|  |
| --- |
| **{COMMAND}** |
| **{SYSTEM NAME} {ACRONYM}** |
| **System Version: {VERSION}**  **eMASS# {EMASS#}**  **Confidentiality: {CONFIDENTIALITY}**  **Integrity: {INTEGRITY}**  **Availability: {AVAILABILITY}** |
| **Department of the {SERVICE}** |
| **{LOGO}** |
|  |
| **Security Awareness and Training 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. Department of Defense Directive Number 8140.01, "Cyberspace Workforce Management" [PDF icon](http://www.dtic.mil/whs/directives/corres/pdf/814001_2015_dodd.pdf)
2. NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program" [PDF icon](http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf)
3. NIST Special Publication 800-16, "Information Technology Security Training Requirements" [PDF icon](http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf)

**Table of Contents**

[1.0 OVERVIEW 1](#_Toc433183139)

[1.1 Applicability 1](#_Toc433183140)

[2.0 CYBER TRAINING 1](#_Toc433183141)

[2.1 General User Training 1](#_Toc433183142)

[2.2 Privileged User Training 2](#_Toc433183143)

[2.3 Role-Based Training 2](#_Toc433183144)

[3.0 PHYSICAL SECURITY TRAINING 5](#_Toc433183145)

[3.1 Applicable Security Controls 5](#_Toc433183146)

[3.2 Personnel and Roles 5](#_Toc433183147)

[4.0 MALICIOUS CODE TRAINING 6](#_Toc433183148)

[APPENDIX A – DETAILED COMPLIANCE MATRIX 7](#_Toc433183149)

[APPENDIX B – TRAINING RESOURCES 16](#_Toc433183150)

[Figure 1 - Cybersecurity Roles 3](#_Toc433183135)

[Table 1 - SP-800-53v4 Compliance Matrix 1](#_Toc433183129)

[Table 2 - Cybersecurity Roles 5](#_Toc433183130)

[Table 3 - Physical Security Control Training 5](#_Toc433183131)

[Table 4 - Physical Security Roles and Personnel 5](#_Toc433183132)

# **OVERVIEW**

Federal agencies and organizations cannot protect the confidentiality, integrity, and availability of information in today’s highly networked systems environment without ensuring that all people involved

in using and managing IT:

1. Understand their roles and responsibilities related to the organizational mission;
2. Understand the organization’s IT security policy, procedures, and practices; and
3. Have at least adequate knowledge of the various management, operational, and technical controls required and available to protect the IT resources for which they are responsible.

As cited in audit reports, periodicals, and conference presentations, it is generally understood by the IT security professional community that people are one of the weakest links in attempts to secure systems and networks. The “people factor” - not technology - is key to providing an adequate and appropriate level of security. If people are the key, but are also a weak link, more and better attention must be paid to this “asset.”

This plan does not claim to cover all possible means of security awareness and training. Higher level guidance is contained within the [Amplifying Guidance](#guidance) section of this document.

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 |
| [AT-1](#AT1) | Security Awareness and Training Policy and Procedures | P1 | AT-1 | AT-1 | AT-1 |
| [AT-2](#AT2) | Security Awareness Training | P1 | AT-2 | AT-2 (2) | AT-2 (2) |
| [AT-3](#AT3) | Role-Based Security Training | P1 | AT-3 | AT-3 | AT-3 |
| [AT-4](#AT4) | Security Training Records | P3 | AT-4 | AT-4 | AT-4 |
| AT-5 | Contacts With Security Groups And Associations | Not Selected | Not Selected | Not Selected | Not Selected |

Table 1 - SP-800-53v4 Compliance Matrix

## **1.1 Applicability**

This Security Awareness and Training Plan applies to {ACRONYM} and all of its users.

# **2.0 CYBER TRAINING**

## **2.1 General User Training**

IT has enabled the Department of Defense to transmit, communicate, collect, process, and store unprecedented amounts of information. Increasing dependence on information systems has focused attention on the need to ensure that these assets, and the information they process, are protected from actions that would jeopardize the DoD’s ability to effectively function. Responsibility for securing the Department’s information and systems lies with the DoD Components. The trained and aware user is the first and most vital line of defense.

