DoD Cybersecurity Discipline

Implementation Plan

October 2015

Amended February 2016

Executive Summary

"Cyber defense of DoD systems is [my] highest cyber priority; if DoD systems are not dependable in the face of cyber warfare, all other DoD missions are at risk."

– Secretary of Defense Ashton Carter, April 18, 2015

Inspections and incidents across the Department of Defense (DoD) reveal a need to reinforce basic cybersecurity requirements identified in policies, directives, and orders. In agreement with the Secretary of Defense, the Deputy Secretary of Defense, and the Joint Chiefs of Staff, the DoD Chief Information Officer (CIO) identified key tasks needed to ensure those requirements are achieved. The DoD Cybersecurity Campaign reinforces the need to ensure Commanders and Supervisors at all levels, including the operational level, are accountable for key tasks, including those identified in this Implementation Plan. The Campaign does not relieve a Commander's and Supervisor's responsibility for compliance with other cybersecurity tasks identified in policies, directives, and orders, but limits the risk assumed by one Commander or Supervisor in key areas in order to reduce the risk to all other DoD missions.

As part of the Campaign, this Implementation Plan is grouped into four Lines of Effort. The requirements within each Line of Effort represent a prioritization of all existing DoD cybersecurity requirements. Each Line of Effort focuses on a different aspect of cybersecurity defense-in-depth that is being exploited by our adversaries to gain access to DoD information networks. The four Lines of Effort are:

1. Strong authentication - to degrade the adversaries' ability to maneuver on DoD information networks;
2. Device hardening - to reduce internal and external attack vectors into DoD information networks;
3. Reduce attack surface - to reduce external attack vectors into DoD information networks; and
4. Alignment to cybersecurity / computer network defense service providers - to improve detection of and response to adversary activity

In conjunction with this Implementation Plan, a DoD Cybersecurity Scorecard effort led by the DoD CIO includes prioritized requirements within these Lines of Effort. Although similar to and supportive of one another, they maintain two distinct reporting mechanisms with two distinct targets. Commanders and Supervisors at all levels will report their status with the requirements in this Implementation Plan via the Defense Readiness Reporting System (DRRS), allowing leadership to review compliance down to the tactical level. In contrast, the Cybersecurity Scorecard is a means for the Secretary of Defense to understand cybersecurity compliance at the strategic level by reporting metrics at the service tier.

Securing DoD information networks to provide mission assurance requires leadership at all levels to implement cybersecurity discipline, enforce accountability, and manage the shared risk to all DoD missions. By including cybersecurity compliance in readiness reporting, this campaign forces awareness and accountability for these key tasks into the command chains and up to senior leadership, where resourcing decisions can be made to address compliance shortfalls.

The Cybersecurity Discipline Implementation Plan and Cybersecurity Scorecard efforts are critical to achieving the strategic goal of Defending DoD information networks, securing DoD data, and mitigating risks to DoD missions as set forth in the 2015 DoD Cyber Strategy. The aforementioned line of efforts and associated tasks shall be linked to DoD Cyber Strategy implementation efforts whenever possible.

The DoD Cybersecurity Campaign, reinforced by the USCYBERCOM Orders, will begin as soon as possible. Reporting on cybersecurity readiness in the scorecard and DRRS will begin as soon as possible.

Introduction

Threats against the Department's networks and information systems (IS) continue to increase. It is time for Commanders and Supervisors at all levels, including the operational level, to lead engagement in improving cybersecurity readiness across the force. Inspection reports and lessons learned from recent network intrusions have revealed Department-wide, systemic shortfalls in implementing basic cybersecurity requirements established in policies, directives, and orders. Most successful cyberspace intrusions exploit preventable and generally well-known vulnerabilities. The mission is at risk, and every individual must understand their roles, responsibilities, and actions necessary to maintain a high, persistent state of cybersecurity readiness required to deliver mission assurance.

Purpose. In coordination between Commander, USCYBERCOM and the DoD CIO, this Implementation Plan directs Commanders and Supervisors to implement the four prioritized Lines of Effort herein to mitigate risks and operationalize cyber readiness reporting for the information systems they own, manage, or lease for mission assurance through DRRS.

End State. A persistent state of high enterprise cybersecurity readiness across the DoD environment required to deliver mission assurance on all unclassified, Secret fabric, and Top Secret (TS) collateral DoD information systems, including DoD programs; special access programs; mission systems; and strategic, tactical, and RDT&E systems - hereafter called "DoD information networks."

Method. In order to raise Commanders' and Supervisors' awareness and accountability for critical cybersecurity readiness of their information systems, associated reporting requirements will be included in DRRS and the cybersecurity scorecard. Details regarding the reporting criteria are included in each section of this Implementation Plan. Leaders throughout the Department are responsible for ensuring the information capabilities they own, manage, or lease have implemented the requisite level of cybersecurity. The security principles in cyberspace are very similar to those in securing physical battlespace.

- Fortify the security posture for DoD information networks by reducing the number of vulnerable points through which an adversary could gain access and move laterally. This critical area drives three requirements: use strong authentication, harden the devices, and reduce the attack surface.
- Ensure continued protection, monitoring, analysis, detection, and response against intrusion attempts. Computer Network Defense Service Providers (CNDSPs) perform this function for the DoD information networks, requiring Commanders to align their systems and networks to CNDSPs.

The Lines of Effort within this document comprise the first phase of this Implementation Plan in order to maximize the initial reduction of network- and system-based risk to mission readiness. The DoD Cybersecurity Campaign will continue to prioritize efforts to assist Commanders and Supervisors in focusing on the most important requirements contained within existing cybersecurity policies, directives, and orders. Follow on guidance regarding specific objectives and required support will be promulgated separately. Appendix D provides the mapping of this Implementation Plan's Lines of Effort to the DoD Cybersecurity Scorecard.

For all instances where DoD Component CIOs and/or Authorizing Officials determine it is not possible to comply with the requirements within the Lines of Effort below due to operational or system constraints, a

risk management decision may be made by the DoD Information Security Risk Management Committee (ISRMC) to allow continued operation in accordance with DoDI 8510.01 (Reference (e)). The DoD ISRMC will evaluate the risk to the DoD as a whole and balance that against the impact on the mission.

Lines of Effort.

1. Strong Authentication. Reducing anonymity as well as enforcing authenticity and accountability for actions on DoD information networks improves the security posture of the DoD. The connection between weak authentication and account takeover is well-established. Strong authentication helps prevent unauthorized access, including wide-scale network compromise by impersonating privileged administrators. Commanders and Supervisors will focus attention on protecting high-value assets, such as servers and routers, and privileged system administrator access. This line of effort supports objective 3-4 in the DoD Cyber Strategy, requiring the DoD CIO to mitigate known vulnerabilities by the end of 2016.

