|  |
| --- |
| **{COMMAND}** |
| **{SYSTEM NAME} {ACRONYM}** |
| **System Version: {VERSION}**  **eMASS# {EMASS#}**  **Confidentiality: {CONFIDENTIALITY}**  **Integrity: {INTEGRITY}**  **Availability: {AVAILABILITY}** |
| **Department of the {SERVICE}** |
| **{LOGO}** |
|  |
| **Program Management 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 Instruction 8500.01, "Cybersecurity", as amended [PDF icon](http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf)
3. Committee on National Security Systems (CNSS) Instruction No. 1253, " Security Categorization and Control Selection for National Security Systems" [PDF icon](https://www.cnss.gov/CNSS/openDoc.cfm?fB+AFcOU6MhwNopIHS6VaQ==)
4. NIST Special Publication 800-55 Revision 1a, “Performance Measurement Guide for Information Security” [PDF icon](http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf)

**Table of Contents**

[**1.0** **OVERVIEW** 1](#_Toc461110533)

[**2.0** **INFORMATION SECURITY RESOURCES** 2](#_Toc461110534)

[**3.0** **PLAN OF ACTION AND MILESTONES PROCESS** 2](#_Toc461110535)

[**4.0** **INFORMATION SYSTEM INVENTORY** 3](#_Toc461110536)

[**5.0** **INFORMATION SECURITY MEASURES OF PERFORMANCE** 3](#_Toc461110537)

[**5.1** **Roles and Responsibilities** 3](#_Toc461110538)

[**5.2** **Types of Measures** 4](#_Toc461110539)

[**5.3** **Tracked Measures** 5](#_Toc461110540)

[**6.0** **MISSION/BUSINESS PROCESS DEFINITION** 5](#_Toc461110541)

[**7.0** **INSIDER THREAT PROGRAM** 5](#_Toc461110542)

[**8.0** **TESTING, TRAINING, AND MONITORING** 5](#_Toc461110543)

[**9.0** **CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS** 5](#_Toc461110544)

[**10.0** **THREAT AWARENESS PROGRAM** 5](#_Toc461110545)

[**APPENDIX A – DETAILED COMPLIANCE MATRIX** 6](#_Toc461110546)

[**ENCLOSURE 1 – INFORMATION SECURITY MEASURES** 23](#_Toc461110547)

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

# **OVERVIEW**

The objective of program management is to ensure that security considerations are planned for early and handled consistently in the project lifecycle.

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 program management. The formal System Security Plan is documented separately. The purpose of this document is to consolidate information and provide traceability to security control requirements.

The following subject areas are considered Tier-1 requirements and are covered at the DoD level:

* PM-1 Information Security Program Plan
* PM-2 Senior Information Security Officer
* PM-7 Enterprise Architecture
* PM-8 Critical Infrastructure Plan
* PM-9 Risk Management Strategy
* PM-10 Security Authorization Process
* PM-13 Information Security Workforce

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 |
| --- | --- | --- | --- | --- | --- |
| [PM-1](#PM1) | Information Security Program Plan | Not Selected | Not Selected | Not Selected | Not Selected |
| [PM-2](#PM2) | Senior Information Security Officer | Not Selected | Not Selected | Not Selected | Not Selected |
| [PM-3](#PM3) | Information Security Resources | Not Selected | PM-3 | PM-3 | PM-3 |
| [PM-4](#PM4) | Plan of Action and Milestones Process | Not Selected | PM-4 | PM-4 | PM-4 |
| [PM-5](#PM5) | Information System Inventory | Not Selected | PM-5 | PM-5 | PM-5 |
| [PM-6](#PM6) | Information Security Measures of Performance | Not Selected | PM-6 | PM-6 | PM-6 |
| [PM-7](#PM7) | Enterprise Architecture | Not Selected | Not Selected | Not Selected | Not Selected |
| [PM-8](#PM8) | Critical Infrastructure Plan | Not Selected | Not Selected | Not Selected | Not Selected |
| [PM-9](#PM9) | Risk Management Strategy | Not Selected | Not Selected | Not Selected | Not Selected |
| [PM-10](#PM10) | Security Authorization Process | Not Selected | Not Selected | Not Selected | Not Selected |
| [PM-11](#PM11) | Mission/Business Process Definition | Not Selected | PM-11 | PM-11 | PM-11 |
| [PM-12](#PM12) | Insider Threat Program | Not Selected | PM-12 | PM-12 | PM-12 |
| [PM-13](#PM13) | Information Security Workforce | Not Selected | Not Selected | Not Selected | Not Selected |
| [PM-14](#PM14) | Testing, Training, and Monitoring | Not Selected | PM-14 | PM-14 | PM-14 |
| [PM-15](#PM15) | Contacts with Security Groups and Associations | Not Selected | PM-15 | PM-15 | PM-15 |
| [PM-16](#PM16) | Threat Awareness Program | Not Selected | PM-16 | PM-16 | PM-16 |