Cyber training must be current, engaging, and relevant to the target audience to enhance its effectiveness. Its primary purpose is to educate and influence behavior. The focus must be on education and awareness of threats and vulnerabilities so users do not perform actions that lead to or enable exploitations of the DoD ISs. Authorized users must understand that they are a critical link in their organization’s overall IA success.

DISA’s [DoD Cyber Awareness Challenge](http://iatraining.disa.mil/eta/cyberchallenge/launchpage.htm) is the DoD baseline standard. It meets all DoD level requirements for end user awareness training. DISA will ensure it provides distributive awareness content to address evolving requirements promulgated by Congress, the OMB under the ISS LoB for Tier I, or the Office of the Secretary of Defense.

The DoD Components are required to use the DoD SSC as their Cyber Awareness Provider. The DoD Cyber Awareness Challenge will be used to meet the initial and annual training mandated by DoD regulations.

To ensure understanding of the critical importance of Cyber, all individuals with access to DoD IT systems are required to receive and complete initial Cyber awareness training before being granted access to the system(s) and annual Cyber awareness training to retain access.

All training is tracked at the {COMMAND} level.

## **2.2 Privileged User Training**

A privileged user is a user that is authorized (and, therefore, trusted) to have elevated rights to perform security-relevant functions that ordinary users are not authorized to perform. A number of high profile security incidents over the last year have proven, yet again, that privileged users -- administrators, contractors, and others with system-level access to IT infrastructure -- are a critical element of {ACRONYM}'s overall risk profile.

In addition to signing a Privileged Access Agreement for prior to account creation, individuals will take the [Privileged User Training](http://www.cdse.edu/catalog/elearning/DS-IA112.html) created by DISA.

All training is tracked at the {COMMAND} level.

## **2.3 Role-Based Training**

DISA has gathered inputs from the USCYBERCOM, [National Initiative for Cyberspace Education (NICE)](http://csrc.nist.gov/nice/framework/) and other partners to provide a catalog of training resources that are categorized by cyber work roles. The work roles used on this site were taken from [USCYBERCOM's Joint Cyberspace Training & Certification Standard (JCT&CS) v1.2, 7 Feb 2012](https://disa.deps.mil/ext/cop/iase/specialty_courses/Documents/20120207-B_Signed_JCTandCS.pdf). As the cyber work role process matures it will be integrated into future policy and doctrine to better recruit, train, promote and retain a superior cyberspace workforce.

While the cyber work roles may correlate to military specialties and civilian occupational classifications, they are not intended to be synonymous with discrete job positions. Each work role is listed with the associated tasks that an individual may be expected to perform the requisite skill sets needed to perform the work role tasks as related to conducting missions that span the three Lines of Operations (LOO): DoD DGO, DCO and OCO. As noted below in the diagram a cyberspace professional need to fill both a supporting and an operational warfighting role when operating in the Joint Information Environment (JIE).