2. Device Hardening. Ensuring devices are properly hardened increases the cost of, and complexity required for, successful exploitation attempts by the adversary. Commanders and Supervisors must prevent common exploitation techniques through proper configuration, vulnerability patching, and disabling active content in emails. These measures are critical to thwarting an adversary's ability to escalate privileges and maneuver freely within a DoD enclave. This line of effort supports objective 3-4 in the DoD Cyber Strategy, requiring the DoD CIO to mitigate known vulnerabilities by the end of 2016.

3. Reduce Attack Surface. The attack surface of DoD information networks has many aspects that must be addressed to improve cybersecurity readiness. Commanders and Supervisors will mitigate the threat of Internet-based adversaries by eliminating Internet-facing servers from the DoDIN core, ensuring Internet-facing servers in DoD demilitarized zones (DMZ) are operationally required, and removing trust relationships with external authentication services. If adversaries are able to gain access to systems within a DoD DMZ, they must be prevented from exploiting Active Directory trust relationships to gain elevated privileges inside the DoDIN core. This requires the proper management of trust relationships between DoD enclaves. Commanders and Supervisors must ensure only authorized devices are able to access DoD infrastructure physically and logically. All of these protections come from security measures that are already required. This line of effort supports objectives 3-1 and 3-2 in the DoD Cyber Strategy, requiring DoD to build the JIE single security architecture and follow best-in-class cybersecurity practices to allow USCYBERCOM and DoD components to maintain comprehensive situational awareness of network threats and mitigations.

4. Alignment to Cybersecurity / Computer Network Defense Service Providers. Monitoring activity at the perimeter, on the DoDIN, and on all DoD information networks ensures rapid identification and response to potential intrusions. The alignment of networks and information systems to CNDSPs is required to mitigate cybersecurity threats and enable the provision of accurate, timely, and secure information to the warfighter. Commanders and Supervisors will provide standardized information to the CNDSP. CNDSPs will exercise response plans to validate the processes, subscriber documents, contact information, and communication mechanisms. This line of effort supports objective 3-5 in the DoD Cyber Strategy, requiring the DoD CIO to improve the effectiveness of the current DoD CNDSP construct in defending and protecting DoD networks.

Background

Inspections, reports, and lessons learned from recent intrusions have revealed Department-wide systemic shortfalls in implementing the basic cybersecurity requirements. These requirements are established in DoD issuances, USCYBERCOM tasking orders (TASKORDs), Information Assurance Vulnerability Alerts (IAVAs), and DISA Security Requirements Guides (SRGs) and Security Technical Implementation Guides (STIGs). Due to the interconnected nature of DoD information networks, an increased degree of risk tolerance within one enclave constitutes a threat to the entire enterprise, effectively lowering the barrier to success for DoD cyber adversaries. Information technology (IT) operational readiness, cybersecurity, and accountability must be re-prioritized as DoD's mission is increasingly dependent upon the security of its IT investments.

The marketplace has lowered the cost of computing resources, reducing the cost of entry and enabling the success of less sophisticated actors. This has resulted in steadily increasing levels of cybersecurity risk to the Department's networks and critical infrastructure. These threats and risks have been recognized by DoD for several years, and the Department has responded with policies and procedures directing the implementation of cybersecurity practices for DoD IT.

Reviews of lessons learned show the Department has achieved modest reductions in its attack surface and still allows its highest privileged users to leverage the weakest means of authentication. There are still accredited/authorized information systems without CNDSP monitoring, and many of those assets still lack proper device hardening. Mitigation of risks to these areas can only be achieved through diligent adherence to system acquisition and accreditation/authorization standards, STIG/SRG implementation, system patching activities, identification and access controls, and other activities designed to heighten DoD IS security postures.

Line of Effort 1: Strong Authentication

The goal of strong authentication is to reduce anonymity and improve the security posture of the Department and DoD information networks. Strong authentication as defined by CNSSI 4009 (Reference (u)) requires two or more factors in order to securely authenticate a user: 1) something the user knows, such as a password or key code; 2) something the user is, such as biometrics; and 3) something the user has, such as a security token. The ultimate outcome is that systems (of whatever sort) require PKI-based authentication/credentials. The connection between weak passwords and account takeovers via brute force attacks are well-established. Traditionally, individuals requiring access to DoD information networks had to create network- and system-specific user names and passwords to access information online. DoDI 8520.03 (Reference (f)) requires system owners to evaluate the sensitivity level of the information on their system to determine what type of authentication credential is required from the user. The question is: "Can an adversary access resources using a password even if DoD personnel cannot?" Logging on via PKI may still leave a gap if the attacker can log on using a password. Therefore, the system must require PKI.

Per Component responses to TASKORDs and FRAGOs, DoD compliant tokens have been issued to the majority of DoD system users and their use is mandated for access to NIPRNet and Secret-level networks. Per USCYBERCOM ORDERS (Reference (ae)), the strong authentication requirements for Privileged Users across the DoD information network are established. The Department is a high-profile target; web servers, web applications, user systems, and network devices are constantly vulnerable to password-based exploitation. Requiring strong authentication helps prevent compromised user credentials from being exploited for unauthorized lateral movement within trusted zones, web servers, and web applications : 1)

internal to the NIPRNet (not in a DoD DMZ); 2) hosting controlled unclassified information within a DoD DMZ; and 3) on all Secret-level networks will improve DoD required strong authentication.

Task 1.1: Commanders and Supervisors must ensure their web servers and web applications internal to the NIPRNet (not in a DoD DMZ) require DoD-approved PKI user authentication.

DoDI 8520.03 (Reference (f)) states: "For all sensitivity levels, information systems will support identity authentication using all credential strengths that meet or exceed the minimum identified." This means that all DoD information systems must support user authentication with DoD-approved PKI, regardless of the sensitivity level of information on the system. In the face of current threats, this higher level of trust is needed for authenticating users to web servers and web applications internal to the NIPRNet (not in a DoD DMZ). In preferential order:

i. PK-enable requiring DoD-approved PKI to PKI authenticate directly at the web server or web application. This requirement is satisfied when web servers require direct PKI authentication for web applications they host.

ii. If i. is not possible, then the web server or web application must be served by a DoD-approved, PK-enabled proxy (Example: DoD Authentication Gateways).

iii. For users unable to use i. or ii. and if it is operationally approved by the requisite DoD Component CIO, use an assertion service that is compliant with DoD standards. Ensure you include justification for this selection. An assertion service is a DoD strong authentication mechanism that provides additional challenges and responses to prove an identity (Example: DoD Self-service Logon).

- If all users are required to be authenticated to web servers and web applications internal to the NIPRNet (not in a DoD DMZ) via one of the three methods, then Achieved.
- If any users are able to be authenticated to web servers and web applications internal to the NIPRNet (not in a DoD DMZ) without using one of the three methods, or are able to access them anonymously, then Not Achieved.

Task 1.2: Commanders and Supervisors must ensure their web servers and web applications hosting controlled unclassified information (CUI) within a DoD DMZ require DoD approved PKI user authentication.