Table 1 - SP-800-53v4 Compliance Matrix

# **2.0 INFORMATION SECURITY RESOURCES**

Increased competition for limited federal budgets and resources requires that system owners allocate available funding toward their highest-priority information security investments to ensure the appropriate degree of security for their needs.

Do planning and investment requests include the resources needed to implement the information security program for {ACRONYM}?

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

Is an OMB Exhibit 300 required for {ACRONYM}?

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

If Yes, has the OMB Exhibit 300 been approved?

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

Are information security resources available for expenditure as planned for {ACRONYM}?

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

# **PLAN OF ACTION AND MILESTONES PROCESS**

The Plan of Action and Milestones (POA&M) is a key document in the {ACRONYM} information security program and is subject to federal reporting requirements established by OMB. With the increasing emphasis on organization-wide risk management across all three tiers in the risk management hierarchy (i.e., organization, mission/business process, and information system), organizations view POA&Ms from an organizational perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization. POA&M updates are based on findings from security control assessments and continuous monitoring activities.

The following process is used by {ACRONYM} to ensure compliance with POA&M requirements:

1. The POA&M is required and will be maintained in eMASS
2. The POA&M will be updated based on assessment and continuous monitoring activities. At a minimum, the eMASS PO&AM will be updated quarterly
3. All ongoing findings in the POA&M will contain an adequate risk mitigation
4. PO&AM reporting will be executed in accordance with higher-level guidance
5. All {ACRONYM} stakeholders will review the POA&M annually to ensure consistency

# **INFORMATION SYSTEM INVENTORY**

The {ACRONYM} inventory is contained within the Hardware and Software lists. The {ACRONYM} is maintained by the Configuration Control Board (CCB). {ACRONYM} does not have OMB or annual FISMA reporting requirements for its inventory.

# **INFORMATION SECURITY MEASURES OF PERFORMANCE**

The requirement to measure information security performance is driven by regulatory, financial, and organizational reasons. A number of existing laws, rules, and regulations cite information performance measurement in general, and information security performance measurement in particular, as a requirement. These laws include the Clinger-Cohen Act, the Government Performance and Results Act (GPRA), the Government Paperwork Elimination Act (GPEA), and the Federal Information Security Management Act (FISMA).

Information security measures are used to facilitate decision making and improve performance and accountability through the collection, analysis, and reporting of relevant performance-related data. The purpose of measuring performance is to monitor the status of measured activities and facilitate improvement in those activities by applying corrective actions based on observed measurements.

## **5.1 Roles and Responsibilities**

This section outlines the key roles and responsibilities for developing and implementing information security measures.

Program Manager / Information System Owner

Program managers, as well as information system owners, are responsible for ensuring that proper security controls are in place to address the confidentiality, integrity, and availability of information and information systems. The program manager/information system owner has the following responsibilities related to information security measurement:

* Participating in information security measurement program development and implementation by providing feedback on the feasibility of data collection and identifying data sources and repositories;
* Educating staff on the development, collection, analysis, and reporting of information security measures and how it will affect information security policy, requirements, resource allocation, and budget decisions;
* Ensuring that measurement data is collected consistently and accurately and is provided to designated staff who are analyzing and reporting the data;
* Directing full participation and cooperation of staff, when required;
* Reviewing information security measures data regularly and using it for policy, resource allocation, and budget decisions; and
* Supporting implementation of corrective actions, identified through measuring information security performance.

Information System Security Officer (ISSO)

The ISSO has the following responsibilities related to information security measurement:

* Participating in information security measurement program development and implementation by providing feedback on the feasibility of data collection and identifying data sources and repositories; and
* Collecting data or providing measurement data to designated staff that are collecting, analyzing, and reporting the data.