The cyber role tasks and skill associated sets establish a proficiency baseline for a workforce capable of integrating, synchronizing, and executing sustained cyber space operations designed to achieve strategic, operational and tactical objectives. Future cyber training assessments will ensure development of necessary knowledge and skills required for increased competency in accomplishing DoD individual, staff and collective tasks. The following figure displays the USCYBERCOM cyberspace roles organized by Lines of Operations:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **Combat Element** | | | **Combat Support** | | | | | | | |
|  | |  | **Server Administrator** |  | **Technical Support Specialist** | **Systems Developer** | |  |  | | | |
| **I & W Analyst** | Administration | Logistic | Finance |
|  | CYBER Roles |
| **CND Analyst** |
| **Systems Security Analyst** | **Systems Test &**  **Eval Specialist** | **Software Engineer** | |
| **Intel Analyst** |
| **Network Operations Manager** |  |  |  | |  | |
| **Knowledge Manager** | **Systems Architect** | |  | **CND Forensic Analyst** |
| **CND Incident Responder** | **Data Administer** | **IA Compliance**  **Agent** | |  | **Endpoint Exploit Analyst** |
| **Cyber Security/ IS Professional** | **System Requirements Plan** | **Net Infrastructure Spec** | |  | **Cryptographic Cyber Planner** |
| **CND Manager** | **Technical Support Specialist** |  | **Systems Developer** |  | **BDA Analyst** |
| **Forensic Analyst** |
| **Interactive Operator** | **CND Auditor** |  |  |
| **Test & Eval Engineer** |
|  | |
|  | **Operational Target Dev Analyst** |
|  |  |  |
| **Production Operator** | **Assessment Analyst** |  | **Partner Ops Planner** |
| **Digital Network Exploit Analyst** |
| **Close Access**  **Network Operator** | **Network Warfare Cyber Planner** |  | **R&D Engineer** |
|  |
| **Target Digital**  **Network Analyst** |
|  | | | **Legal Advisor/ SJA** |  | **Cyber Policy & Strategy Planner** |
| **Target Analyst Reporter** |
|  | | | |
|  | |  | | |
|  | | | | | | | |

Figure 1 - Cybersecurity Roles

Lines of Operation Definitions:

1. Combat Element: Operational element of the Cyberspace organization
2. Combat Support: Operational assistance provided to combat elements. (Source: JP 4-0)
3. Defensive Cyberspace Operations: Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. Also called DCO. (Source: JP 3-12)
4. DoD Global Information Grid Operations: Employment of manual and automated methods to preserve and sustain the availability, confidentiality, integrity and non-repudiation of military information networks. The DoD GIG is the globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems.
5. Offensive Cyberspace Operations: Cyberspace operations intended to project power by the application of force in or through cyberspace. Also called OCO. (Source: JP 3-12)

The following table contains training resources based on assigned role:

