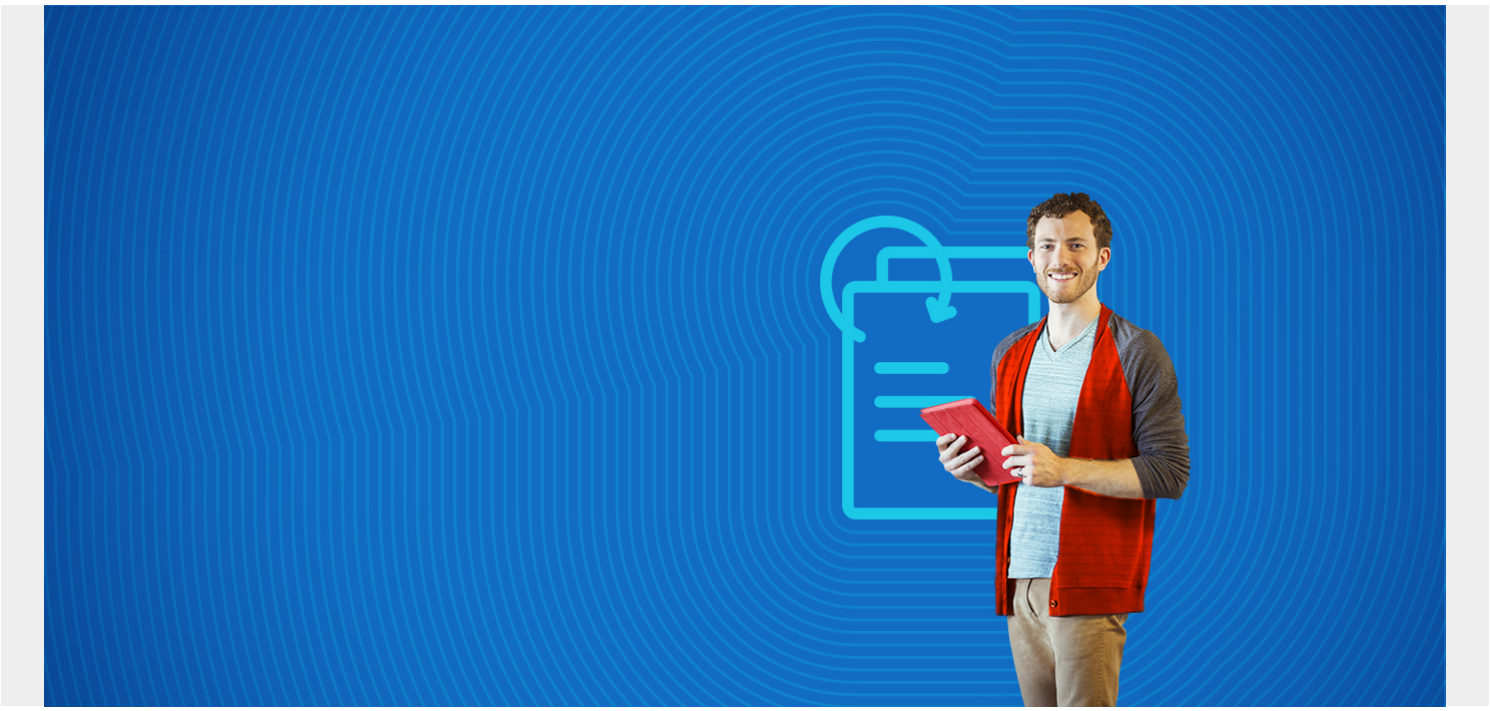
INTRODUCTION TO DISA COMPLIANCE



What is DISA compliance?

The Defense Information Systems Agency is a part of the Department of Defense (DoD), and is a combat support agency. As part of their mission of providing information technology and communications support to the government and associated defense agencies, they have created and maintain a security standard for computer systems and networks that connect to the DoD. These guidelines are sets of configurations and checklists, known as Security Technical Implementation Guides, which ensure the security of computer networks and systems. These standards have become the de facto policy for many DoD organizations, saving them significant time and effort in developing independent standards.

STIGs also lay out things like how people running systems should be trained and how often security checks and updates need to be done. Essentially, they are a set of documents that tell organizations how to handle their computer systems and networks, sometimes in minute detail. Failure to stay compliant with guidelines issued by DISA can result in an organization being denied access to DoD networks.

(This article is part of our Security & Compliance Guide. Use the right-hand menu to navigate.)