## **5.2 Types of Measures**

The following types of measures will be maintained:

* Implementation Measures - used to demonstrate progress in implementing information security programs, specific security controls, and associated policies and procedures. Examples of implementation measures related to information security programs include the *percentage of information systems with approved system security plans* and the *percentage of information systems with password policies configured as required*.
* Effectiveness/efficiency Measures - used to monitor if program-level processes and system- level security controls are implemented correctly, operating as intended, and meeting the desired outcome. These measures concentrate on the evidence and results of assessments and may require multiple data points quantifying the degree to which information security controls are implemented and the resulting effect(s) on the organization’s information security posture. For example, the percentage of enterprise operating system vulnerabilities for which patches have been applied or that have been otherwise mitigated is both an implementation and effectiveness measure.
* Impact Measures - used to articulate the impact of information security on an organization’s mission. These measures are inherently organization-specific since each organization has a unique mission.

The following sources will contain information from which measures data will be generated:

* System Security Plans;
* Plan of Action and Milestones (POA&M) reports;
* Latest CCRI and IG findings;
* Tracking of information security-related activities, such as incident handling and reporting, testing, network management, audit logs, and network and information system billing;
* Risk assessments and penetration testing results;
* C&A documentation (e.g., security assessment reports);
* Continuous monitoring results;
* Contingency plans;
* Configuration management plans; and
* Training results and statistics.

## **5.3 Tracked Measures**

{ACRONYM} utilizes measures of performance to determine the effectiveness or efficiency of the {ACRONYM} information security program and the security controls employed in support of {ACRONYM}. [Enclosure 1](#_ENCLOSURE_1_–) contains the reportable measures used by {ACRONYM}.

# **MISSION/BUSINESS PROCESS DEFINITION**

Information protection needs determine the required security controls for {ACRONYM}. Inherent in defining the {ACRONYM} information protection needs is an understanding of the level of adverse impact that could result if a compromise of information occurs. The security categorization process is used to make such potential impact determinations. Mission/business process definitions and associated information protection requirements are documented by the organization in accordance with organizational policy and procedure. Step 1, “System Categorization” contains the information protection requirements and impacts for {ACRONYM}.

# **INSIDER THREAT PROGRAM**

The {ACRONYM} Insider threat program leverages the existing of incident handling teams already have in place.

# **TESTING, TRAINING, AND MONITORING**

The {ACRONYM} Continuous Monitoring Strategy implements the process for the required security testing, training, and monitoring activities.

# **CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS**

Ongoing contact with security groups and associations is of paramount importance in an environment of rapidly changing technologies and threats.

{ACRONYM} personnel collaborate with the {ACRONYM} Cyber Security team to:

1. facilitate ongoing security education and training
2. maintain currency with recommended security practices, techniques, and technologies
3. share current security-related information including threats, vulnerabilities, and incidents

# **THREAT AWARENESS PROGRAM**

The constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it is becoming more likely. One of the best techniques to address this concern is for {ACRONYM} to share threat information.

{ACRONYM} personnel collaborate with the {ACRONYM} Cyber Security team to share threat information.