This higher level of trust is also needed for authenticating users to web servers and web applications hosting CUI within a DoD DMZ. DoDM 5200.01-V4 (Reference (i)) defines CUI as "unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies." In preferential order:

i. PK-enable using DoD-approved PKI and require direct PKI authentication at the web server or web application. This requirement is satisfied when web servers require direct PKI authentication for web applications they host.

ii. If i. is not possible, then the web server or web application must be served by a DoD-approved, PK-enabled proxy (Example: DoD Authentication Gateways).

iii. For users unable to use i. or ii. and if it is operationally approved by the requisite DoD Component CIO, use an assertion service that is compliant with DoD standards. Ensure you include justification for this selection. An assertion service is a DoD strong authentication mechanism that provides additional challenges and responses to prove an identity (Example: DoD Self-service Logon).

- If all users are required to be authenticated to web servers and web applications hosting CUI within a DoD DMZ via one of the three methods, then Achieved.
- If any users are able to be authenticated to web servers and web hosting CUI within a DoD DMZ without using one of the three methods, or able to access them anonymously, then Not Achieved.

Task 1.3: Commanders and Supervisors must ensure their web servers and web applications residing on Secret-level networks require DoD approved PKI user authentication.

This higher level of trust is also needed for authenticating users to web servers and web applications on Secret-level networks. In preferential order:

i. PK-enable using DoD-approved PKI and require direct PKI authentication at the web server or web application. This requirement is satisfied when web servers require direct PKI authentication for web applications they host.

ii. If i. is not possible, then the web server or web application must be served by a DoD-approved, PK-enabled proxy (Example: DoD Authentication Gateways).

iii. For users unable to use i. or ii. and if it is operationally approved by the requisite DoD Component CIO, use an assertion service that is compliant with DoD standards. Ensure you include justification for this selection. An assertion service is a DoD strong authentication mechanism that provides additional challenges and responses to prove an identity (Example: Authentication Gateway Service).

- If all users are required to be authenticated to web servers and web applications on a Secret-level network via one of the three methods, then Achieved.
- If any users are able to be authenticated to web servers and web on a Secret-level network without using one of the three methods, or able to access them anonymously, then Not Achieved.

Task 1.4: Commanders and Supervisors must ensure 100% use of separate PKI identity authentication credentials for system administrators of any DoD information network, and disable username/passwords.

Privileged user accounts present a higher risk if compromised. According to DoDI 8520.03, "information systems with administrative accounts and other accounts or roles that authorize entities access to data regardless of sensitivity level within a system shall be required to use an identity credential that meets [hardware token PKI technology]." Per Technical TASKORDs, Enterprise or Domain Administrator accounts that require smart card (e.g. Common Access Card, PIV/PIV-I, National Security System PKI Token) logon [must] use a different smart card for these accounts than for their other accounts. Amplifying direction from that Technical Attachment states that Enterprise or Domain Administrators must have at least two different smart cards, each with different PKI credentials. Ultimately, privileged credentials must be the

only acceptable access for administering a domain or system. Commands may not load multiple certificates for different privilege levels onto a single smart card. From this point forward, PKI-based authentication/credentials will be used to indicate hardware token PKI technology and two factor authentication.

a. Per Technical TASKORDs, do all Enterprise and Domain Administrators have separate PKI credentials on separate smart cards that are issued and in use?
   - If yes, then Achieved.
   - If no, then Not Achieved.

b. Does Active Directory require separate credentials?
   - If yes, then Achieved.
   - If no, then Not Achieved.

c. Has compliance been achieved with USCYBERCOM TASKORDS?
   - If disabled, then Achieved.
   - If not disabled, then Not Achieved.

d. Has compliance been achieved with USCYBERCOM TASKORDS?
   - If compliant, then Achieved.
   - If not compliant, then Not Achieved.

Task 1.5: Commanders and Supervisors will ensure any login to a network infrastructure device requires PKI-based authentication/credentials.

Network infrastructure devices are the backbone of the DoD information networks. If compromised, they can provide an accurate picture of cyber terrain, access to network configurations, and data. Strengthening the cyber defenses for network infrastructure devices remains a priority for the Department. Username and password logins are easily captured and exploited by the adversary.

STIG ID NET0445 from the Network Policy STIG (Reference (z)) states: "To ensure the proper authorized network administrator is the only one who can access the device [(e.g. routers, Layer 2 and Layer 3 switches, firewalls, intrusion detection/ prevention systems)], the [Information System Security Officer] will ensure device management is restricted by two-factor authentication (e.g., SecurID [(RSA keys)], DoD PKI, or alternate token logon)."

a. Do all network infrastructure devices require PKI-based authentication/credentials for login?

   - If all require PKI-based authentication/credentials for authentication, then Achieved.
   - If any network infrastructure device is either not capable of PKI-based authentication/credentials or is capable, but still allows username and password for login, then Not Achieved.

ENFORCING STRONG AUTHENTICATION LINE OF EFFORT OVERALL SCORING IN DRRS:

- If all are Achieved, then Achieved overall.
- If any are Not Achieved, then Not Achieved overall.

Line of Effort 2: Device Hardening

Device vulnerabilities are exploitable weaknesses in software or hardware that provide an adversary with an opportunity to compromise the confidentiality, integrity, and/or availability of an IS. Adversaries attempt to exploit vulnerabilities successfully for various purposes, including accessing or exfiltrating sensitive information, modifying system configurations, installing malicious code, and/or denying system access to authorized users. For example, a number of widely deployed operating systems have become obsolete and must be removed from the network. It is critical that those responsible for building, operating, securing, maintaining, and ensuring the confidentiality, integrity, and availability of DoD information systems maintain a unified and resilient capability to minimize the effects of these vulnerabilities on mission operations.

The Department has instituted various means to mitigate such vulnerabilities, including STIGs, the Information Assurance Vulnerability Management (IAVM) program, and the security controls adopted from National Institute of Standards and Technology (NIST) 800-53 (Reference (v)) in coordination with CNSSI 1253 (Reference (t)) within the DoD Risk Management Framework (RMF). Per DoDI 8510.01 (Reference (e)), "IT products (including applications), as defined in [DoDI 8500.01 (Reference (d))], will be configured in accordance with applicable STIGs under a cognizant [Information System Security Manager] and security control assessor." Furthermore, CJCSM 6510.02 (Reference (k)) outlines the IAVM program and its requirements, including that "[Combatant Commands/Services/Agencies/Field Agencies] are responsible for ensuring all affected assets under their purview are compliant with IAVA directives." These programs, in concert with properly configured hardening and attack detection tools such as the Host Based Security System (HBSS), assist in defending DoD assets and networks from adversarial activity.