Why STIGs are used

Many software packages, operating systems and even firmware configurations are not designed with security first in mind. Default settings often leave a system relatively vulnerable for attack by a hacker. An example of this is the way that Windows operating systems are set up. The default

settings in Windows tend to leave an enormous number of remote connections open, and these configurations can allow outsiders to easily take over the computer.

Further, because of the complexity of the operating system, vulnerabilities are found on a regular basis as hackers figure out ways to get into areas that were intended to be inaccessible. Windows updates and patches as well as firewalls and antimalware software are needed to protect systems from unauthorized access. In general, the same issues tend to be true of other operating systems, hardware configurations and software suites. Leaving settings at their default and failing to install updates and patches or configure additional protections can make it easy for a hacker to access a system.

Security issues can be frustrating and problematic enough for an individual with a personal computer, but for the government or an organization that connects to government servers, it can be a matter of national security. Failing to keep a personal computer secure may lead to having to reinstall an operating system, or actual identity theft like the Office of Personnel Management breach in 2015, that resulted in the compromise of more than 22 million personnel records. If a system that connects to the DoD is hacked, it could mean someone gets a hold of classified information. Since the DoD cannot just assume that all entities connecting to their networks are using the most secure configurations on all of their systems, they created guidelines in the form of STIGs that detail security standards.

The purpose of STIGs is to make sure that any organization that is connecting to DoD networks is using the most secure settings possible. This also ensures that there is a standard that all organizations accessing DoD systems must follow, which can help with configuration and connection issues. STIGs both improve security and simplify IT services.

DISA does regular testing and research to identify which are the most secure configurations, and they do updates on a regular basis to ensure that any newly discovered vulnerabilities are addressed. On a quarterly basis, DISA goes through STIGs and updates them to fix errors, reflect policy changes and to provide clarity. Along with ensuring that systems remain compliant, organizations must also update their servers and systems when updates are made available. Major updates may be published at any time in the year, so organizations should check for updates regularly, not just on a quarterly basis.

Who must follow DISA guidelines

According to DISA, "All DoD developed, architected and administered applications and systems connected to DoD networks" must adhere to STIG guidelines; essentially, anyone that connects to the DoD in any way must comply with their standards. In addition to departments that are directly related to defense, a variety of government agencies and private contractors also have access to DoD systems and must follow the guidelines laid out in STIGs.

Organizations that connect to DoD servers must use the configurations as well as follow policies and processes laid out by STIGs, and they must ensure that configurations and processes are updated as new and amended STIGs are released. If an organization is out of compliance or out of compliance and not acting to address it, its Authorization to Operate may be revoked, and access to the DoD system may be rescinded. Checks are done regularly to ensure that all systems connecting are compliant, and auditors have the ability to check many configurations remotely.

While complying with DISA standards is required to be able to connect to DoD systems, it's not just

organizations that are associated with these systems that use STIGs as a benchmark for security. STIGs are free to download and available to the public, so private organizations can use them to improve their security. The scope of the DISA STIG implementation, initially intended for DISA has made them effectively a standard across DoD and organizations that work with DoD and other Federal government organizations.

Security technical implementation guides

There are an enormous number of STIGs; more than 400 documents lay out how to configure hardware and software and outline security protocols and training processes. STIGs provide settings for computers, operating systems, servers and networks with a goal of keeping data secure and preventing hackers from being able to access systems. Recently, STIGs have been released that cover configurations for cloud computing systems and mobile devices. Guidelines cover more than just configurations though; they also cover things like how project management, software development and testing should be handled.

The requirements of STIGs can be very precise or quite vague. For example, APP3510 simply calls for validation of a user's input, and APP3540 only states that a program should be safe from SQL injections. However, other STIGs may be very specific; APP3390 requires a programmer to lock users out of an account for an hour after three unsuccessful login attempts. Additionally, STIGs may require programmers to use particular methods of securing an application or applying encryption. Complying with STIG requirements can be a very long and in depth process; this is particularly true for operating systems, which have an enormous number of settings to configure. One of the great advantages of systems that provide out of the box (OOTB) DISA STIG Compliance Content, like TrueSight Automation for Servers, is that the bulk of the work, of defining the policy and remediations, is already done for an organization. The TrueSight Automation for Servers compliance engine allows organizations to quickly audit server compliance and show results, usually within the first hours of a POC, within the first week of a production implementation.