# **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** | **References** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| PM-1 | PM-1 (a) (1) | CCI-000073 | Low Moderate High | Low Moderate High | Low Moderate High | DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls, they must be documented in their Security Plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-1 | PM-1 (a) (1) | CCI-002985 | Low Moderate High | Low Moderate High | Low Moderate High | DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls, they must be documented in their Security Plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-1 | PM-1 (a) (2) | CCI-001680 | Low Moderate High | Low Moderate High | Low Moderate High | DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls, they must be documented in their Security Plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-1 | PM-1 (a) (2) | CCI-002986 | Low Moderate High | Low Moderate High | Low Moderate High | DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls, they must be documented in their Security Plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-1 | PM-1 (a) (3) | CCI-002984 | Low Moderate High | Low Moderate High | Low Moderate High | DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls, they must be documented in their Security Plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-1 | PM-1 (a) (3) | CCI-002987 | Low Moderate High | Low Moderate High | Low Moderate High | DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls, they must be documented in their Security Plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-1 | PM-1 (a) (4) | CCI-000074 | Low Moderate High | Low Moderate High | Low Moderate High | DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls, they must be documented in their Security Plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-1 | PM-1 (a) (4) | CCI-002988 | Low Moderate High | Low Moderate High | Low Moderate High | DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls, they must be documented in their Security Plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-1 | PM-1 (b) | CCI-000076 | Low Moderate High | Low Moderate High | Low Moderate High | 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 |
| PM-1 | PM-1 (b) | CCI-000075 | Low Moderate High | Low Moderate High | Low Moderate High | DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls, they must be documented in their Security Plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-1 | PM-1 (c) | CCI-000077 | Low Moderate High | Low Moderate High | Low Moderate High | DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls, they must be documented in their Security Plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-1 | PM-1 (d) | CCI-002989 | Low Moderate High | Low Moderate High | Low Moderate High | DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls, they must be documented in their Security Plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-1 | PM-1 (d) | CCI-002990 | Low Moderate High | Low Moderate High | Low Moderate High | DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls, they must be documented in their Security Plan. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-10 | PM-10 (a) | CCI-000229 | Low Moderate High | Low Moderate High | Low Moderate High | DoDI 8510.01 meets the DoD requirement to manage the security authorization process.   DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-10 | PM-10 (a) | CCI-000230 | Low Moderate High | Low Moderate High | Low Moderate High | DoDI 8510.01 meets the DoD requirement to manage the security authorization process.   DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-10 | PM-10 (a) | CCI-000231 | Low Moderate High | Low Moderate High | Low Moderate High | DoDI 8510.01 meets the DoD requirement to manage the security authorization process.   DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-10 | PM-10 (b) | CCI-000233 | Low Moderate High | Low Moderate High | Low Moderate High | DoDI 8510.01 meets the DoD requirement to designate roles and responsibilities for the risk management process.   DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-10 | PM-10 (c) | CCI-000234 | Low Moderate High | Low Moderate High | Low Moderate High | DoDI 8510.01 meets the DoD requirement to fully integrate the security authorization process.   DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-11 | PM-11 (a) | CCI-000235 | Low Moderate High | Low Moderate High | Low Moderate High | DoDI 8510.01 meets the DoD requirement to define mission/business processes.   DoD components are automatically complaint with this control as they are covered at the DoD level, DoDI 8510.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-11 | PM-11 (b) | CCI-000236 | Low Moderate High | Low Moderate High | Low Moderate High | The organization conducting the inspection/assessment obtains and examines the security plan to ensure the security categorization has been documented IAW CNSSI 1253. | [Section 6](#_INSIDER_THREAT_PROGRAM) |
| PM-12 | PM-12 | CCI-002996 | Low Moderate High | Low Moderate High | Low Moderate High | The organization conducting the inspection/assessment obtains and examines the documented insider threat program to ensure the organization being inspected/assessed implements an insider threat program that includes a cross-discipline insider threat incident handling team. | [Section 7](#_INSIDER_THREAT_PROGRAM) |
| PM-13 | PM-13 | CCI-002997 | Low Moderate High | Low Moderate High | Low Moderate High | DoD 8570.01-M meets the DoD requirement to establish an information security workforce development and improvement program.   DoD components are automatically complaint with this control as they are covered at the DoD level, DoDI 8570.01-M. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-14 | PM-14 (a) (1) | CCI-002998 | Low Moderate High | Low Moderate High | Low Moderate High | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security testing activities associated with organizational information systems are developed. | [Section 8](#_TESTING,_TRAINING,_AND) |