In some cases, cybersecurity requires risk decisions with high impact. Per DoDI 8510.01 (Reference (e)), only the DoD Component CIO is allowed to accept a "High" or "Very High" level of risk and "the authority cannot be delegated below the DoD Component CIO." Any concurrence and authorization decision documentation for systems with "High" or "Very High" levels of risk will be routed to the Information Security Risk Management Committee (ISRMC) which provides strategic guidance to Tiers 2 and 3; assesses Tier 1 risk; authorizes information exchanges and connections for enterprise ISs, cross-MA ISs, cross security domain connections, and mission partner connections. Compliance with the associated POA&M timelines for these high levels of risk is critical to ensuring the cybersecurity of the Department.

Task 2.1: Commanders and Supervisors will ensure the upgrade or removal of Windows XP and Windows Server 2003 operating systems on unclassified, Secret level networks, and DoD Top Secret networks is accomplished.

Obsolete operating systems such as Windows XP and Windows Server 2003 have fewer security features and more latent vulnerabilities that are no longer remediated by the vendor.

a. Have all Windows XP operating systems been upgraded or removed from unclassified networks?
   - If yes, then Achieved.
   - If no, then Not Achieved.

b. Have all Windows XP operating systems been upgraded or removed from Secret-level networks?
   - If yes, then Achieved.

- If no, then Not Achieved.

c. Have all Windows XP operating systems been upgraded or removed from Top Secret collateral DoD information systems including DoD programs; special access programs; mission systems; and strategic, tactical, and RDT&E systems ?
   - If yes, then Achieved.
   - If no, then Not Achieved.

d. Have all Windows Server 2003 operating systems been upgraded or removed from unclassified networks?
   - If yes, then Achieved.
   - If no, then Not Achieved.

e. Have all Windows Server 2003 operating systems been upgraded or removed from Secret-level networks?
   - If yes, then Achieved.
   - If no, then Not Achieved.

f. Have all Windows Server 2003 operating systems been upgraded or removed from Top Secret collateral DoD information systems including DoD programs; special access programs; mission systems; and strategic, tactical, and RDT&E systems?
   - If yes, then Achieved.
   - If no, then Not Achieved.

Task 2.2: Commanders and Supervisors will ensure the proper configuration of all physical and virtual servers per STIGs.

Per DoDI 8510.01 (Reference (e)), servers "will be configured in accordance with applicable STIGs or SRGs where STIGs are not available." STIGs are published as tools to improve the security of DoD information systems and are hosted on DISA's Information Assurance Support Environment website (See: http://iase.disa.mil/stigs/Pages/index.aspx). STIGs and SRGs provide configuration for technologies such as operating systems, browsers, antivirus, web services, databases, Active Directory, and domain name services. The combination of applicable STIGs and SRGs will result in a secure configuration to prevent issues such as insider threats, data exfiltration, or advanced persistent threats.

a. Have the required operating system and application STIGs been implemented and validated as current on all physical and virtual servers?
   - If yes, then Achieved.
   - If no, then Not Achieved.

b. Has a risk assessment been conducted in accordance with DoDI 8510.01(Reference (e)) for all identified vulnerabilities associated with non-compliant physical and virtual server STIGs?
   - If yes, or if no operating system and application STIG vulnerabilities exist for all physical and virtual servers, then Achieved.
   - If no, then Not Achieved.

c. If the risk assessment of physical or virtual server vulnerabilities results in a "High" or "Very High" risk level, has compliance with the associated POA&M timelines approved by the cognizant Authorizing Official been achieved?
   - If compliance with the associated POA&M timelines approved by the cognizant AO has been achieved or if there are no "High" or "Very High" risk assessment results, then Achieved.
   - If compliance has not been achieved, then Not Achieved.

Task 2.3: Commanders and Supervisors will ensure HBSS is in compliance with the DoD CS direction.

a. Is HBSS in compliance with the requirements identified in the DoD CIO, CS directions?
   - If yes, then Achieved.
   - If no, then Not Achieved.

Task 2.4: Commanders and Supervisors will ensure HyperText Markup Language (HTML), Rich Text Format (RTF), and active links are disabled for Outlook email clients on unclassified and classified networks.

Common methods of exploitation in email are user interaction of clicking on malicious links or the auto-execution of malicious code on a target system. This threat exists on unclassified networks as well as classified networks primarily due to the existence of cross domain solutions. By configuring Outlook clients to disable active links and convert HTML or RTF to plain text, this attack vector can be mitigated. The Outlook 2010 (Reference (x)) and Outlook 2013 (Reference (w)) STIGs contain multiple rules for disabling this content, including STIG IDs DTOO425, DTOO214, DTOO215, DTOO314, and DTOO344.

This action does not apply to web-based email.

a. Are HTML, RTF, and active links disabled on Outlook email clients on unclassified networks?
   - If yes, then Achieved.
   - If no, then Not Achieved.

b. Are HTML, RTF, and active links disabled on Outlook email clients on classified networks?
   - If yes, then Achieved.
   - If no, then Not Achieved.

Task 2.5: Commanders and Supervisors will ensure HTML and RTF for government-provided email services are disabled for commercial mobile devices.

Similar methods in desktop email exploitation are also applicable to mobile devices. STIG ID WIR-WMS-MEM-23 within the Mobile Email Management (MEM) Server STIG (Reference (y)) requires the use of "a MEM product that either blocks or converts all active content in email (HTML, RTF, etc.) to text before the email is forwarded to the mobile device."

a. Are Mobile Email Managers configured to block or convert all active content in email (HTML, RTF, etc.) to text before the email is forwarded to all mobile devices?
   - If yes, then Achieved.
   - If no, then Not Achieved.

Task 2.6: Commanders and Supervisors will ensure all servers and network infrastructure devices (e.g., IDS, routers, RAS, NAS, firewalls) are compliant with all current (i.e., those that have not been rescinded or superseded) IAVA patch releases.

Inspections reflect an unacceptable number of unpatched vulnerabilities. The IAVM program is responsible for releasing IAVAs, ensuring an integrated capability to improve continually the Department's ability to identify and respond rapidly to vulnerabilities that adversely affect DoD servers and network infrastructure devices.

a. Are all servers and network infrastructure devices (e.g., IDS, routers, RAS, NAS, firewalls,) compliant with all current (i.e., those that have not been rescinded or superseded) IAVA patch releases?
   - If yes, then Achieved.
   - If no or if the status is unknown, then Not Achieved.

DEVICE HARDENING LINE OF EFFORT OVERALL SCORING IN DRRS:
- If all are Achieved, then Achieved overall.
- If any are Not Achieved , then Not Achieved overall.

Line of Effort 3: Reduce Attack Surface

The Department has become reliant on the connectivity between unclassified DoD information networks and the Internet as a principal mechanism for sharing information and executing enterprise-wide processes. As the DoD information network architectures have evolved, Internet-facing servers and web applications have been improperly placed in the DoDIN core. This architecture allows Internet-based users to traverse the DoDIN to connect to these Internet-facing servers. Because Internet users are allowed access to resources inside the DoDIN core, this architecture increases the attack surface of the DoDIN.

Task 3.1: Commanders and Supervisors will review all Internet-facing assets to ensure they are hosted in a DoD DMZ and disconnect all Internet-facing web servers and web applications without an operational requirement.