| Cybersecurity Role | Proficiency Level | Specific Task or KSA |
| --- | --- | --- |
| CND Analyst: Uses data collected from a variety of CND tools (including intrusion detection system alerts, firewall and network traffic logs, and host system logs) to analyze events that occur within their environments for the purposes of mitigating threats. | [Entry](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?CND-ANLevel1.xml)  [Intermediate](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?CND-ANLevel2.xml)  [Advanced](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?CND-ANLevel3.xml) | [Tasks](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/qs_schedule.aspx?011)  [KSAs](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/ksa_schedule.aspx?011) |
| CND Auditor: Performs assessments of systems and networks within the NE or enclave and indentifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. | [Entry](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?CND-AULevel1.xml)  [Intermediate](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?CND-AULevel2.xml)  [Advanced](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?CND-AULevel3.xml) | [Tasks](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/qs_schedule.aspx?009)  [KSAs](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/ksa_schedule.aspx?009) |
| CND Incident Responder: Investigates and analyzes all response activities related to cyber incidents within the network environment or enclave. | [Entry](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?CND-IRLevel1.xml)  [Intermediate](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?CND-IRLevel2.xml)  [Advanced](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?CND-IRLevel3.xml) | [Tasks](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/qs_schedule.aspx?018)  [KSAs](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/ksa_schedule.aspx?018) |
| CND Infrastructure Support Specialist: Tests, implements, deploys, maintains, and administers the infrastructure hardware and software which are required to effectively manage the CND-SP network and resources. | [Entry](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?CNDISSLevel1.xml)  [Intermediate](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?CNDISSLevel2.xml)  [Advanced](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?CNDISSLevel3.xml) | [Tasks](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/qs_schedule.aspx?017)  [KSAs](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/ksa_schedule.aspx?017) |
| CND Manager: Oversees the CND-SP operations within their organization. | [Entry](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?CND-MGRLevel1.xml)  [Intermediate](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?CND-MGRLevel2.xml)  [Advanced](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?CND-MGRLevel3.xml) | [Tasks](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/qs_schedule.aspx?014)  [KSAs](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/ksa_schedule.aspx?014) |
| Cyber Security Analyst Information Security Professional: Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats. | [Entry](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?CSA-ISPLevel1.xml)  [Intermediate](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?CSA-ISPLevel2.xml)  [Advanced](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?CSA-ISPLevel3.xml) | [Tasks](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/qs_schedule.aspx?013)  [KSAs](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/ksa_schedule.aspx?013) |
| Cyber Trainer: Develops, plans, coordinates, and evaluates cyber training courses, methods, and techniques. Develops training policy and plans for personnel involved in all facets of cyber operations. | [Entry](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?TRAINLevel1.xml)  [Intermediate](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?TRAINLevel2.xml)  [Advanced](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?TRAINLevel3.xml) | [Tasks](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/qs_schedule.aspx?012)  [KSAs](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/ksa_schedule.aspx?012) |
| IA Compliance Agent: Manages and administers the documentation, validation, and accreditation processes necessary to assure that new IT systems meet DOD IA requirements. | [Entry](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?IACALevel1.xml)  [Intermediate](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?IACALevel2.xml)  [Advanced](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?IACALevel3.xml) | [Tasks](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/qs_schedule.aspx?005)  [KSAs](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/ksa_schedule.aspx?005) |
| Network Infrastructure Specialist: Installs, configures, tests, and maintains networks including hardware (hubs, bridges, switches, multiplexers, and routers) and software that permit the sharing and transmission of information. | [Entry](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?NETWLevel1.xml)  [Intermediate](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?NETWLevel2.xml)  [Advanced](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?NETWLevel3.xml) | [Tasks](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/qs_schedule.aspx?002)  [KSAs](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/ksa_schedule.aspx?002) |
| Network Operations Manager: Provides management of network operations. | [Entry](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?NETOPLevel1.xml)  [Intermediate](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?NETOPLevel2.xml)  [Advanced](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?NETOPLevel3.xml) | [Tasks](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/qs_schedule.aspx?016)  [KSAs](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/ksa_schedule.aspx?016) |
| Server Administrator: Installs, configures, troubleshoots, and maintains server hardware and software to ensure their confidentiality, integrity, and availability. | [Entry](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?SALevel1.xml)  [Intermediate](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?SALevel2.xml)  [Advanced](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?SALevel3.xml) | [Tasks](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/qs_schedule.aspx?001)  [KSAs](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/ksa_schedule.aspx?001) |
| System Security Analyst: Responsible for the integration, testing, operations, and maintenance of systems security. | [Entry](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?SSALevel1.xml)  [Intermediate](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?SSALevel2.xml)  [Advanced](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?SSALevel3.xml) | [Tasks](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/qs_schedule.aspx?007)  [KSAs](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/ksa_schedule.aspx?007) |
| Systems Architect: Responsible for the systems concepts and capabilities phases of the systems development lifecycle. | [Entry](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?SYS-ARCHLevel1.xml)  [Intermediate](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?SYS-ARCHLevel2.xml)  [Advanced](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?SYS-ARCHLevel3.xml) | [Tasks](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/qs_schedule.aspx?006)  [KSAs](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/ksa_schedule.aspx?006) |
| Technical Support Specialist: Provides technical support to customers who need assistance utilizing client level hardware and software. | [Entry](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?SUPPLevel1.xml)  [Intermediate](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?SUPPLevel2.xml)  [Advanced](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/levels_schedule.aspx?SUPPLevel3.xml) | [Tasks](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/qs_schedule.aspx?019)  [KSAs](https://disa.deps.mil/ext/cop/iase/specialty_courses/schedule/Pages/ksa_schedule.aspx?019) |