| PM-14 | PM-14 (a) (1) | CCI-002999 | Low Moderate High | Low Moderate High | Low Moderate High | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security testing activities associated with organizational information systems are maintained. | [Section 8](#_TESTING,_TRAINING,_AND) |
| PM-14 | PM-14 (a) (1) | CCI-003000 | Low Moderate High | Low Moderate High | Low Moderate High | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security training activities associated with organizational information systems are developed. | [Section 8](#_TESTING,_TRAINING,_AND) |
| PM-14 | PM-14 (a) (1) | CCI-003001 | Low Moderate High | Low Moderate High | Low Moderate High | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security training activities associated with organizational information systems are maintained. | [Section 8](#_TESTING,_TRAINING,_AND) |
| PM-14 | PM-14 (a) (1) | CCI-003002 | Low Moderate High | Low Moderate High | Low Moderate High | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems are developed. | [Section 8](#_TESTING,_TRAINING,_AND) |
| PM-14 | PM-14 (a) (1) | CCI-003003 | Low Moderate High | Low Moderate High | Low Moderate High | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems are maintained. | [Section 8](#_TESTING,_TRAINING,_AND) |
| PM-14 | PM-14 (a) (2) | CCI-003004 | Low Moderate High | Low Moderate High | Low Moderate High | The organization conducting the inspection/assessment obtains and examines the documented process as well as records of execution to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security testing associated with organizational information systems continue to be executed in a timely manner. | [Section 8](#_TESTING,_TRAINING,_AND) |
| PM-14 | PM-14 (a) (2) | CCI-003005 | Low Moderate High | Low Moderate High | Low Moderate High | The organization conducting the inspection/assessment obtains and examines the documented process as well as the records of execution to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security training associated with organizational information systems continue to be executed in a timely manner. | [Section 8](#_TESTING,_TRAINING,_AND) |
| PM-14 | PM-14 (a) (2) | CCI-003006 | Low Moderate High | Low Moderate High | Low Moderate High | The organization conducting the inspection/assessment obtains and examines the documented process as well as the records of execution to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems continue to be executed in a timely manner. | [Section 8](#_TESTING,_TRAINING,_AND) |
| PM-14 | PM-14 (b) | CCI-003007 | Low Moderate High | Low Moderate High | Low Moderate High | 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 testing plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. | [Section 8](#_TESTING,_TRAINING,_AND) |
| PM-14 | PM-14 (b) | CCI-003008 | Low Moderate High | Low Moderate High | Low Moderate High | 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 training plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. | [Section 8](#_TESTING,_TRAINING,_AND) |
| PM-14 | PM-14 (b) | CCI-003009 | Low Moderate High | Low Moderate High | Low Moderate High | 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 monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. | [Section 8](#_TESTING,_TRAINING,_AND) |
| PM-15 | PM-15 (a) | CCI-003010 | Low Moderate High | Low Moderate High | Low Moderate High | The organization conducting the inspection/assessment obtains and examines artifacts showing contact to ensure the organization being inspected/assessed establishes and institutionalizes contact with selected groups and associations within the security community to facilitate ongoing security education and training for organizational personnel. | [Section 9](#_CONTACTS_WITH_SECURITY) |
| PM-15 | PM-15 (b) | CCI-003011 | Low Moderate High | Low Moderate High | Low Moderate High | The organization conducting the inspection/assessment obtains and examines artifacts showing contact to ensure the organization being inspected/assessed establishes and institutionalizes contact with selected groups and associations within the security community to maintain currency with recommended security practices, techniques, and technologies. | [Section 9](#_CONTACTS_WITH_SECURITY) |
| PM-15 | PM-15 (c ) | CCI-003012 | Low Moderate High | Low Moderate High | Low Moderate High | The organization conducting the inspection/assessment obtains and examines artifacts showing contact to ensure the organization being inspected/assessed establishes and institutionalizes contact with selected groups and associations within the security community to share current security-related information including threats, vulnerabilities, and incidents. | [Section 9](#_CONTACTS_WITH_SECURITY) |
| PM-16 | PM-16 | CCI-003013 | Low Moderate High | Low Moderate High | Low Moderate High | The organization conducting the inspection/assessment obtains and examines the documented threat awareness program to ensure the organization being inspected/assessed implements a threat awareness program that includes a cross-organization information-sharing capability. | [Section 10](#_THREAT_AWARENESS_PROGRAM) |
| PM-2 | PM-2 | CCI-000078 | Low Moderate High | Low Moderate High | Low Moderate High | DoD organizations are automatically compliant with this control as they are covered by the appointment of the DoD SISO. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-3 | PM-3 (a) | CCI-000080 | Low Moderate High | Low Moderate High | Low Moderate High | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement. | [Section 2](#_2.0_INFORMATION_SECURITY) |