Commanders and Supervisors will review and report Internet-facing assets at least quarterly; remove Internet-facing assets that no longer have a mission requirement from the network; and, for the remaining Internet-facing assets, verify that accessibility to/from the Internet is still required to support the mission. If Internet access is no longer required or the asset is removed from the network, Commanders and Supervisors will ensure the IP addresses are removed from the DISA IAP whitelist. Commanders and Supervisors will also ensure all operationally required Internet-facing assets are hosted, physically or logically, in a DoD DMZ. Per Orders & FRAGOs, Commanders have the option to host unrestricted (i.e., public) applications and data in authorized Cloud Service Providers (CSPs) in lieu of a DoD DMZ. These actions will reduce the attack surface available to the adversary for exploitation.

a. Are any assets (e.g., web server, web application) Internet-facing?
   - If yes and they are in a DoD DMZ, then Achieved.
   - If yes and they are in the DoDIN core, then Not Achieved.
   - If none exist or if unrestricted data is in an authorized CSP, (Not Applicable).

b. Has the operational requirement for all Internet-facing servers and web applications that have access to/from the Internet been validated within the last three months?
   - If yes, then Achieved.
   - If no, then Not Achieved.
   - If no Internet-facing servers and web applications exist, (Not Applicable).

c. Have all Internet-facing web servers and web applications that do not have an operational requirement been disconnected from the network?
   - If yes, and they are removed from DISA IAP whitelist, then Achieved.
   - If no, then Not Achieved.
   - If no Internet-facing servers and web applications exist, (Not Applicable).

d. Have all DoDIN web servers and web applications that do not need access to/from the Internet been removed from the DISA IAP whitelist?
   - If yes, then Achieved.
   - If no, then Not Achieved.
   - If no web servers and web applications exist, (Not Applicable).

ITEM #1 OVERALL SCORING IN DRRS:
- If all four are Achieved, then Achieved overall.
- If a. is Not Achieved, then Not Achieved overall.
- If a. is Achieved and any of b., c., or d. are Not Achieved, then Amber (Qualified Yes) overall.

Task 3.2: Commanders and Supervisors will ensure that no internal DoDIN Active Directory trusts any DoD DMZ or external Active Directory.

Commanders and Supervisors will maintain visibility and report compliance of all trust relationships on the networks they control, manage, or for which they have administrator privileges. Poor management of trust relationships between authentication services remains a threat vector for the DoD's information networks. Poorly configured trust relationships allow an adversary to move undetected throughout the information networks with escalated privileges. The most critical areas of concern are the trust relationships between a DoD DMZ and the DoDIN core.

As noted in TASKORDs, once Internet-facing assets are moved into a DoD DMZ, the next step is to separate any associated applications and/or databases from these Internet-facing systems. Optimally, there are no trust relationships between a DoD DMZ and the DoDIN core; at a minimum, there are no bi-directional trust relationships. There will be no trust relationships between any part of the DoDIN and any external network.

a. Do any Active Directory controllers inside DoD information networks (DoDIN core internal to the DoDIN IAPs) trust any Active Directories external to DoD information networks or in a DoD DMZ?
   - If no, then Achieved.
   - If yes, then Not Achieved.

Task 3.3: Commanders and Supervisors will report all commercially provided Internet connections to the NIPRNet.

DoD information networks IAPs provide a standardized and centralized point of entry into the DoDIN core. Alternate entry points through commercially provided sources increase DoD's attack surface and allow adversaries unprotected pathways into the DoDIN core. Optimally, all network traffic to/from the Internet will traverse a DoD IAP. At a minimum, any commercially provided Internet connectivity will have a current DoDIN waiver. Commanders and Supervisors will identify and report Internet traffic to/from the DoD information networks that does not traverse the IAPs.

a. Are any Internet connections to DoD information networks commercially provided?
   - If none exist, then Achieved.
   - If yes, and a current DoD information networks waiver exists, then Amber (Qualified Yes).
   - If yes, and a current DoD information networks waiver does not exist, then Not Achieved.

Task 3.4: Commanders and Supervisors will ensure the physical security of their network infrastructure devices.

Physical security of network devices is paramount to mission assurance. An adversary with physical access can reconfigure network devices or connect unauthorized devices in order to exploit DoD data and disrupt mission systems. Physical security of network infrastructure devices and physical port security of these devices reduce the attack surface.

Commanders and Supervisors will ensure that all DoD-owned network infrastructure devices are physically secured in locked cabinets or in controlled access areas to prevent unauthorized access in accordance with the Network Policy STIG (Reference (z)). In addition, Commanders and Supervisors will ensure that only authorized devices can physically connect to DoD-owned network infrastructure. 802.1x authentication is the primary method of ensuring that only authorized devices can connect. Where 802.1x is unavailable, media access control (MAC) port security must be enabled.

Per the Network Policy STIG (Reference (z)), physically secured is defined as: "All network infrastructure devices (i.e., IDS, routers, RAS, NAS, firewalls) must be located in a secure room with limited access. Move all critical communications into controlled access areas. Controlled access area in this case means controlled restriction to authorized site personnel, i.e., dedicated communications rooms or locked cabinets. This is an area afforded entry control at a security level commensurate with the operational requirement. This protection will be sufficient to protect the network from unauthorized personnel. The keys to the locked cabinets and dedicated communications rooms will be controlled and only provided to authorized network/network security individuals."

a. Have all DoD network infrastructure devices been physically secured to prevent unauthorized access?
   - If yes, then Achieved.
   - If no, then Not Achieved.

Per the Network Layer 2 Switch STIG (Reference (aa)), the Network Infrastructure Router Layer 3 Switch STIG (Reference (ab)) and the Network Perimeter Router Layer 3 Switch STIG (Reference (ac))**,** a malicious user can access physical ports to connect an unauthorized device and inject or steal data from the network undetected without the use of 802.1x. Physical ports on network infrastructure devices (i.e., IDS, routers, RAS, NAS, firewalls) must be configured to use

802.1x authentication on host facing access switch ports. If they are unable to use 802.1x, then they must be configured to use MAC port security, which will shut down upon receiving a frame with a different Layer 2 source address than what has been configured or learned for port security.

b. Has physical port security been enabled on network(s) (wired or wireless)?
- If yes, then Achieved.
- If no, then Not Achieved.

ITEM #4 OVERALL SCORING IN DRRS:
- If both 4.a. and 4.b. are Achieved, then Achieved overall.
- If either 4.a. or 4.b. are Not Achieved, then Not Achieved overall.

REDUCE THE ATTACK SURFACE LINE OF EFFORT OVERALL SCORING IN DRRS:
- If all are Achieved, then Achieved overall.
- If any are Not Achieved, then Not Achieved overall.

Line of Effort 4: Alignment to Cybersecurity / Computer Network Defense Service Providers

For the purposes of this Implementation Plan, the term cybersecurity / computer network defense service provider (CNDSP), refers to accredited Tier 2 CNDSP (listed at the following site: https://disa.deps.mil/ext/cop/FSO/cndsp_PM) unless otherwise specified.