Table 2 - Cybersecurity Roles

# **3.0 PHYSICAL SECURITY TRAINING**

## **3.1 Applicable Security Controls**

The following physical security controls have been documented as requiring training:

|  |  |  |  |
| --- | --- | --- | --- |
| Number | Control | Control Text | Training Resource |
| PE-1 | Physical and Environmental Protection Policy and Procedures | This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PE family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance | [Introduction to Physical Security](http://www.cdse.edu/catalog/elearning/PY011.html) |
| PE-2 | Physical Access Authorizations | This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards, and smart cards | [Physical Security Planning and Implementation](http://www.cdse.edu/catalog/elearning/PY106.html)  [Implementing Effective Physical Security Countermeasures](http://www.cdse.edu/catalog/webinars/physical-security/physical-security-countermeasures.html) |
| PE-3 | Physical Access Control | This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Physical access devices include, for example, keys, locks, combinations, and card readers. | [Lock and Key Systems](http://www.cdse.edu/catalog/elearning/PY104.html) |
| PE-6 | Monitoring Physical Access | Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities | [Physical Security Measures](http://www.cdse.edu/catalog/elearning/PY103.html) |

Table 3 - Physical Security Control Training

## **3.2 Personnel and Roles**

The following roles have been identified as requiring physical security training:

|  |  |  |
| --- | --- | --- |
| Role | Personnel | Training Completed? |
| Security Manager |  | Choose an item. |
| Physical Security Manager |  | Choose an item. |
| Base Security |  | Choose an item. |

Table 4 - Physical Security Roles and Personnel

# **4.0 MALICIOUS CODE TRAINING**

A well-trained workforce provides another organizational safeguard that can be employed as part of a defense-in-depth strategy to protect {ACRONYM} against malicious code coming in to {ACRONYM} via email or the web applications. Personnel are trained to look for indications of potentially suspicious email (e.g., receiving an unexpected email, receiving an email containing strange or poor grammar, or receiving an email from an unfamiliar sender but who appears to be from a known sponsor or contractor). Personnel are also trained on how to respond to such suspicious email or web communications (e.g., not opening attachments, not clicking on embedded web links, and checking the source of email addresses). For this process to work effectively, all {ACRONYM} personnel are trained and made aware of what constitutes suspicious communications. Training personnel on how to recognize anomalous behaviors in {ACRONYM} information systems can potentially provide early warning for the presence of malicious code. Recognition of such anomalous behavior by {ACRONYM} personnel can supplement automated malicious code detection and protection tools and systems employed by {ACRONYM}.

DISA’s [DoD Cyber Awareness Challenge](http://iatraining.disa.mil/eta/cyberchallenge/launchpage.htm) contains the following modules that meet the DoD requirement for malicious code training.

Malicious code can do damage by corrupting files, erasing your hard drive, and/or allowing hackers access. Malicious code includes viruses, Trojan horses, worms, macros, and scripts and can be spread by e-mail attachments, downloading files, and visiting infected Websites. To prevent viruses and the download of malicious code:

1. Turn off automatic downloading
2. Scan all external files before uploading to your computer
3. Don’t e-mail infected files to anyone
4. Don’t access Websites in e-mail or popups

Mobile Code Tips - Mobile code can be malicious code. To prevent damage from malicious mobile code:

