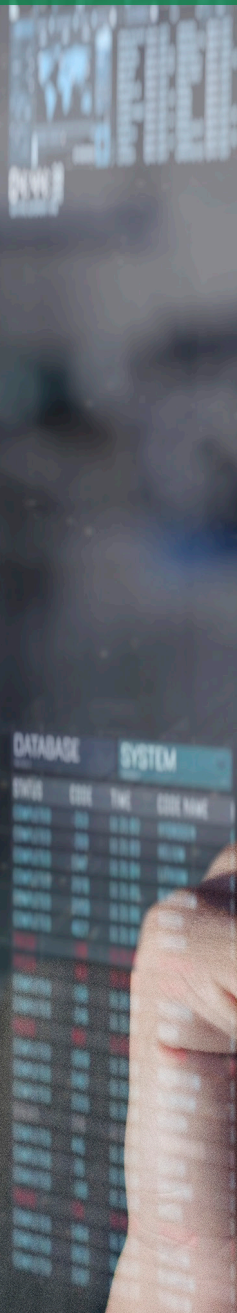
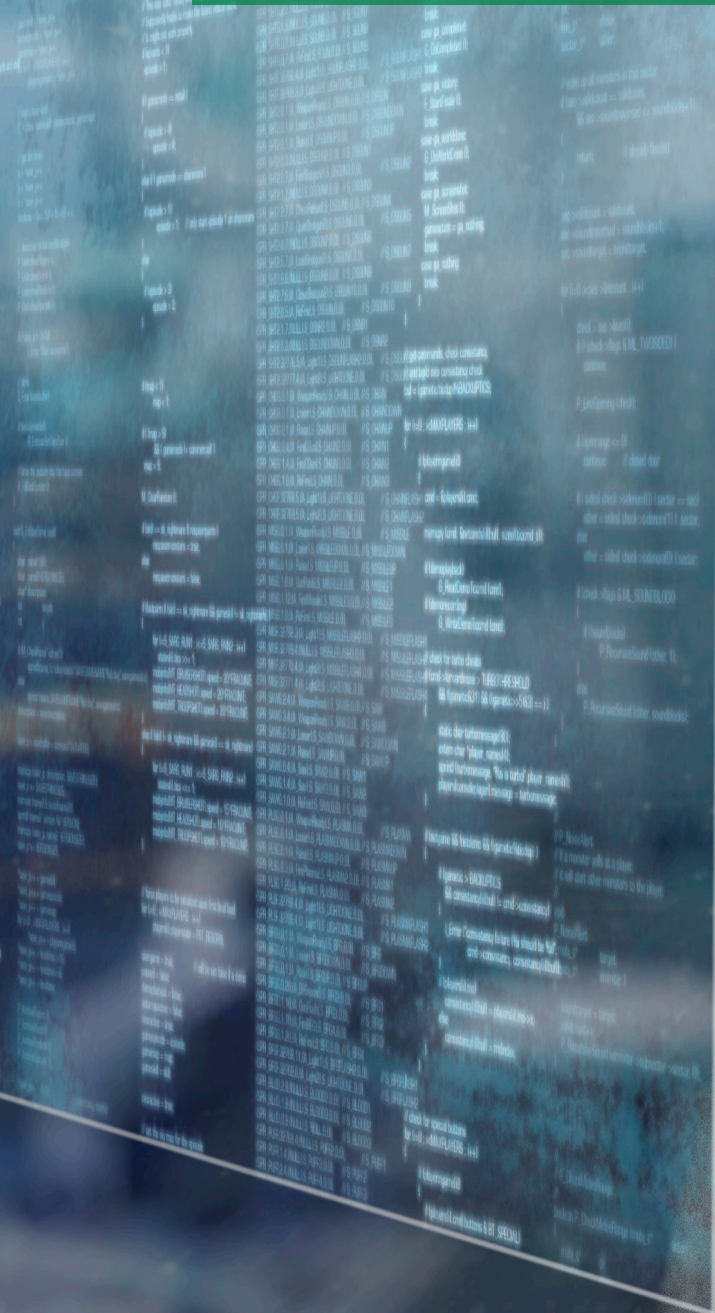



eBook

STIG 101

SteelCloud





Everything you've always wanted to know about STIGs but were afraid to ask.

As we speak, there are as many as 10,000 vulnerabilities in your system that, if not secured, could be a gateway to phishing, hacking or malware. This is why the [Defense Information Systems Agency \(DISA\)](#) created [Security Technical Implementation Guides \(STIGs\)](#). STIGs encompass a standardized and customizable set of rules for installing, supporting, running, and securing systems in the government against cyberattack.

[STIGs are critical](#) to protecting our most sensitive data. Throughout the DoD and other agencies—such as TSA and the DoJ—they are a mandated part of securing and maintaining systems and devices.

How did STIGs come about?