The current DoD information environment is a complex layering of multiple networks with overlapping, duplicative roles and responsibilities. As stated by the Commander, USCYBERCOM, the current network is "not defendable." For this reason, the Department must move to a more agile and defendable posture that will enable the Department's vision and strategy for U.S. military forces as they execute their assigned missions in all operational environments. The alignment of networks and information systems to CNDSPs as a centrally controlled authority is imperative to thwart cybersecurity threats and enable the provision of accurate, timely, and secure information to the warfighter.

DoD Component internal or external CNDSPs are responsible for implementing cybersecurity services in accordance with the applicable DoD Component policy (for internal CNDSPs), or the CNDSP Service Agreement (for external CNDSPs). CNDSP Service Agreements may include memoranda of agreement (MOAs), Service Level Agreements (SLAs), or support agreements such as a DD Form 1144, "Support Agreement," in accordance with DoDI 4009.19 (Reference (b)). In addition, if the CNDSP elects to contract for any supporting elements of its cybersecurity services, the CNDSP must ensure that all applicable requirements are included in the contract(s). CNDSPs will be held accountable for incorporation of the requirements in Task 4.1.a into their Component level policies, CNDSP Service Agreements, and supporting contracts, as well as the cyber incident response plan requirements in Task 4.2.

Lastly, CNDSPs must share lessons learned in accordance with CJCSI 6510.01F (Reference (m)) to facilitate better cyberspace defense. Therefore, CNDSPs will report lessons learned into the Joint Lessons Learned Information System (JLLIS) identified in CJCSI 3150.25E (Reference (l)). USCYBERCOM will periodically check for CNDSP updated information into JLLIS and this requirement will be incorporated into internal and external validation procedures.

Task 4.1: Commanders and Supervisors will ensure alignment to a CNDSP.

Per DoDI O-8530.2 (Reference (g)), "all information systems and computer networks must enter into a service relationship with a [computer network defense service] provider." Service relationships require subscribers to contribute to computer network situational awareness, including information such as asset inventory and changes in configuration (DoDI O-8530.2 (Reference (g)); updates to ports, protocols, and services (PPS) registration (DoDI 8551.01 (Reference (h)); and other data as identified in the governing CNDSP component-level policies and Service Agreements.

Alignment to a CNDSP is defined as follows:

a. Ensure a Component-established policy, or signed CNDSP Service Agreement, has been established and executed. In addition to any other requirements, the policy or Service Agreement (and any supporting contracts) will include the following requirements:
    - Maintain and provide at least every six months, or upon CNDSP request, accurate configuration management (CM) documentation. At a minimum, documentation will include network diagrams, software and hardware inventories, and any PPS listing changes in the PPS Management Registry.
    - Notify the CNDSP and provide at least annually any CM changes involving connectivity, including location, sensor name, CCSDs, bandwidth, IP address space, backend connections, and any changes that could affect NETOPS.
    - Update POC information every six months, including leadership/management, all POCs involved in cyber incident handling during and after normal work hours, Senior Security Officer (SSO), policy POC lists, and other POCs as requested.
    - Provide HBSS data feeds as agreed-upon between the subscriber and the CNDSP.
        i. If implemented, make HBSS data feeds available to the CNDSP.
    - Specify and document agreed-upon security log data and an agreed-upon interval to facilitate network defense and incident response.

    i. Is there a Component-established policy for, or signed Service Agreement with, a CNDSP that meets the identified requirements?
    - If yes, then Achieved.
    - If no, then Not Achieved.

b. Provide the CNDSP with network diagrams, software and hardware inventories, network PPS registration, updated POC information, HBSS data feeds (if implemented), and security log data as agreed to in the Agreement or Component-established policy.

    i. Have the network diagrams and network PPS listings been updated within six months?
    - If yes to both, then Achieved.
    - If no to either or both, then Not Achieved.

    ii. Has the POC information defined in Agreement or Component-established policy with the CNDSP been updated within six months?
    - If yes, then Achieved.
    - If no, then Not Achieved.

    iii. Are HBSS feeds, if implemented, provided to the CNDSP?

- If implementation of HBSS is required and the feeds have been made available, then Achieved.
- If HBSS is implemented and operating in a Disconnected, Intermittent, or Limited-bandwidth (DIL) environment that limits the ability to transmit the feeds, then Amber (Qualified Yes).
- If implementation of HBSS is required and the feeds have not been made available, then Not Achieved.
- If implementation of HBSS is not required, then Gray (Not Applicable).

iv. Are security logs provided in accordance with the Agreement or Component-established policy with the CNDSP?
- If yes, then Achieved.
- If no, then Not Achieved.

100% CNDSP ALIGNMENT LINE OF EFFORT OVERALL SCORING IN DRRS:
- If 1.a.i., 1.b.i., 1.b.ii., 1.b.iii., and 1.b.iv. are all Achieved, then Achieved overall.
- If 1.a.i, 1.b.i, AND 1.b.ii. are Achieved and 1.b.iii. and 1.b.iv. are other than Achieved, then Amber (Qualified Yes) overall.
- If 1.a.i., 1.b.i., OR 1.b.ii. are Not Achieved, then Not Achieved overall.

Task 4.2: Commanders and Supervisors with CNDSP responsibility will ensure the cyber incident response plan(s) are properly exercised and documented.

CJCSM 6510.01B (Reference (j)) requires DoD Components with CNDSP responsibilities to maintain and update a cyber incident response plan to respond to potential malicious activity. Recent events have revealed some CNDSPs do not have updated subscriber documentation and are not familiar with executing the processes outlined in their response plans. To address this shortfall, USCYBERCOM will establish via an order a requirement for CNDSPs to exercise or execute (real-world) the cyber incident response plans with at least one subscriber at least every six months, document the results, and update the response plan with the subscriber as required.

Every six months, CNDSPs will:

a. Conduct at least one exercise of a DoD Component or a subscriber organization cyber incident response plan with key stakeholders to validate the processes, subscriber documentation, contact information, and communication mechanisms included in the response plan.

- Acceptable exercise types include, in preferential order:
  a. Red team or threat emulation engagements, if and only if such activity was initiated by the CNDSP; or
  b. a table-top exercise; or
  c. a real-world event that mirrors the above requirements.

- Key stakeholders include, but are not limited to, the USCYBERCOM Joint Operations Center, the associated service cyber component or JFHQ-DoDIN, and at least one subscriber.

i. Has at least one acceptable exercise been executed with key stakeholders within the last six months?

- If yes, then Achieved.
- If no, then Not Achieved.

b. Document and retain on file the results of the exercise or real-world event for a minimum of three years.

   i. Has the documentation of the results of the exercise or real-world event been retained on file for a minimum of three years?
   - If yes, then Achieved.
   - If no, then Not Achieved.

c. Update the cyber incident response plan to reflect revised processes based on the exercises and/or real world events.