1. Require confirmation before enabling ActiveX or other mobile code technology
2. Only allow mobile code to run from your organization or your organization’s trusted sites
3. Contact your security POC or help desk for assistance, especially with e-mails requesting personal 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 | Reference |
| --- | --- | --- | --- | --- | --- | --- | --- |
| AT-1 | AT-1 (a) | CCI-002048 | 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 roles as organizational personnel with security awareness and training responsibilities. | Automatically compliant with this CCI because they are covered at the DoD level |
| AT-1 | AT-1 (a) | CCI-002049 | 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 roles as organizational personnel with security awareness and training responsibilities. | Automatically compliant with this CCI because they are covered at the DoD level |
| AT-1 | AT-1 (a) (1) | CCI-000100 | High Moderate Low | High Moderate Low | High Moderate Low | DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures.   DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.   Comment: The organization's use of their higher command policy/procedures meets this requirement if more stringent. | Automatically compliant with this CCI because they are covered at the DoD level |
| AT-1 | AT-1 (a) (1) | CCI-000101 | High Moderate Low | High Moderate Low | High Moderate Low | DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| AT-1 | AT-1 (a) (2) | CCI-000103 | High Moderate Low | High Moderate Low | High Moderate Low | DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| AT-1 | AT-1 (a) (2) | CCI-000104 | High Moderate Low | High Moderate Low | High Moderate Low | DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.  DoD has defined the roles as organizational personnel with security awareness and training responsibilities. | Automatically compliant with this CCI because they are covered at the DoD level |
| AT-1 | AT-1 (b) (1) | CCI-000102 | High Moderate Low | High Moderate Low | High Moderate Low | DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures.   DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| AT-1 | AT-1 (b) (1) | CCI-001564 | 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 reviewed annually - updated as appropritate but at least within 10 years of date of issuance. | Automatically compliant with this CCI because they are covered at the DoD level |
| AT-1 | AT-1 (b) (2) | CCI-000105 | High Moderate Low | High Moderate Low | High Moderate Low | DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.  DoD has defined the frequency as annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| AT-1 | AT-1 (b) (2) | CCI-001565 | 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 reviewed annually - updated as appropriate. | Automatically compliant with this CCI because they are covered at the DoD level |
| AT-2 | AT-2 | CCI-001480 | 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 (DoDD 8570.01).    DoD has defined the frequency as annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| AT-2 (1) | AT-2 (1) | CCI-000107 | blank | blank | blank | DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT is the DoD baseline standard.    DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| AT-2 (2) | AT-2 (2) | CCI-002055 | High Moderate Low | High Moderate Low | High Moderate Low | The IA Awareness CBT, "Cyber Awareness Challenge," and Virtual Training Environment (VTE) Courses: "Introduction to Insider Threat" and "Monitoring for Insider Threat" available on the IASE website meet the DoD requirement to include security awareness training on recognizing and reporting potential indicators of insider threat.   DoD Components are automatically compliant with this CCI because they are covered by the DoD level training available on the IASE website. | Automatically compliant with this CCI because they are covered at the DoD level |
| AT-2 | AT-2 (a) | CCI-000106 | High Moderate Low | High Moderate Low | High Moderate Low | DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT is the DoD baseline standard.    DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| AT-2 | AT-2 (b) | CCI-000112 | High Moderate Low | High Moderate Low | High Moderate Low | DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT is the DoD baseline standard.    DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| AT-2 | AT-2 (c ) | CCI-001479 | High Moderate Low | High Moderate Low | High Moderate Low | DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT is the DoD baseline standard.    DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| AT-3 (1) | AT-3 (1) | CCI-001481 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines: 1. Documentation of environmental controls that require training.  2. Documented list of personnel defined in AT-3 (1), CCI 2050 3. Ensures identified personnel have received the initial training. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AT-3 (1) | AT-3 (1) | CCI-001482 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines: 1. Documentation of environmental controls that require training.  2. Documented list of personnel defined in AT-3 (1), CCI 2050 3. Ensures identified personnel have received training annually.   DoD has defined the frequency as annually. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AT-3 (1) | AT-3 (1) | CCI-002050 | 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 whom initial and refresher training in the employment and operation of environmental controls is to be provided.   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. |