| PM-3 | PM-3 (b) | CCI-000081 | Low Moderate High | Low Moderate High | Low Moderate High | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed employs a business case/Exhibit 300/Exhibit 53 to record the resources required. | [Section 2](#_2.0_INFORMATION_SECURITY) |
| PM-3 | PM-3 (c) | CCI-000141 | Low Moderate High | Low Moderate High | Low Moderate High | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed ensure that information security resources are available for expenditure as planned. | [Section 2](#_2.0_INFORMATION_SECURITY) |
| PM-4 | PM-4 (a) (1) | CCI-002991 | Low Moderate High | Low Moderate High | Low Moderate High | DoDI 8510.01 and the Knowledge Service meet the DoD requirements to develop a process for plans of action and milestones for the security program.   DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-4 | PM-4 (a) (1) | CCI-000142 | Low Moderate High | Low Moderate High | Low Moderate High | DoDI 8510.01 and the Knowledge Service meet the DoD requirements to maintain a process for plans of action and milestones for the security program.   DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-4 | PM-4 (a) (2) | CCI-000170 | Low Moderate High | Low Moderate High | Low Moderate High | DoDI 8510.01 and the Knowledge Service meet the DoD requirements to maintain a process to document the remedial information security actions that mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.   DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-4 | PM-4 (a) (3) | CCI-002992 | Low Moderate High | Low Moderate High | Low Moderate High | DoDI 8510.01 and the Knowledge Service meet the DoD requirements to implement a process ensuring that the plans of action and milestones for the security program are reported in accordance with OMB FISMA reporting requirements.   DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-4 | PM-4 (b) | CCI-002993 | Low Moderate High | Low Moderate High | Low Moderate High | 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 plans of action and milestones for the security program and associated organization information systems for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. | [Section 3](#_PLAN_OF_ACTION) |
| PM-5 | PM-5 | CCI-000207 | Low Moderate High | Low Moderate High | Low Moderate High | DITPR is the inventory for all DoD information systems.   The organization conducting the inspection/assessment obtains and examines the inventory of information systems via DITPR to ensure the organization being inspected/assessed registers their information systems in DITPR. | [Section 4](#_INFORMATION_SYSTEM_INVENTORY) |
| PM-6 | PM-6 | CCI-000209 | Low Moderate High | Low Moderate High | Low Moderate High | The Federal Information Systems Management Act (FISMA) meets the DoD requirements for information security performance measures of performance.   DoD organizations are automatically compliant with this control as they are covered at the DoD level by FISMA. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-6 | PM-6 | CCI-000210 | Low Moderate High | Low Moderate High | Low Moderate High | The Federal Information Systems Management Act (FISMA) meets the DoD requirements for information security performance measures of performance.   DoD organizations are automatically compliant with this control as they are covered at the DoD level by FISMA. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-6 | PM-6 | CCI-000211 | Low Moderate High | Low Moderate High | Low Moderate High | The organization conducting the inspection/assessment obtains and examines FISMA reporting documentation. | [Section 5](#_INFORMATION_SECURITY_MEASURES) |
| PM-7 | PM-7 | CCI-000212 | Low Moderate High | Low Moderate High | Low Moderate High | The GIG IA Architecture meets the DoD requirements for enterprise architecture.   DoD components are automatically compliant with this CCI as they covered at the DoD level. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-8 | PM-8 | CCI-000216 | Low Moderate High | Low Moderate High | Low Moderate High | DoDD 3020.40 meets the DoD requirement for the development of a critical infrastructure and key resource protection plan.   DoD components are automatically compliant with this control as they are covered by the DoD level, DoDD 3020.40. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-8 | PM-8 | CCI-001640 | Low Moderate High | Low Moderate High | Low Moderate High | DoDD 3020.40 meets the DoD requirement for the development of a critical infrastructure and key resource protection plan.   DoD components are automatically compliant with this control as they are covered by the DoD level, DoDD 3020.40. | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-9 | PM-9 (a) | CCI-000227 | Low Moderate High | Low Moderate High | Low Moderate High | DoD Risk Management Framework meets the requirement for a comprehensive organizational risk strategy.   DoD components are automatically compliant with this CCI because they are covered by DoD Risk Management Framework (DoDI 8510.01). | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-9 | PM-9 (b) | CCI-000228 | Low Moderate High | Low Moderate High | Low Moderate High | DoD Risk Management Framework meets the requirement for a comprehensive organizational risk strategy.   DoD components are automatically compliant with this CCI because they are covered by DoD Risk Management Framework (DoDI 8510.01). | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-9 | PM-9 (c ) | CCI-002994 | Low Moderate High | Low Moderate High | Low Moderate High | DoD Risk Management Framework meets the requirement for a comprehensive organizational risk strategy.   DoD components are automatically compliant with this CCI because they are covered by DoD Risk Management Framework (DoDI 8510.01). | Automatically compliant with this CCI because they are covered at the DoD level |
| PM-9 | PM-9 (c ) | CCI-002995 | Low Moderate High | Low Moderate High | Low Moderate High | 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 |

