting the inspection/assessment obtains and examines the rules of behavior to ensure the organization being inspected/assessed includes explicit restrictions on posting organizational information on public websites IAW DoDI 8550.01. | [Section 4](#_4.0_RULES_OF) |
| PL-4 | PL-4 (a) | CCI-000592 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the organization's AUP to ensure the organization has clearly defined and established rules describing information system user responsibilities and expected behavior with regard to information and information system usage. | [Section 4](#_4.0_RULES_OF) |
| PL-4 | PL-4 (a) | CCI-001639 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines rules that describe information system user responsibilities via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated. | [Section 4](#_4.0_RULES_OF) |
| PL-4 | PL-4 (b) | CCI-000593 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains a list of individuals with active accounts and validates the existence of signed acknowledgements (paper or electronic signature) of the organizational AUP associated with a sampling of individuals selected from the list. | [Section 4](#_4.0_RULES_OF) |
| PL-4 | PL-4 (c ) | CCI-003068 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed reviews and updates the rules of behavior annually. DoD has defined the frequency as annually. | [Section 4](#_4.0_RULES_OF) |
| PL-4 | PL-4 (c ) | CCI-003069 | HighModerateLow | HighModerateLow | HighModerateLow | 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 |
| PL-4 | PL-4 (d) | CCI-003070 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated. | [Section 4](#_4.0_RULES_OF) |
| PL-7 | PL-7 (a) | CCI-003071 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the security CONOPS to ensure the organization being inspected/assessed develops a security CONOPS for the information system containing at a minimum, how the organization intends to operate the system from the perspective of information security. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| PL-7 | PL-7 (b) | CCI-000578 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed reviews and updates the security CONOPS annually. DoD has defined the frequency as annually. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| PL-7 | PL-7 (b) | CCI-000577 | 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 frequency as annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| PL-8 (1) | PL-8 (1) (a) | CCI-003081 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the security architecture to ensure the organization being inspected/assessed designs its security architecture using a defense-in-depth approach that allocates security safeguards defined in PL-8 (1), CCI 3083 to locations defined in PL-8 (1), CCI 3085. | [Section 6](#_6.0_INFORMATION_SECURITY)eMASS SSP |
| PL-8 (1) | PL-8 (1) (a) | CCI-003082 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the security architecture to ensure the organization being inspected/assessed designs its security architecture using a defense-in-depth approach that allocates security safeguards defined in PL-8 (1), CCI 3084 to architectural layers defined in PL-8 (1), CCI 3086. | [Section 6](#_6.0_INFORMATION_SECURITY)eMASS SSP |
| PL-8 (1) | PL-8 (1) (a) | CCI-003083 | HighModerateLow | HighModerateLow | HighModerateLow | 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 allocated to organization-defined locations. DoD has determined the security safeguards are not appropriate to define at the Enterprise level. | [Section 6](#_6.0_INFORMATION_SECURITY)eMASS SSP |
| PL-8 (1) | PL-8 (1) (a) | CCI-003084 | HighModerateLow | HighModerateLow | HighModerateLow | 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 allocated to organization-defined architectural layers. DoD has determined the security safeguards are not appropriate to define at the Enterprise level. | [Section 6](#_6.0_INFORMATION_SECURITY)eMASS SSP |
| PL-8 (1) | PL-8 (1) (a) | CCI-003085 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the documented locations to ensure the organization being inspected/assessed defines the locations to which it allocates organization-defined security safeguards in the security architecture. DoD has determined the locations are not appropriate to define at the Enterprise level. | [Section 6](#_6.0_INFORMATION_SECURITY)eMASS SSP |
| PL-8 (1) | PL-8 (1) (a) | CCI-003086 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the documented architectural layers to ensure the organization being inspected/assessed defines the architectural layers to which it allocates organization-defined security safeguards in the security architecture. DoD has determined the architectural layers are not appropriate to define at the Enterprise level. | [Section 6](#_6.0_INFORMATION_SECURITY)eMASS SSP |
| PL-8 (1) | PL-8 (1) (b) | CCI-003087 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines security architecture to ensure the organization being inspected/assessed designs its security architecture using a defense-in-depth approach that ensures that the allocated security safeguards operate in a coordinated and mutually reinforcing manner. | [Section 6](#_6.0_INFORMATION_SECURITY)eMASS SSP |
| PL-8 (2) | PL-8 (2) | CCI-003088 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines procurement records to ensure that different suppliers are used to procure security safeguards defined in PL-8 (1), CCIs 3083 and 3084 allocated to locations and architectural layers defined in PL-8 (1) CCIs 3085 and 3086. | [Section 6](#_6.0_INFORMATION_SECURITY)eMASS SSP |
| PL-8 | PL-8 (a) | CCI-003072 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the documented information security architecture to ensure the organization being inspected/assessed develops an information security architecture for the information system. | [Section 6](#_6.0_INFORMATION_SECURITY)eMASS SSP |
| PL-8 | PL-8 (a) (1) | CCI-003073 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the information security architecture to ensure the organization being inspected/assessed describes within the information security architecture for the information system, the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information. | [Section 6](#_6.0_INFORMATION_SECURITY)eMASS SSP |
| PL-8 | PL-8 (a) (2) | CCI-003074 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the information security architecture to ensure the organization being inspected/assessed describes within the information security architecture for the information system, how the information security architecture is integrated into and supports the enterprise architecture. | [Section 6](#_6.0_INFORMATION_SECURITY)eMASS SSP |
| PL-8 | PL-8 (a) (3) | CCI-003075 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the information security architecture to ensure the organization being inspected/assessed describes within the information security architecture for the information system, any information security assumptions about, and dependencies on, external services. | [Section 6](#_6.0_INFORMATION_SECURITY)eMASS SSP |
| PL-8 | PL-8 (b) | CCI-003076 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed reviews and updates the information security architecture annually to reflect updates in the enterprise architecture. DoD has defined the frequency as annually. | [Section 6](#_6.0_INFORMATION_SECURITY)eMASS SSP |
| PL-8 | PL-8 (b) | CCI-003077 | HighModerateLow | HighModerateLow | HighModerateLow | 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 |
| PL-8 | PL-8 (c ) | CCI-003078 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed includes planned information security architecture changes in the security plan. | [Section 6](#_6.0_INFORMATION_SECURITY)eMASS SSP |
| PL-8 | PL-8 (c ) | CCI-003079 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines security CONOPS to ensure the organization being inspected/assessed includes planned information security architecture changes in the security CONOPS. | [Section 6](#_6.0_INFORMATION_SECURITY)eMASS SSP |
| PL-8 | PL-8 (c ) | CCI-003080 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines a sampling of procurement materials to ensure the organization being inspected/assessed includes planned information security architecture changes in organizational procurements/acquisitions. | [Section 6](#_6.0_INFORMATION_SECURITY)eMASS SSP |
| PL-9 | PL-9 | CCI-003117 | blank | blank | blank | DoDI 8500.01, DoDI 8510.01, and CNSSI 1253 meet the DoD requirements for centrally managing security controls and related processes. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8500.01 and CNSSI 1253. | Automatically compliant with this CCI because they are covered at the DoD level |
| PL-9 | PL-9 | CCI-003118 | 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 security controls and related processes to be centrally managed as CNSSI 1253, DoDI 8510.01, and DoDI 8500.01. | Automatically compliant with this CCI because they are covered at the DoD level |