[STIGs are created and maintained by DISA](#), an agency of the DoD. A government study was conducted to determine whether government systems were being implemented securely and if there was consistency across agencies.

The result of the study was a recognized need to create rules, identify best practices and provide guidance around the technical aspects of organizing, delivering, and managing defense-related information. This encompasses not just rules around system implementation and maintenance, but also [the human behaviors that frequently result in breaches](#). Those rules, also known as controls, are what make up the Security Technical Implementation Guides that we call STIGs.

What all gets STIGged in a system?

As you can imagine, commercial applications are not created to align with internal DoD mandates. The operating systems, routers, printers, apps—the elements that make up modern systems—all need to go through the STIG process before they are secure enough to be used in government systems.

DISA lists over 10,000 controls that need to be STIGged to meet mandates. Then, 90 days later, you need to do it again when updates come out. Whether you are a small network managed by just one expert or a larger organization with a team of dozens, it is an overwhelming effort. There are not enough experts in the workforce to do the work easily and efficiently.

But STIGs are a vital factor in our nation's cybersecurity. And, mandated or not, government or not, organizations look to STIGs as the gold standard. This level of security is becoming more accessible – both inside the government and out – with the help of [automation solutions](#) that do the work in hours, not weeks or months.



Where do STIGS fit in the government cybersecurity process?

STIGs were developed by DISA with defense networks and components in mind. Not surprisingly, the DoD uses STIGs as their exclusive benchmarks. They are a key part of the [Risk Management Framework \(RMF\)](#), a standard developed by the [National Institute of Standards and Technology \(NIST\)](#) to identify, assess, mitigate, monitor and govern information systems.

Before an application, update, or network component can go live, it needs [Authority to Operate \(ATO\)](#). That means you've STIGged everything, remediated to government satisfaction, plugged all the holes, and have signoff to go live with all the work you've done. Now, the government [wants agencies to provide continuous ATO \(cATO\)](#) and [take an even more aggressive cybersecurity defense posture](#).

Can everyone use STIGs?

Within the more than 10,000 controls and endpoints that STIGs address, you'll find the same Windows vulnerabilities any network would have. The same router vulnerabilities. The same iPad vulnerabilities. The default settings for these technologies ensure they work as intended, but they leave vulnerabilities in their wake. These might be acceptable risks for commercial users, but in an organization, they put valuable data at risk. STIGs tell you where to look and where to harden within your system and applications to lower your attack surface and protect you from bad actors.

If you do business with the federal government, STIGs may be mandated. The RMF and ATO that STIGs support is vital to protecting the supply chain. So, it's no surprise that organizations outside the DoD—and even outside of government contracting—are adopting STIGs voluntarily as their benchmarks. They do the work and successfully prevent breaches. But there is another option that delivers similar results.

[The Center for Internet Security \(CIS\)](#) developed their own Benchmarks that are based on the same NIST standards as STIGs. They offer broader functionality that suits multiple industries. CIS Benchmark compliance is the North Star many organizations follow because, while different from STIGs, they are similar and take less effort to implement. Both [CIS Benchmarks](#) and [STIGs](#) are free and downloadable.

How often are STIGs updated?

DISA updates and releases new STIGs [quarterly](#), though there may be interim updates in response to emerging threats. Addressed manually, updates could take weeks to implement. And the new and updated software versions the updates reflect cannot be implemented until they have been STIGged and granted authority to operate. Therefore, the vulnerabilities these updates protect remain in your system until it has been STIGged. Thus, the speed at which you STIG your system and process these updates is a critical factor in its security.



Who in the organization implements STIGs?

This differs in every organization. System Administration people and Information Assurance professionals do most of the work, but in smaller organizations, it may be the person who implements your software.

The bigger question is “are they capable?” And, outside of the government who have cornered the market on expensive and in-short-supply STIG experts, the answer is “maybe”. [There is a serious lack of qualified professionals in the marketplace.](#) And, depending on the complexity of your network, it takes an entire team working all day, every day, year-round to complete.

What makes STIGs so hard to implement?

Beyond the 10,000 controls to review and repair, there is one frustrating truth that makes STIGs hard to implement—STIGs break things. Systems, apps, and devices that work perfectly well in an unsecured environment “break” when STIGs are applied.

There are two sides to this truth. Fixing things that STIGs broke makes the work of compliance more difficult. But you also know that, when things break, it’s because there is a vulnerability that can lead to a breach. And you’re finding that vulnerability before the bad guys have a chance to exploit it.

Why do things break?

From Windows operating systems to Symantic antiviral software, [the government largely uses commercial solutions.](#) But, because they are made for the masses, those applications and devices are not developed or tested in a STIG environment. So once an application environment is hardened or secured to STIG specifications, the application won’t run or install properly. In this way, it “breaks”. It doesn’t matter whether it’s new software or a legacy application, STIGs will break it.