# **ENCLOSURE 1 – INFORMATION SECURITY MEASURES**

| ID | Goal | Measure | Measure Type | Formula | Target | Evidence | Frequency | Responsibility | Data Source |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| VULN-001 | Ensure all vulnerabilities are identified and mitigated | Percentage (%) of high vulnerabilities mitigated within organizationally defined time periods after discovery | Effectiveness/Efficiency | (# of high vulnerabilities identified and mitigated within targeted time frame during the time period /number of high vulnerabilities identified within the time period) \*100 | 100% | 1. Number of high vulnerabilities identified.  2. Number of high vulnerabilities mitigated. | Collection Frequency: Monthly Reporting Frequency: Monthly | ISSO | ACAS Scans VRAM |
| AT-001 | Ensure that organization personnel are adequately trained to carry out their assigned information security-related duties and responsibilities | Percentage (%) of information system security personnel that have received security training. | Implementation | (Number of information system security personnel that have completed security training within the past year/total number of information system security personnel) \*100 | 100% | 1. Number of personnel completing required training | Collection Frequency: Yearly Reporting Frequency: Yearly | ISO ISSO | Training and awareness tracking records |
| AUD-001 | Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate activity | Average frequency of audit records review and analysis for inappropriate activity | Effectiveness/Efficiency | Average frequency during reporting period | 100% | 1. Is logging set per STIG?  2. Are audit logs reviewed daily? | Collection Frequency: Daily Reporting Frequency: Monthly | ISSO | Audit log reports |
| CA-001 | Ensure all information systems have been certified and accredited as required. | Percentage (%) of systems that have completed certification and accreditation | Effectiveness/Efficiency | (Number of systems with complete C&A packages with Authorizing Official [AO] approval/(total number of new systems) \*100 | 100% | 1. Is the system accredited? | Collection Frequency: Monthly Reporting Frequency: Monthly | ISSO | ATO Letter |
| CM-001 | Establish and maintain baseline configurations throughout the system lifecycle. | Percentage (%) approved and implemented configuration changes identified | Implementation | (Number of approved and implemented configuration changes identified/total number of configuration changes identified through automated scans) \*100 | 100% | 1. Have all changes been documented? | Collection Frequency: Quarterly Reporting Frequency: Quarterly | ISO ISSO | Change Requests Scans |
| CP-001 | Establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations | Percentage (%) of information systems that have conducted annual contingency plan testing | Effectiveness/Efficiency | (Number of information systems that have conducted annual contingency plans testing/number of information systems in the system inventory) \*100 | 100% | 1. has the Contingency Plan been exercise? | Collection Frequency: Yearly Reporting Frequency: Yearly | ISO ISSO | CP Test Artifact Lessons Learned |
| IA-001 | All system users are identified and authenticated using PKI | Percentage (%) of users with CAC access | Effectiveness/Efficiency | (Number of users with CAC-based accounts/total number of users) \*100 | 100% | 1. Are all users authenticated with CAC? | Collection Frequency: Quarterly Reporting Frequency: Quarterly | ISO ISSO | Scans Interview |
| IR-001 | Track, document, and report incidents to appropriate organizational officials and/or authorities | Percentage (%) of incidents reported within required time frame per applicable incident category | Effectiveness/Efficiency | For each incident category (number of incidents reported on time/total number of reported incidents) \*100 | 100% | 1. Where all incidents reported? | Collection Frequency: As Needed Reporting Frequency: Yearly | ISO ISSO | After Actions Report Lessons Learned |
| PE-001 | Ensure that individuals occupying positions of responsibility within organizations are trustworthy and meet established security criteria for those positions. | Percentage (%) of individuals screened before being granted access to system. | Implementation | (Number of individuals screened/total number of individuals with access) \*100 | 100% | 1. How many individuals have been granted access to the system?  2. What is the number of individuals who have completed personnel screening? | Collection Frequency: As Needed Reporting Frequency: Yearly | ISO ISSO | SAAR Form |