Addressing the Department of Defense Cybersecurity Discipline Implementation Plan
# Table of Contents

Introduction ................................................................................................................................ 3

Line of Effort 1 - Strong Authentication....................................................................................... 4

Line of Effort 2 – Device Hardening............................................................................................ 5

Line of Effort 3 – Reduce Attack Surface.................................................................................... 6

Line of Effort 4 – Alignment to Cybersecurity/Computer Network Defense Service Providers .... 7

About BeyondTrust .................................................................................................................... 9
Introduction

In September 2015, the Secretary of Defense and Chairman of the Joint Chiefs of Staff published a document titled, “Department of Defense Cybersecurity Culture and Compliance Initiative.” In it they identified several key cyber security requirements that all agencies must address in order to improve the resilience of the Department of Defense (DoD) IT networks. One of the outcomes was the Cybersecurity Discipline Implementation Plan.

The plan identifies four Lines of Effort, each representing a prioritization of all the DoD’s cyber security requirements. 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.
4. Alignment to cybersecurity / computer network defense service providers – to improve detection of and response to adversary activity.

The purpose of this document is to summarize each of the DoD’s Lines of Effort, and enumerate how The BeyondTrust IT Risk Management Platform for Federal Agencies can address them.
Line of Effort 1 - Strong Authentication

The link between weak authentication methods and account takeover is well documented. The goal of strong authentication is to reduce anonymity and enforce accountability for all DoD network actions. With strong authentication, DoD agencies can prevent unauthorized access through methods such as compromised privileged credentials.

“Ultimately, privileged credentials must be the only acceptable access for administering a domain or system.”

- DoD Cybersecurity Implementation Plan

THE BEYONDTRUST SOLUTION FOR STRONG AUTHENTICATION

BeyondTrust automates privileged password and privileged session management, providing secure access control, auditing, alerting and recording for any privileged account. To improve control over multiple authentication mechanisms, BeyondTrust centralizes authentication for Unix, Linux and Mac environments by extending Microsoft Active Directory's Kerberos authentication and single sign-on capabilities to these platforms. By improving the accountability and control over privileged access, federal agencies will reduce security risks and meet compliance requirements.

BeyondTrust solutions help reduce risk, meet compliance requirements and improve efficiency by:

- Securing and automating the process of managing and cycling privileged account passwords and SSH keys
- Controlling how people, services, applications and scripts access credentials, and alert in real-time as passwords are released and session activity is started
- Recording all user and administrator activity in a comprehensive audit trail
- Extending beyond privileged passwords, providing better threat intelligence
- Enabling users to leverage familiar (and fewer) secure credentials to access Unix, Linux or Mac systems, simplifying the user experience
- Help IT consolidate the number of directories down to as few as possible, simplifying the management of complex environments
PowerBroker Identity Services

PowerBroker Identity Services provides a simple way to maintain Active Directory as a single authentication platform across your enterprise. To provide increased security, you can leverage multi-factor authentication with Smartcards like Common Access Cards (CAC), or one-time passwords (OTP) on Unix, Linux and Mac. PowerBroker also supports multi-factor authentication for single sign-on in heterogeneous environments.

PowerBroker Password Safe

PowerBroker Password Safe is an automated password and privileged session management solution offering secure access control, auditing, alerting and recording for any privileged account – from local or domain shared administrator, to a user’s personal admin account (in the case of dual accounts), to service, operating system, network device, database (A2DB) and application (A2A) accounts – even to SSH keys and cloud accounts.

Line of Effort 2 – Device Hardening

Recent security threats show a trend toward attacks initiating through third-party credentials and mimicking normal user transactions on the network. These seemingly innocuous users are then able to navigate horizontally through the organization versus a head-on attack. The goal of device hardening is to strengthen a network by making it more difficult for threat actors to gain access through tactics like vulnerability patching, and disabling active content in email.

THE BEYONDTRUST SOLUTION FOR DEVICE HARDENING

BeyondTrust’s Vulnerability Management solutions deliver data in the proper context.

Specifically, enabling the team to proactively identify security exposures, analyze business impact, and plan and conduct remediation across network, web, mobile, cloud and virtual infrastructures, and communicate that risk to operations and compliance teams to reduce risk.