Implementing STIGs requires you to change application controls or block capabilities the app needs in order to operate. There are no generic rules that can be applied across all applications all the time. So, system administrators and information assurance experts have to address these issues on a one-by-one, case-by-case basis.



How do you fix the breaks?

Breaking sounds like a bad thing, but it's not entirely. When apps break, you have an opportunity to make them stronger. Breakages are the proof that STIGs are finding vulnerabilities, and you need to create policies to address those vulnerabilities. After all, that is the point of cybersecurity.

But fixing these breaks takes time and expertise of which nobody has enough. That is why [compliance automation is making big news](#) in the industry. The right automation solution can [save 90% of the effort](#) it takes to scan and remediate STIG policy across a network—and by “remediate” we mean fix all those breaks. It can ease the strain of [today's cyber workforce challenges](#). And it can get new applications and updates online faster, ensuring you always have the best, most secure technology at hand.

Do STIGs have an impact on other cybersecurity practices?

STIGs provide good cyber hygiene and enable world-class cybersecurity in the organization. The security they establish and maintain is a foundation for building other cybersecurity practices upon. STIGs not only address creating a secure baseline, but they also address [ransomware threats](#) and [Zero Trust implementation](#), two of the hottest topics in cybersecurity today.

How do STIGs help with ransomware?

Ransomware is one of the most common and effective forms of malware attack. Bad actors enter the system through phishing or an infected server or site. Then they render your files unusable and demand a ransom to get them back. Ransomware attacks cost millions, damage your reputation, and erode trust.

Overall, STIGs support a healthy cyber regimen. And a healthy cyber regimen helps keep bad actors out and unable to attack the network. But more specifically, there are STIGs in place to address known ransomware attack vectors. For example:

- ✓ In Microsoft Office, STIGs prevent linking to other sites from within documents, as bad actors commonly embed malicious links in files.
- ✓ In operating systems, STIGs block malicious actors from entering by requiring complex logon requirements, limiting failed logon attempts, and enabling early warning of questionable activity on the network.
- ✓ With browsers, STIGs reduce the attack surface by preventing the running of mini Java applets or the download of cookies and software without authorization.

In essence, [STIG compliance reduces the avenues of attack within your system](#). When used in tandem with traditional approaches, such as password protection, it is extremely rare to suffer a major attack with a fully STIGged system.



Are STIGs and Zero Trust compatible?

In addition to STIGs, [Zero Trust](#) is another preventative measure government organizations implement to ward off bad actors. The DoD is already transitioning to Zero Trust cybersecurity frameworks and urges all its agencies and organizations to follow suit. As you might imagine, Zero Trust means that you trust nobody who enters your system.

With Zero Trust, authentication moves [from the perimeter to data-specific entryways](#). The five fundamental assertions of a Zero Trust network are:

- ✓The network is always assumed to be hostile.
- ✓There are external and internal threats on the network at all times.
- ✓Network locality is not sufficient enough for deciding trust in the network.
- ✓Every device, user, and network flow is authenticated and authorized.
- ✓Policies must be dynamic and calculated from multiple sources of data.

In other words, a Zero Trust approach assumes [every attempt to access the system is a breach](#). You only get to access the data and capabilities you need, authenticating again and again the deeper your access takes you. This contains the blast radius of malicious activity to just the part of your system that got breached. Having [a secure baseline that meets STIG standards](#) helps capture unauthorized access attempts and makes your network that much harder to attack.

How do organizations find the bandwidth to implement STIGs?

STIGs are a way of life in government agencies, as well as in many of the organizations that serve them. And because it's a way of life, you must find a way to make it livable. With over 10,000 system controls, unique policies for every solution and updates every 90 days, STIG compliance is becoming harder and harder to do by manual means alone.

With qualified professionals in extremely short supply, many organizations are looking to automation. [SteelCloud's patented ConfigOS](#) can reduce weeks and months of manual scanning and remediation work to just an hour. Which is what has made it the DoD's primary cybersecurity automation solution. With the help of proven automation solutions like ConfigOS, STIG (and CIS) compliance is within reach for even the smallest IT teams to achieve.

What else do I need to know about STIGs?

SteelCloud is an established authority on STIGs and cybersecurity automation. To learn more about STIGs, join one of our social channels, [visit our blog](#), or download our [free STIGs for Dummies eBook](#) that goes into even greater detail about STIGs. You can also [schedule a demo](#) and see how drastically automation simplifies cybersecurity.



About SteelCloud

SteelCloud's patented ConfigOS software is the industry leader for automating STIG, CIS and CMMC compliance, detecting vulnerabilities, and remediating issues. With ConfigOS, weeks of manual work is completed in about an hour. Better yet, maintaining secure baselines is effortless, providing a strong foundation for Zero Trust and other emerging cybersecurity initiatives in the government and DIB. SteelCloud makes hard things—and hardening things—simple. For more information call (703) 674-5500, email info@steelcloud.com or visit www.steelcloud.com.