FORTRA®

GUIDE (TRIPWIRE)

Navigating DISA Compliance the Smart Way

Fulfilling Defense Information Systems Agency Standards

U.S. Federal Government agencies arguably have more at stake in the event of a cyberattack than other types of entities. After all, they are responsible for the stability and security of day-to-day life for Americans as well as overall national security. To ensure an impeccable level of cybersecurity across the Department of Defense (DoD) in particular, the Defense Information Systems Agency (DISA) maintains rigid cybersecurity standards with which DoD agencies must comply.

As a combat support agency, DISA applies to all six military service branches, communications centers like the Pentagon, the DoD's Cloud Computing Program Office (CCPO), the DISN (Defense Information Systems Network, and the DoD Information Network (DODIN). Numerous DISA pilot programs are continually developed and implemented to tighten DoD cybersecurity as new digital environments and threat vectors emerge.

This pivotal agency creates and maintains multiple facets of DoD cybersecurity, including the Cybersecurity Service Provider (CSSP) program and the Security Technical Implementation Guides (STIGs). In this guide, we will look at an overview of both programs along with practical advice for protecting your DoD agency with automated, continuous DISA compliance.

The DISA CSSP Program

The DISA CSSP provides a range of cybersecurity services to federal agencies. The Cybersecurity Service Provider program also monitors for cybercriminal activity, reports on cyber incidents, and communicates with the DODIN about cyber situational awareness. One way the CSSP program helps federal agencies quickly align with cybersecurity best practices is through its cloud-native monitoring tools for Microsoft Azure-hosted applications.

DISA STIG Standards

Another key function of DISA is the creation and enforcement of its Security Technical Implementation Guides. DISA STIGs give federal agencies a set of clear, explicit policies, controls, and requirements to follow to minimize their attack surface and make their networks more resilient to cyber incidents. They are created by DISA on its own or in collaboration with other federal agencies and, in some cases, directly with software and device vendors.

The settings and configurations of commercial-grade software are often set to defaults that prioritize functionality over security and therefore cannot be run as-is without concerted effort towards hardening them against cyberattacks. The purview of STIGs includes software, operating systems, servers, mobile devices, databases, network devices, and a variety of both physical and cloud endpoints. DISA releases new STIGs throughout each quarter, with hundreds of individual guides published to date.

Who Do DISA STIGs Apply to?

While DISA STIGs are mandatory for U.S. federal agencies, any organization can download and implement them freely from the STIGs Document Library to enhance their cybersecurity analogously to the Center for Internet Security's CIS Controls.

Any organization or agency that connects to DoD networks falls under the purview of DISA STIGs, as well as "all DoD developed, architected, and administered applications and systems connected to DoD networks," according to DISA.[2] Upon audit, non-compliant organizations can have their Authorization to Operate revoked and their DoD system access removed.

WHAT IS DISA?

Established in 1960, the Defense Information Systems Agency (DISA) is a United States federal agency that supports the DoD with IT services, communications technology, and regulatory compliance standards for DoD-connected networks and infrastructure. DISA's motto is "Secure the net. Defend the nation."[1]

STIG Compliance Categories

DISA breaks vulnerabilities down into three categories based on their potential severity and immediate level of risk:

- **Category I:** This category covers the most serious of threats, including vulnerabilities that directly threaten the wider network and cause significant loss of service or data breaches.
- **Category II:** The second category encompasses medium-level risks that have the potential to cause cybersecurity incidents. While they might not cause immediate harm to system integrity, these risks could expose sensitive data if not dealt with right away.
- **Category III:** Lower-level risks are more related to the accuracy and availability of data rather than potential exfiltration. However, category III risks can escalate to Categories II or I if left unchecked.

Common DISA Compliance Challenges

Considering there are hundreds of individual STIGs for agencies to apply across each and every one of their servers, operating systems, and endpoints, it would be impossible to succeed with a manual approach to DISA compliance. Manual implementation would require far too many resources and hours to consider, so agencies rely on automated solutions to apply STIGs across their environments.

In addition to the scope of DISA compliance, the other major challenge is the continual evolution of threats. New vulnerabilities and cybercriminal tactics emerge constantly, and new STIGs are also continually added and updated. At the same time, software updates can take systems out of compliance and new technology is added to the ecosystem regularly. This creates an incredibly complex moving target for agencies to hit, but advanced DISA compliance software that is kept up to date by its vendors takes some of this complexity off agencies' shoulders.

DISA Compliance with Fortra's Tripwire

With over 25 years of trailblazing experience in the cybersecurity industry, Fortra's Tripwire has a long history of helping government agencies harden their systems and eliminate vulnerabilities while maintaining regulatory compliance. Tripwire provides agencies with 200 built-in DISA Policy Frameworks to automatically enforce across their connected systems on premises and in the cloud. Tripwire keeps its policies current, so agencies don't have to continually check for updates.

Agencies trust Tripwire for unparalleled integrity management that keeps their digital environments compliant not just at audit time but around the clock. User-friendly dashboards and reports provide instant visibility into DISA STIG compliance alignment with clear remediation instructions for instances of non-compliance. Tripwire also

HOW FORTRA SUPPORTS DISA COMPLIANCE

- Automated policy enforcement
- File integrity monitoring (FIM)
- Security configuration management (SCM)
- Vulnerability management (VM)
- Penetration testing
- Red team operations
- Antivirus for servers
- Email security

Fortra's Cybersecurity Solutions for Government

Integrity Management

Tripwire® Enterprise is the leading compliance monitoring solution, using security configuration management (SCM), system and file integrity monitoring (SIM/FIM), and system monitoring for OS, firmware, and non-file related changes in real time. Backed by decades of experience, it's capable of advanced use cases unmatched by other solutions.

Vulnerability Management

Fortra's vulnerability management solution gives users complete visibility into their networks, both on-premises and in the cloud, including all devices and their associated operating systems, applications, and vulnerabilities.

Offensive Security

Fortra's offensive security solutions and services help Federal Government agencies proactively seek out weaknesses and vulnerabilities before adversaries can find them, from penetration testing with Core Impact to red team operations with Cobalt Strike.

Virus Protection

Protect your systems against malware and viruses on AIX, IBM i, Linux, Solaris, and Intel X86/X64 with behavior-based detection and customizable scanning options. Fortra's Powertech Antivirus provides server-level, native virus protection across IBM systems.

Email Security

Fortra's email security solutions safeguard federal email inboxes against common threats like account takeover, domain impersonation, spoofing, phishing, and social engineering. For example, you can combat government-targeted threats like spear phishing with DMARC email authentication from Agari DMARC Protection.

includes a Policy Editor to provide the ability to change the conditions of a specific test to determine pass/fail. The ability to employ automated-remediation workflows is also supported. In addition to DISA STIGs, Tripwire has built-in policies for National Institute of Standards and Technology (NIST) 800-53, 800-71 and Cybersecurity Maturity Model Certification (CMMC).

Tripwire's tried and true vulnerability management offering also proactively scores vulnerabilities by their associated risks to help agencies tackle their biggest issues right away. Offensive security solutions from the Fortra portfolio make it simple to run pen testing and red team operations under one unified vendor. In combination and individually, these solutions help speed up the audit process and ensure success — all while hardening systems against cyberattacks.

Fortra's Tripwire is here to partner with you as your integrity management ally. Contact us today to get started.

Sources

1. https://www.disa.mil/About
2. https://public.cyber.mil/stigs/faqs/#toggle-id-3

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

(fta-tw-gd-1224-r1-hm)