



# Encyclopedia of Security

**TECHNICAL GUIDES AND STANDARDS HELP AGENCIES PROTECT DEFENSE NETWORKS, AND COMPANIES ARE EAGER TO ASSIST WITH COMPLIANCE.**

**By PETER BUXBAUM  
MIT CORRESPONDENT  
BUXBAUM@KMIMEDIAGROUP.COM**

In the ongoing battle to protect Department of Defense networks, one of the bulwarks is a set of security standards and guidance documents that collectively could be called an “encyclopedia of security”—the Security Technical Implementation Guides (STIGs) developed by the Defense Information Systems Agency (DISA).

In a nutshell, DISA STIGs are the configuration standards for hardening DoD information systems and devices. There are STIGs on dozens of information system and networking components and on thousands of vulnerabilities, covering topics from application security, biometrics, databases and desktop applications to enterprise resource planning, instant messaging, network infrastructure, operating systems and wireless communications.

Complying and tracking compliance with STIGs can be a daunting task for defense organizations, however. In response, a number of companies have stepped forward to offer products and services that can help agencies stay on top of these demanding but essential tasks.

The STIGs are released under the authority of DoD Directive 8500.1, which requires that “all information assurance and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD approved security configuration guidelines.” The directive tasks DISA to “develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with the director of National Security Agency.”

“The DISA STIGs are key to establish-

ing a repeatable secure baseline for defense and industry computing devices and applications,” said Colin Corlett, president of Excentium, which provides information assurance management services. “Initially, STIGs were available only for standard operating systems and databases. Recently DISA has focused its attention on developing standard guidance to establish baseline security for applications.”

“STIGs reflect DISA’s desire to provide prescriptive guidance on how to use common COTS software and configure it to remove the default settings and move to a higher level of security,” said Sean Sherman, a senior compliance architect at Tripwire, which provides configuration control services. “The STIGs provide the nuts and bolts on how to check configuration settings. DoD has so many systems in the field, and their users need consistent security advice.”

The STIGs are increasingly seen as the gold standard for information system security and have been gaining momentum outside of DoD, both in the private and public sectors. “Organizations trying to get government contracts often need to comply with the STIGs just to get a foot in the door of federal agencies,” said Tom Bain, manager for marketing and corporate communications at Application Security, a provider of database security solutions.

State government agencies are also starting to get into the act. “The state of Alabama uses a number of DISA STIGs as the basis for their own statewide IT security policies and standards,” said Tony Pompliano, chief executive officer of Refense Technologies, a provider of vulnerability and compliance management solutions. “We expect this trend to continue

throughout government and private enterprise.”

DISA has found the STIGs to have been well accepted. “For the most part, the feedback has been very good,” said Terry Sherald, chief of the agency’s information assurance standards branch. “Systems administrators like the STIGs, they want to use them, and they see their value. When we are developing or updating a STIG, we allow the community to comment after we have written a draft.”

“There is a need being satisfied here,” added William Keely, DISA director of field security operations. “The STIGs give systems administrators some level of assurance that they are doing the right thing even if they do not always agree with the STIG in every detail.”

## **BEYOND MANUAL**

Not surprisingly, the process of evaluating operating systems, databases, Web servers and applications can become unwieldy with manual methods alone. “Although manual methods are still key to a complete security evaluation,” said Corlett, “automated tools have become necessary in today’s world of fast-paced and agile development.”

There are a number of tools available on the market today that automate what was traditionally a manual auditing process to verify compliance with various STIG and other standards. “When an engineer is tasked with verifying that a network device is properly configured according to a security standard, he has to manually log in to that device and look at the configuration field to confirm that it is configured in the way the STIG requires,” explained

Pompliano. “That manual process can take a well-skilled engineer an hour or two per device. Not only is this labor intensive, but it is also difficult to achieve a high degree of accuracy because people doing the audits are the same people who configured the device to begin with.”

One of the products Excentium uses to evaluate the security baseline and STIG compliance of database applications is Application Security’s AppDetective product. “The product incorporates the configuration requirements identified in the database STIG,” said Corlett. “By using this product we have been able to reduce the evaluation time from a minimum of one day to a couple of hours.”

DISA’s database STIG requires an in-depth review of users, roles and privilege assignments, and mandates a process to approve those privileges. Application Security helps organizations comply with the database STIG and the specific requirements provided for Microsoft SQL Server, Oracle and IBM DB2.

“Manually assessing the security posture of a database is a complex task that requires expertise and significant resources,” said Josh Shaul, the company’s vice president for product management. “Manually measuring and demonstrating compliance with industry and government regulations is even more difficult.”

