SteelCloud

The Federal STIG Field Guide: Why Compliance Can't Wait

Keeping Compliance Moving When Government Pauses

Government disruptions don't erase risk. They don't eliminate threats, and they certainly don't pause the need for compliance. Whether operations are fully staffed or momentarily stalled, securing systems through STIGs remains mission-critical.

This guide is your plainspoken walkthrough of STIGs: why they exist, what they protect, and how automation is transforming the path forward for government and contractor teams, especially when uncertainty strikes.

What Are STIGs and Why Do They Matter?

Right now, your systems may have thousands of vulnerabilities—potential entry points for phishing, malware, or worse. That's why the Defense Information Systems Agency (DISA) created Security Technical Implementation Guides (STIGs). These are standardized, customizable rulesets that guide how government systems are installed, supported, and secured.

They're a mandatory part of protecting sensitive assets across the Department of Defense and the Defense Industrial Base (DIB). Whether it's normal operations or a shutdown scenario, these standards don't disappear.

How Did STIGs Come About?

A government study revealed inconsistent security practices and rising risk. In response, DISA developed a consistent set of technical controls designed to standardize how government systems are built and maintained. These controls cover both systems and the human behaviors that often expose them to compromise.

What Gets STIGged in a System?

Everything. Operating systems, applications, databases, routers, printers—any element of a modern environment that touches government data needs to be hardened. More than 10,000 controls may apply. And those controls evolve regularly. Even in times of disruption, updates continue, and new vulnerabilities are discovered.

Manual STIG efforts require an army of experts. But those experts are in short supply. That's why teams across the federal ecosystem are leaning into automation. What once took months now takes minutes.

Where Do STIGs Fit in the Cybersecurity Process?

Before systems go live, STIGs must help you:

- ✓ **Establish a secure baseline**
  Review and configure systems against more than 10,000 DISA controls to reduce risk.
- ✓ **Achieve Authority to Operate (ATO)**
  Validate that all required systems have been hardened, documented, and approved.
- ✓ **Ensure CSRMC/RMF alignment**
  STIGs support the Cybersecurity Risk Management Construct (CSRMC) which is set to replace the Risk Management Framework (RMF). This new construct will guide the assessment and security of federal systems.
- ✓ **Identify and remediate vulnerabilities**
  Locate weak points, implement fixes, and keep evidence ready for audit and compliance review.
- ✓ **Support continuous ATO (cATO)**
  More agencies now require systems to maintain secure configurations on an ongoing basis — not just at deployment.
- ✓ **Enable Zero Trust strategies**
  STIGs help restrict access and create segmentation, enabling a more resilient cybersecurity architecture.

These requirements don't disappear with federal funding delays or furloughs. They persist.

Can Organizations Outside of Government Use STIGs?

Absolutely. Commercial systems have the same vulnerabilities as government ones. While some may accept those risks, organizations with high-value data are adopting STIGs and CIS Benchmarks to raise their baseline and protect against advanced threats.

STIGs are free to use. So are CIS Benchmarks. The difference is in their structure and depth. Many industries now turn to CIS for broader applicability, but STIGs remain the gold standard where the mission requires precision.

How Often Are STIGs Updated?

Quarterly. Every new version of software must be hardened before it can be safely used in a government setting. If you don't keep up, you don't stay secure.

A shutdown may slow business processes, but attackers don't take breaks. If you fall behind, your risk grows. Automation is the only way to keep pace consistently, especially when operations are understaffed or delayed.

Who Implements STIGs?

In larger organizations, it's typically your System Admin or Information Assurance team. In smaller ones, it may fall to a single IT lead. In either case, STIGs require deep technical knowledge and constant time investment.

When those resources are limited—because of budget cuts, staff furloughs, or an agency-wide pause—compliance doesn't wait. That's where automation becomes essential.

Why Are STIGs So Hard to Implement?

STIGs break things. That's part of the process. They identify insecure configurations, and those configurations often conflict with how an application runs. Fixing the breaks means hardening your environment; but also introduces risk of downtime, user disruption, or instability if not done carefully.

These aren't one-size-fits-all rules. Every break must be reviewed, resolved, and documented. That's why STIG work takes so long and why teams fall behind without help.

How Do You Fix Those Breaks Without Slowing Down?

STIG automation platforms like SteelCloud's ConfigOS are purpose-built to solve this challenge. They scan for gaps, fix what's broken, and maintain documentation for audit readiness, all in minutes, not weeks.

Automated remediation ensures systems stay in compliance even when your team is limited, out-of-office, or focused on more urgent priorities.

How Do STIGs Strengthen Other Security Practices?

STIGs create a hardened baseline that supports other initiatives like ransomware defense and Zero Trust.

Against ransomware, STIGs block dangerous macros, limit exposure to phishing links, and reduce opportunities for lateral movement once inside the network.

For Zero Trust, STIGs provide the secure baseline that enables granular access control, segmentation, and validation across every layer of your system.

How Can You Possibly Keep Up—Especially Now?

STIGs are complex and constant. You can't pause them when budgets freeze or wait for full staffing to return. Whether it's normal operations or a government shutdown, systems must be secured.

That's why so many agencies have turned to automation. SteelCloud's patented ConfigOS solution compresses what used to take weeks into an hour. It's how organizations are staying compliant, audit-ready, and mission-focused even when everything else is on hold.

Ready to Simplify COMPLIANCE?

We built ConfigOS to help federal teams overcome complexity. If you're facing delayed projects, limited staff, or increasing pressure to stay secure, SteelCloud can help.

- ✓ See how we automate and remediate STIG and CIS Benchmarks policy implementations
- ✓ Learn how we reduce risk across disconnected and classified networks
- ✓ Schedule a demo to see ConfigOS in action

Compliance doesn't stop—and with SteelCloud, neither do you.

SteelCloud
20110 Ashbrook Place, Suite 200 | Ashburn, VA 20147
1.703.674.5500 | info@steelcloud.com | **steelcloud.com**