   - If there are no revisions, the date of validation will be included in the response plan. USCYBERCOM will spot check these records at will, and the CNDSP certifier will inspect these records as part of the CNDSP reauthorization process. There will be no more than six months between each response plan exercise/real-world event.

   i. Has the cyber incident response plan been updated to reflect revised processes based on the exercises and/or real world events?
   - If yes, then Achieved.
   - If no, then Not Achieved.

Appendix A - References

(a) DoDD 7730.65, "Defense Readiness Reporting System," April 23, 2007.

(b) DoDI 4009.19, "Support Agreements," April 25, 2013.

(c) DoDI 7730.66, "Guidance for the Defense Readiness Reporting System," July 8, 2011.

(d) DoDI 8500.01, "Cybersecurity," March 14, 2014.

(e) DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology," March 12, 2014.

(f) DoDI 8520.03, "Identity Authentication for Information Systems," May 13, 2011.

(g) DoDI O-8530.2, "Support to Computer Network Defense (CND)," March 9, 2001.

(h) DoDI 8551.01, "Ports, Protocols, and Services Management (PPSM)", May 28, 2014.

(i) DoDM 5200.01-V4, "DoD Information Security Program: Controlled Unclassified Information (CUI)", February 24, 2012.

(j) CJCSM 6510.01B, "Cyber Incident Handling Program," July 10, 2012.

(k) CJCSM 6510.02, "Information Assurance Vulnerability Management (IAVM) Program," November 5, 2013.

(l) CJCSI 3150.25E, "Joint Lessons Learned Program," April 20, 2012.

(m) CJSCI 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011.

(n) FRAGO – Classified as FOUO

(o) TASKORD – Classified as FOUO

(p) FRAGO – Classified as FOUO

(q) TASKORD – Classified as FOUO

(r) TASKORD – Classified as FOUO

(s) TASKORD – Classified as FOUO

(t) CNSSI 1253, "Security Categorization and Control Selection for National Security Systems," March 27, 2014.

(u) CNSSI 4009, "Committee on National Security Systems (CNSS) Glossary," April 6, 2015.

(v) NIST SP 800-53, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations,” December 2014.

(w) Outlook 2013 STIG (Version 1, Release 3), April 24, 2015.

(x) Outlook 2010 STIG (Version 1, Release 10), January 23, 2015.

(y) Mobile Email Management (MEM) Server STIG (Version 1, Release 2), May 9, 2013.

(z) Network Policy STIG (Version 8, Release 18), September 3, 2014.

(aa) Network Layer 2 Switch STIG (Version 8, Release 18), January 23, 2015.

(ab) Network Infrastructure Router Layer 3 Switch STIG (Version 8, Release 18), January 23, 2015.

(ac) Network Perimeter Router Layer 3 Switch STIG (Version 8, Release 19), April 24, 2015.

(ad) JP 6-0, "Joint Communications System," 10 June 2015

(ae) TASKORD – Classified as FOUO

Appendix B - Acronyms

CIO – Chief Information Officer
CCSD - Command Communications Service Designator
CJCSI – Chairman of the Joint Chiefs of Staff Instruction
CJCSM – Chairman of the Joint Chiefs of Staff Manual
CM – Configuration Management
CNSSI - Committee on National Security Systems Instruction
DCID - Director of Central Intelligence Directives
DIACAP – Department of Defense Information Assurance Certification and Accreditation Process
DIL - Disconnected, Intermittent, or Limited-bandwidth
DoD – Department of Defense
DoDD – Department of Defense Directive
DoDI – Department of Defense Instruction
DoDIN – Department of Defense Information Network
FRAGO – Fragmentary Order
HTML - HyperText Markup Language
IAP – Internet Access Point
IAVA – Information Assurance Vulnerability Alert
IAVM – Information Assurance Vulnerability Management
ICD – Intelligence Community Directive
IDS – Intrusion Detection System
IG – Inspector General
IP – Internet Protocol
IT – Information Technology
ISSM – Information System Security Manager
ISRMC - Information Security Risk Management Committee
JFHQ-DoDIN – Joint Force Headquarters-Department of Defense Information Network
JLLIS - Joint Lessons Learned Information System
MAC – Media Access Control
MOA – Memorandum of Agreement
NAS – Network Attached Storage
NIPRNet – Nonsecure Internet Protocol Router Network
NIST – National Institute of Standards and Technology
OPORD – Operations Order
PK – Public Key
PKE – Public Key Enable
PKI – Public Key Infrastructure
POA&M – Plan of Action and Milestones
POC – Point of Contact
PPS - Ports, Protocols, and Services
RAS – Remote Access Server
RTF – Rich Text Format
SLA – Service Level Agreement
SISO – Senior Information Security Officer
SRG – Security Requirements Guide
SSO – Senior Security Officer
STIG – Security Technical Implementation Guide
TASKORD – Tasking Order
USCYBERCOM – United States Cyber Command

Appendix C - Order of Priority and Task Accomplishment

This appendix prioritizes the seven primary objectives listed in the Cybersecurity Campaign memorandum and further prioritizes the tasks included in the Cybersecurity Discipline Implementation Plan. Work on these tasks can proceed in parallel; these lists guide the application of limited resources to the most critical tasks for securing and defending segments of the network across the Department.

Of primary importance is implementing a healthy cybersecurity culture across all ranks, one that ingrains a self-correcting discipline similar to the nuclear enterprise or other critical, highly reliable organizations. If we fail to change the culture, we will fail to secure the enterprise regardless of any defenses installed otherwise. Of the other six campaign objectives, the weight of effort is as follows:

- Providing accurate reporting on Components' cybersecurity posture through the DoD Cybersecurity Scorecard;
- Completing the tasks listed in the Cybersecurity Discipline Implementation Plan;
- Developing a framework for the Defensive Cyberspace Operations-Internal Defense Measures (DCO-IDM) concept of operations;
- Implementing the initiatives from the DoDIN Enterprise Cyber Readiness Executive Committee;
- Supporting the Platform Information Technology-Control Systems (PIT-CS) Working Group
- Retooling the Command Cyber Readiness Inspection (CCRI) process to CCRI 2.0.

In the table below, the right columns denote if the task is tracked on the DoD Cybersecurity DoD CIO, CS directions in implementation and reporting of DoD Public Key Infrastructure (PKI) System Administrator and Privileged User Authentication.