| AT-3 (1) | AT-3 (1) | CCI-001483 | 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 annual. | Automatically compliant with this CCI because they are covered at the DoD level |
| AT-3 (2) | AT-3 (2) | CCI-001566 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines: 1. Documentation of physical security controls that require training.  2. Documented list of personnel defined in AT-3 (2), CCI 2051 3. Ensures identified personnel have received the initial training. | [Section 3.1](#_3.1_Applicable_Security)  [Section 3.2](#_3.2_Personnel_and) |
| AT-3 (2) | AT-3 (2) | CCI-001567 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines:  1. Documentation of physical security controls that require training.  2. Documented list of personnel defined in AT-3 (2), CCI 2051 3. Ensures identified personnel have received training annually.   DoD has defined the frequency as annual. | [Section 3.1](#_3.1_Applicable_Security)  [Section 3.2](#_3.2_Personnel_and) |
| AT-3 (2) | AT-3 (2) | CCI-002051 | High Moderate Low | High Moderate Low | High Moderate Low | 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 whom initial and refresher training in the employment and operation of physical security controls is to be provided.   DoD has determined the personnel or roles are not appropriate to define at the Enterprise level. | [Section 3.2](#_3.2_Personnel_and) |
| AT-3 (2) | AT-3 (2) | CCI-001568 | 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 annual. | Automatically compliant with this CCI because they are covered at the DoD level |
| AT-3 (3) | AT-3 (3) | CCI-002052 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the security training materials to ensure the organization being inspected/assessed includes practical exercises in security training that reinforce training objectives. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| AT-3 (4) | AT-3 (4) | CCI-002053 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the training materials and indicators of malicious code defined in AT-3 (4), CCI 2054 to ensure the organization being inspected/assessed provides users with the means to recognize suspicious communications and anomalous behavior in organizational information systems. | [Section 4](#_4.0_MALICIOUS_CODE) |
| AT-3 (4) | AT-3 (4) | CCI-002054 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented indicators to ensure the organization being inspected/assessed defines indicators of malicious code to recognize suspicious communications and anomalous behavior in organizational information systems.   DoD has determined the indicators are not appropriate to define at the Enterprise level. | [Section 4](#_4.0_MALICIOUS_CODE) |
| AT-3 | AT-3 (a) | CCI-000108 | High Moderate Low | High Moderate Low | High Moderate Low | DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT for privileged users is the DoD baseline standard.    DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDD 8570.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| AT-3 | AT-3 (b) | CCI-000109 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines documented records (IAW AT-4) of their privileged users training. | [Section 2.2](#_2.2_Privileged_User) |
| AT-3 | AT-3 (c ) | CCI-000110 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines documented records (IAW AT-4) of their privileged users training. | [Section 2.2](#_2.2_Privileged_User) |
| AT-3 | AT-3 (c ) | CCI-000111 | 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 |
| AT-4 | AT-4 (a) | CCI-000113 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the security awareness training activities to ensure the organization being inspected/assessed documents training activities to include basic security awareness training (per AT-2) and role-based security related training (per AT-3) IAW DoD 8570.01M. | [Section 2.1](#_2.1_General_User)  [Section 2.3](#_2.3_Role-Based_Training) |
| AT-4 | AT-4 (a) | CCI-000114 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines records identifying personnel who have received training and the date the training was received | Externally available |
| AT-4 | AT-4 (b) | CCI-001336 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines training records to ensure records have been maintained for at least 5 years or 5 years after completion of a specific training program.    DoD has defined the frequency as at least 5 years or 5 years after completion of a specific training program. | Externally available |
| AT-4 | AT-4 (b) | CCI-001337 | 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 at least 5 years or 5 years after completion of a specific training program. | Automatically compliant with this CCI because they are covered at the DoD level |

# **APPENDIX B – TRAINING RESOURCES**

The below resources have been compiled to assist with Security Awareness Training requirements. Additional, commercial-based training, may be used to supplement in-house DoD provided training.

* Federal Virtual Training Environment [](https://fedvte.usalearning.gov/)
* Center for Development of Security Excellence [](http://www.cdse.edu/catalog/elearning/)
* DISA Cybersecurity Online Training [](http://iase.disa.mil/eta/Pages/index.aspx)
* DISA Cybersecurity Classroom Training [](https://disa.deps.mil/ext/cop/iase/classroom_training/Pages/index.aspx)
* DISA Cybersecurity Role-based Training [](https://disa.deps.mil/ext/cop/iase/specialty_courses/Pages/index.aspx)
* Cyber Awareness Presentations [](https://disa.deps.mil/ext/cop/iase/cyber-presentations/Pages/index.aspx)
* National Security Agency Guidance for Addressing Malicious Code Risk [PDF icon](https://www.nsa.gov/ia/_files/guidance_for_addressing_malicious_code_risk.pdf)