DISA compliance levels

There are three categories or levels of vulnerability that indicate the severity of the risk of failing to address a particular weakness.

Category I
Any vulnerability, the exploitation of which will, directly and immediately result in loss of Confidentiality, Availability or Integrity.

These risks are the most severe, and if an organization does not address them, they will not be granted an Authorization to Operate. The only exceptions to this are when the system is critical or when a failure to use the system could lead to a failed mission. These are vulnerabilities that may result in a loss of life, damage to facilities or a mission failure.

Category I weaknesses can allow unauthorized access to classified data or facilities, and they may also lead to a denial of service or access that could result in mission failure. Systems that have not been approved by an appropriate Designated Accrediting Authority or have not had the risk of their use deemed acceptable by the DAA also fall into this category.

Category II
Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality,

Availability, or Integrity.

An Authorization to Operate may still be granted with unaddressed Category II risks since they can normally be mitigated. Risks in this category can lead to a Category I vulnerability, result in personal injury or damage to equipment or facilities and degrade a mission. These risks can allow unauthorized access and may result in the loss of or compromise of sensitive information, data or materials. Category II weaknesses may also lead to system disruption and could extend the amount of time required to recover from a system malfunction.

Category III
Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity.

Category III risks are those that can be addressed to improve overall security, but they will not prevent an organization from being granted an Authorization to Operate. Risks of this type could lead to a Category II vulnerability or a delay in recovering from an outage, and they may also affect the accuracy of data and information. Category III vulnerabilities can allow the running of applications that aren't related to mission functions and may indicate a need for improved security administration.

In some cases, DISA will issue vulnerability classifications that are more specific, such as in the case of software development, which are listed below.

Category I
Vulnerabilities that allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.

Category II
Vulnerabilities that provide information that have a high potential of giving access to an intruder.

Category III
Vulnerabilities that provide information that potentially could lead to compromise.

However, the standards are fairly similar; Category I risks are the most severe, and Category II and III risks do not normally lead to the denial of an Authorization to Operate.

DISA compliance auditing

Compliance can be fairly difficult because organizations must ensure that they are following DISA prescriptions at all times. This can be a bit like attempting to hit a moving target because STIGs are added and updated as new technology is developed. Additionally, software and hardware upgrades and replacements can cause required settings to be changed or overwritten. As a result, staying compliant means that systems need to be monitored and adjustments must be made on a continuous basis.

The first part of the process of ensuring compliance is understanding which systems need to be configured to meet DISA regulation requirements along with which configurations or processes are mandatory. In STIGs, there are instructions where it is stated that an organization should do something, which means that taking this action would improve security but is not mandatory. However, when a statement says an organization will do a particular task, it is something that must be done. Following all configuration requirements of a STIG may prevent a system from operating correctly, so knowing what is mandatory is important.

It is also of note that some systems may have to be configured to comply with multiple STIGs if a system has multiple roles. Failing to meet DISA standards for any particular system can mean that access to the DoD is denied.

Once it's been established which systems need to be made compliant, STIGs need to be downloaded. From there, individuals can be assigned with the task of making configuration changes and, once this is done, following up regularly to ensure they are still correct. While this tedious and time consuming method was what had to be when DISA first launched this process, many automated tools have become available since, so numerous configurations and verifications no longer need to be done manually.

When the process first began, STIGs were PDF documents that detailed what configurations should be and how to apply them. This meant that checks had to be done by hand, so errors were common. To make the process faster and more accurate, Gold Disk (a scripted process), which scans an operating system or software suite to determine if configurations are correct, was created.

After the Security Content Automation Protocol, developed by the National Institute of Standards and Technology, was developed, it mostly supplanted Gold Disk. However, not all STIGs have a SCAP associated with them, so another type of scanning software has to be used, or the process has to be handled manually. New SCAPs are being created on a regular basis, so manual configuration and verification is slowly being replaced by automation. Solutions like TrueSight Automation for Servers that can readily consume, execute, and report on SCAP compliance can cut significantly the amount of effort required to measure DISA Regulatory & Security compliance.

When using SCAPs for different STIGs, organizations may need to get a DoD PKI Certificate for them to work properly if they were created by DISA. However, there are third party SCAPs that do not require the certificate and will still do scans and provide reporting data. It's important to note that as helpful as automatic scanners can be, they don't all catch everything. For example, the RHEL5 SCAP misses over 100 requirements associated with its STIG, so organizations need to find out what, if anything, a SCAP doesn't cover and check those things manually.