Priority	Task Number	Description	As directed?	In PKI?
1	1.4	Commanders and Supervisors must ensure 100% use of separate PKI-based authentication credentials for system administrators any DoD information network and disable username/passwords.	Yes	Yes
2	3.1	Commanders and Supervisors will review all Internet-facing assets to ensure they are hosted in a DoD DMZ and disconnect all Internet-facing web servers and web applications without an operational requirement.	Yes	No
3	3.2	Commanders and Supervisors will ensure that no internal DoDIN Active Directory trusts any DoD DMZ or external Active Directory.	No	No
4	1.1	Commanders and Supervisors must ensure their web servers and web applications internal to the NIPRNet (not in a DoD DMZ) require DoD approved PKI user authentication.	Yes	Partial
5	1.2	Commanders and Supervisors must ensure their web servers and web applications hosting controlled unclassified information (CUI) within a DoD DMZ require DoD approved PKI user authentication.	Yes	Partial
6	1.3	Commanders and Supervisors must ensure their web servers and web applications residing on Secret-level networks require DoD approved PKI user authentication.	Yes	Partial
7	1.5	Commanders and Supervisors will ensure any login to a	Yes	Partial

		network infrastructure device requires PKI-based authentication/credentials.		
8	2.1	Commanders and Supervisors will ensure the upgrade or removal of Windows XP and Windows Server 2003 operating systems on unclassified, Secret-level, and Top Secret networks.	Yes	No
9	2.3	Commanders and Supervisors will ensure HBSS is in compliance with orders.	Yes	No
10	2.6	Commanders and Supervisors must ensure all servers and network infrastructure devices (e.g., IDS, routers, RAS, NAS, firewalls) are compliant with all current (i.e., those that have not been rescinded or superseded) IAVA patch releases.	Yes	No
11	2.2	Commanders and Supervisors will ensure the proper configuration of all physical and virtual servers per STIGs.	Yes	No
12	2.4	Commanders and Supervisors will ensure HyperText Markup Language (HTML), Rich Text Format (RTF), and active links are disabled for Outlook email clients on unclassified and classified networks.	No	No
13	2.5	Commanders and Supervisors will ensure HTML and RTF for government-provided email services are disabled for commercial mobile devices.	No	No
14	3.4	Commanders and Supervisors will ensure the physical security of their network infrastructure devices.	No	No
15	3.3	Commanders and Supervisors will report all commercially provided Internet connections to the NIPRNet.	No	No
16	4.1	Commanders and Supervisors will ensure alignment to a CNDSP.	No	No
17	4.2	Commanders and Supervisors with CNDSP responsibility will ensure the cyber incident response plan(s) are properly exercised and documented.	No	No

Appendix D - Crosswalk With the DoD Cybersecurity Requirements

The purpose of Appendix D is to provide a mapping (both in outline format or chart format) between the cybersecurity requirements within this Implementation Plan and those within the Cybersecurity requirements reported on. As noted above, the two documents are similar and supportive of one another, but maintain two distinct reporting mechanisms with two distinct targets. The below crosswalk identifies the overlaps between the requirements in both documents and clearly denotes where the requirements reside in this Implementation Plan.

Crosswalk for Line of Effort 1: Strong Authentication

Cybersecurity Discipline Implementation Plan	Cybersecurity requirements
Commanders and Supervisors must ensure their web servers and web applications internal to unclassified networks (not in a DoD DMZ) require DoD approved PKI user authentication.	"Every Web Server on SIPRNet and Private Web Server on NIPRNet Must Use Public Key Infrastructure (PKI) for User Authentication" Current Objective: All SIPR web servers and NIPR private web servers must be PK-enabled and require user PKI authentication.
Commanders and Supervisors must ensure their web servers and web applications hosting controlled unclassified information (CUI) within a DoD DMZ require DoD approved PKI user authentication.	
Commanders and Supervisors must ensure their web servers and web applications residing on Secret-level networks require DoD-approved PKI user authentication.	
Commanders and Supervisors must ensure 100% use of separate PKI-based authentication credentials for system administrators on any DoD information network and disable username/passwords.	"Ensure Every System Administrator Logs On via PKI" Current Objective: All DoD system administrators must use PKI credentials for authentication. System administrators not using PKI credentials for system access by August 31, 2015, will be required to implement mandated mitigations.
Commanders and Supervisors will ensure any login to a network infrastructure device requires PKI-based authentication/credentials.	"Ensure Every User Logs On via PKI" Current Objective: All DoD users must use PKI credentials for authentication.

Crosswalk for Line of Effort 2: Device Hardening

Cybersecurity Discipline Implementation Plan	Cybersecurity requirements
Commanders and Supervisors will ensure the upgrade or removal of Windows XP and Windows Server 2003 operating systems on DoD information networks.	"Remove Windows XP Operating System Software from Entire SIPRNet & NIPRNet Inventory" Current Objective: All devices running Windows XP will be upgraded to Windows 7 or higher.
	"Remove Windows Server 2003 Operating System Software from Entire SIPRNet & NIPRNet Inventory"

	Current Objective: All devices running Windows Server 2003 will be upgraded to Windows Server 2008 or higher.
Commanders and Supervisors will ensure the proper configuration of all physical and virtual servers per STIGs.	"Every Computer Configured to DoD Security Standard" Current Objective: All DoD information systems are properly configured, all of the time.
Commanders and Supervisors will ensure HBSS is in compliance with orders.	"Implement Host Based Security System" Current Objective: Fully compliant HBSS installation to support configuration, asset management, attack detection and blocking, and reporting.
Commanders and Supervisors will ensure HyperText Markup Language (HTML), Rich Text Format (RTF), and active links are disabled for Outlook email clients on DoD information networks.	N/A
Commanders and Supervisors will ensure HTML and RTF for government-provided email services are disabled for commercial mobile devices.	N/A
Commanders and Supervisors must ensure all servers and network infrastructure devices (e.g. IDS, routers, RAS, NAS, firewalls) are compliant with all current (i.e. those that have not been rescinded or superseded) IAVA patch releases.	"Every Computer Properly Patched" Current Objective: All DoD information systems have current patches within 21 days of IAVA patch release.
	"Evaluate and Approve Systems, Fix Vulnerabilities, Perform Regular Security Control Testing" Current Objective: Systems with high risk security weaknesses that are over 120 days overdue will be removed from the network.

Crosswalk for Line of Effort 3: Reduce Attack Surface

Cybersecurity Discipline Implementation Plan	Cybersecurity requirements
Commanders and Supervisors will review all Internet-facing assets to ensure they are hosted in a DoD DMZ and disconnect all Internet-facing web servers and web applications without an operational requirement.	"Move all Outward Facing Servers to Approved DMZs" Current Objective: All outward facing web servers must be moved to DMZs.
Commanders and Supervisors will ensure that no internal DoDIN Active Directory trusts any DoD DMZ or external Active Directory.	N/A
Commanders and Supervisors will report all commercially provided Internet connections to the NIPRNet.	N/A
Commanders and Supervisors will ensure the	N/A

physical security of their network infrastructure devices.	

Crosswalk for Line of Effort 4: Alignment to Cybersecurity / Computer Network Defense Service Providers

Cybersecurity Discipline Implementation Plan	Cybersecurity requirements
Commanders and Supervisors will ensure alignment to a CNDSP.	N/A
Commanders and Supervisors with CNDSP responsibility will ensure the cyber incident response plan(s) are properly exercised and documented.	N/A