Retina CS Enterprise Vulnerability Management

Retina CS Enterprise Vulnerability Management is the only vulnerability management software solution designed from the ground up to provide organizations with context-aware vulnerability assessment and risk analysis. Retina’s results-oriented architecture works with users to proactively identify security exposures, analyze business impact, and plan and conduct remediation across disparate and heterogeneous infrastructure.
Retina CS Enterprise Vulnerability Management software enables you to:

- Discover network, web, mobile, cloud and virtual infrastructure
- Profile asset configuration and risk potential
- Pinpoint vulnerabilities, malware and attacks
- Analyze threat potential and return on remediation
- Remediate vulnerabilities via integrated patch management
- Report on vulnerabilities, compliance, benchmarks, etc.
- Protect endpoints against client-side attacks

**Retina Network Security Scanner**

*Retina Network Security Scanner* is the most sophisticated vulnerability assessment solution on the market. Available as a standalone application or as part of Retina CS Enterprise Vulnerability Management, Retina Security Scanner enables you to efficiently identify IT exposures and prioritize remediation enterprise-wide.

- Continually monitor and improve enterprise security posture
- Identify IT assets and sensitive data across disparate environments
- Find security exposures in network, web, database and virtual assets
- Prioritize remediation based on real risk to critical assets
- Easily deploy and scale from small to large environments
- Realize optimal performance via non-intrusive scanning
- Get fast, frequent updates from the BeyondTrust Research Team

**Line of Effort 3 – Reduce Attack Surface**

The third Line of Effort in the implementation plan discusses ways to reduce the attack surface of the DoD information networks. Agencies are challenged to prevent unauthorized external access through DoD servers, and maintain situational awareness of network threats.
In addition to monitoring outside threats through Retina CS Enterprise Vulnerability Management solutions, PowerBroker Password Safe can help agencies gain control over how third parties access DoD networks and applications. Password Safe provides a secure connection gateway with proxied access to RDP, SSH and Windows applications; protects privileged credentials; and records all privileged sessions.

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

Line of Effort 4 challenges agencies in the DoD to monitor network activity at its perimeter, and to employ rapid identification and response to intrusions. The goal is to align the CNDSPs to ensure there are standardized communication mechanisms in place to achieve mission operations.

THE BEYONDTRUST SOLUTION FOR REDUCING THE ATTACK SURFACE

The BeyondTrust IT Risk Management Platform for Federal Agencies

As breaches and threats actors continue to refine their approaches for penetrating agencies’ security perimeters, it is more critical than ever for agencies to have a complete view of their IT landscape and its potential risks.

The BeyondTrust IT Risk Management Platform helps agencies fulfill compliance requirements through its integrated suite of IT security solutions that reduce user-based risk and addresses...
security exposures. The platform provides IT security leaders with a single view of all assets and user activity. With behavioral analytics to understand anomalies, compliance reporting, and the ability to leverage third-party data, the platform reduces risks while helping to maximize the value of existing security investments. Available in software and hardware appliance formats, the BeyondTrust platform integrates two foundational security methodologies:

**Privileged Access Management**

BeyondTrust Privileged Access Management solutions close the gap between IT security requirements and user enablement. With BeyondTrust, security and IT operations teams gain a comprehensive privileged account management solution, deep analytical insights for better decision-making, and extensibility across the security landscape. As a result, your organization reduces IT security risks, simplifies compliance, and maintains user productivity.

**Vulnerability Management**

BeyondTrust Vulnerability Management solutions provide security professionals with vulnerability assessment and risk analysis in context. With BeyondTrust, IT teams can proactively identify security exposures, analyze business impact, and plan and conduct remediation across network, web, mobile, cloud and virtual infrastructures, and communicate that risk to operations and compliance teams to reduce risk.

---

The BeyondInsight IT Risk Management Platform

---

Addressing the DoD Cybersecurity Discipline Implementation Plan

About BeyondTrust

BeyondTrust® is a global cyber security company that believes preventing data breaches requires the right visibility to enable control over internal and external risks.

We give you the visibility to confidently reduce risks and the control to take proactive, informed action against data breach threats. And because threats can come from anywhere, we built a platform that unifies the most effective technologies for addressing both internal and external risk: Privileged Access Management and Vulnerability Management. Our solutions grow with your needs, making sure you maintain control no matter where your organization goes.

BeyondTrust's security solutions are trusted by over 4,000 customers worldwide, including over half of the Fortune 100. To learn more about BeyondTrust, please visit www.beyondtrust.com.