Improving Cyber Basics

DoD Cyber Discipline Implementation Plan and DoD Cyber Scorecard

December 2016

Executive Summary

- Why did DoD develop the Cybersecurity Discipline Implementation Plan?
  - Cyber incidents and inspections across the Department consistently revealed a need to reinforce and reinvigorate **basic, pre-existing cybersecurity requirements**.
  - In short, many incidents within the past year were possible in part due to simple mistakes.
- What is the plan's primary goal?
  - The plan emphasizes the need for organizations across the Department – like the Army, Navy and Marine Corps, Air Force, and the Defense Agencies – **to go back to the cyber basics.**
- What are the plan's areas of focus?
  - 1. **Ensuring Strong Authentication** – How do users log onto devices and systems?
  - 2. **Hardening Devices** – Are devices properly configured and regularly updated?
  - 3. **Reducing the Attack Surface** – How many things directly connect to the public Internet?
  - 4. **Detecting and Responding to Potential Intrusions** – Can cyber defenders do their jobs?
- How does DoD measure progress on the plan?
  - Organizations regularly report progress up the chain of command via the **DoD Cyber Scorecard**.

Background and Priorities

- The Department analyzed inspections, reports, and lessons learned from **recent cybersecurity incidents** affecting its networks and systems.
- This analysis revealed **systematic shortfalls** in the ways in which the Department is taking care of its basic cybersecurity requirements.
- These **cyber basics include things** like ensuring that users with expanded access privileges log on in a special way and keeping software up to date.
- Because of the speed of the cyber threat and the intrinsically interconnected nature of information technology, one vulnerable device or system can present a dire risk to the **entire DoD information enterprise.**
- As a result, this plan was created to **reinforce high-priority cyber basics** that are already required in many DoD policies.

Four Lines of Effort

The Cybersecurity Discipline Implementation Plan advances high-priority cyber basics by focusing on four lines of effort. They are:

1. **Ensuring Strong Authentication** – How do users log onto devices and systems? This reduces a user's anonymity on the networks, while also enforcing authentication and accountability for a user's activities.
2. **Hardening Devices** – Are devices properly configured and regularly updated? This increases the level of difficulty and cost for an attack.
3. **Reducing the Attack Surface** – How many things directly connect to the public Internet? This reduces opportunities for adversaries to gain access.
4. **Detecting and Responding to Potential Intrusions**– Can cyber defenders do their jobs? This allows more rapid identification of incidents, better response to an intrusion, and improved defense of networks and systems.

Implementing Line of Effort #1
Ensuring Strong Authentication

- DoD is replacing usernames and passwords with more unique methods of authentication, combining at least two of the following:
  - 1) **Something the user knows**, like a password or key code
  - 2) **Something the user is**, like a biometric identifier (i.e., fingerprint)
  - 3) **Something the user has**, like a security token (i.e., DoD Common Access Card*)
    - *DoD is moving away from the use of Common Access Cards in favor of other means of access
- Many systems should require access via **Public Key Infrastructure (PKI)**, which is a cryptographic credential that can be stored on a security token
- **PKI is required for authentication in five areas**, called tasks in the plan:
  - (1) all internal Web servers and Web applications; (2) certain Web applications hosting controlled unclassified information; (3) all Web servers and Web applications located on classified networks; (4) all system administrators must have separate authentication credentials – no usernames or passwords; and (5) any network infrastructure device log on must require PKI-based authentication credentials

Implementing Line of Effort #2
Hardening Devices

- **Easily accessible devices** result from things like outdated operating systems or e-mail that does not automatically defend against dangerous links
- These devices **introduce vulnerabilities** in software or hardware that adversaries can exploit through common techniques, like phishing e-mails
- DoD is hardening its devices through several tasks outlined in the plan:
  - **Upgrade or remove operating systems** for all Windows XP and Windows Server 2003* operating systems located on unclassified and classified networks
    - *DoD is currently transitioning all of its major networks and systems to Windows 10
  - **Correctly configure** all physical and virtual servers
  - Ensure that all Host Based Security Systems (HBSS) – which are attack-detection tools that help defend assets and networks – **comply with applicable directives**
  - Disable HyperText Markup Language (HTML), Rich Text Format (RTF), and active links for **Outlook e-mail on unclassified and classified networks, and on mobile devices**
  - **Properly update (or patch)** servers and network infrastructure devices, like routers

Implementing Line of Effort #3
Reducing the Attack Surface

- **Internet-facing servers and applications**, like public Websites, introduce cybersecurity risks from Internet-based adversaries
- Unless operationally required, these connections should be **disconnected**, and if they remain, they should be **treated carefully and actively secured**
- As a result, the Department is reducing the attack surface by **reducing and better protecting these connections** through several tasks in the plan:
  - **Disconnect** all Internet-facing Web servers and Web applications that are not operationally required; if they are needed, host them in a **demilitarized zone**
    - A demilitarized zone in cybersecurity is a physical or logical subnetwork that contains an organization's public-facing servers and applications, adding an extra layer of security
  - Report all **commercially provided Internet connections** to the Department's unclassified network (known as the NIPRNet)
  - Ensure the physical security of all **network infrastructure devices**

Implementing Line of Effort #4
Detecting and Responding to Potential Intrusions

- DoD is moving to a more agile and defendable posture that will **enable cyber defenders** to better view traffic and defend networks
- As a result, DoD is ensuring that all networks and systems have a **cybersecurity service provider** from a DoD organization
- To ensure that networks and systems have a cybersecurity service provider, all organizations must align to one of these providers by:
  - **Establishing an agreement** with a service provider that meets certain criteria through either a policy or a signed and executed service agreement
  - Making sure that the service provider **understands what is on the networks** by providing critical data, such as network diagrams, per the agreement

Metrics – DoD Cyber Scorecard

- The DoD cyber scorecard measures how organizations are achieving compliance with these cyber basics. It is briefed regularly to DoD senior leadership, ensuring **visibility and accountability throughout the chain of command.**
- The scorecard **currently measures progress** on goals that are integral to the plan:
  - Log-on via PKI is required for (a) every user, and (b) every privileged user
  - PKI is used for every:
    - (a) Website and Web application on the Secret network, and
    - (b) Private Website/Web application on the DoD unclassified network
  - All Internet-facing Web servers are moved to approved DMZs
  - All (a) Windows XP, (b) Windows server 2003, and (3) older operating system software are removed from both the unclassified and classified networks
  - All systems are evaluated and approved
  - All security weaknesses are closed
  - Host Based Security Systems (HBSS) are implemented
  - Every computer is (a) properly patched and (b) properly configured

Improving Cyber Basics

DoD Cybersecurity Discipline Implementation Plan

DoD Cyber Scorecard