The Application Security product works “by scanning the target database for vulnerabilities and misconfigurations, and then providing reports on the findings,” explained Shaul. “AppDetectivePro contains scan policies, or templates, specifically for the DISA STIG. The findings generated from the scan are presented in a format that makes it easy for organizations to assert compliance with the STIG.”

The operating system STIG sets requirements for such things as access control, file permission, user accounts, and session management. Trusted Computer Solutions provides software that assess compliance with the STIG and provides fixes for operating systems such as Linux, UNIX and Solaris.

“Operating systems like Linux and UNIX have evolved tremendously in the last 30 years to include a myriad of configuration fields,” said Jamie Adams, a senior secure systems engineer at Trusted Computer Solutions.

“There are 340 line items in the UNIX STIG alone,” added Sherryll Dorch, vice president of marketing at Trusted Computer. “The default settings for Red Hat Linux 5.2 shows 54 discrepancy indicators with respect to the STIG, many of them significant. It would take a system administrator a lot of time to get in there and maintain the level of security required by the STIG.”



Sean Sherman

[ssherman@tripwire.com](mailto:ssherman@tripwire.com)



Tom Bain

[tbain@appsecinc.com](mailto:tbain@appsecinc.com)



William Keely

[william.keely@disa.mil](mailto:william.keely@disa.mil)

“The STIG and checklist don’t always tell you how to configure the system in compliance with the STIG,” said Adams, “so you then have to dig into research to find out how to do that.” Trusted Computer’s Security Blanket product automates both the compliance assessment and the proper configuration of the system.

The network infrastructure STIG is designed to assist in meeting the minimum requirements, standards, controls and options that must be in place for secure network operations. The document includes sections providing the minimum requirements for enclave perimeters, firewalls, routers, device management, authentication, authorization and accounting, passwords, network intrusion detection, switches and virtual local area networks.

Tripwire’s network infrastructure product works by installing a software agent on each device, rather than on switchers and routers, explained Sherman. “The software makes sure that the STIG requirements are complied with,” he said, “such as making sure that passwords are of the required length and that users are locked out after entering three incorrect passwords.” Switchers and routers are monitored by the Tripwire product from servers.

Running Tripwire first generates a report on changes on the system. It checks configurations of devices against the relevant DISA STIG checklist and generates a report showing “whether you are compliant with the STIG or how far off you are from compliance,” said Sherman.

“DISA STIGs, along with VMware virtualization, are helping to provide a reliable and predictable set of processes and tools to efficiently



ForeScout

Do you have the IA capability to control network access?

## CounterACT

Army-approved solution for port-based Network Access Control

Learn more:  
[www.forescout.com/DoD](http://www.forescout.com/DoD)

and effectively manage DoD IT environments,” said David Hunter, chief technology officer for VMware Public Sector. “Starting with virtual machine images whose base operating systems and applications have been configured and validated to STIG requirements, administrators can simply deploy new VMs as required, using a standard master image.

“VMware enables these master images to be modified as STIG requirements change, and then transparently deployed to end-users. Inventory management control and deployment applications such as vCenter Lab Manager and Stage Manager environments can keep track of which VMs are deployed where and to which STIG version they comply. This can easily be done by using standards such as the DMTF’s Open Virtualization Format to ensure compatibility across multiple virtualized environments,” Hunter added.

## VULNERABILITY MANAGEMENT

The Refense VMS (vulnerability management solution) also assists in complying with the DISA network infrastructure STIG by comparing the configuration of network devices against the security policies detailed in the STIG and isolating misconfigurations and known vulnerabilities.

“Refense VMS mimics the tasks performed by an information assurance officer,” said Pompliano. “The solution includes a level of intelligence that is basically akin to human auditors. The process takes a few seconds for each device instead of an hour or two if done manually.”

For example, Refense audits compliance against STIG requirements for routers. “The DISA STIG requires complex checking that if done manually would take some time and would be prone to high error rates,” said Pompliano.

One STIG specification for routers requires that the router administrator restrict the premise router—the router connected to the upstream network provider—from accepting any inbound IP packets having a source field from BOGON or Martian IP addresses. “These BOGON and Martian lists are maintained to track unallocated or reserved IP address space,” explained Pompliano. “Router administrators would have to check this list and compare the IP address space with their access control lists on their premise routers to ensure that the access control lists match the current list.”

Another router requirement is for information assurance officers to ensure that denied attempts to any port, protocol or service is logged. “This would require that the information assurance officer or network administrator check every line of every access control list to ensure that logging is enabled for that entry,” said Pompliano. “If the devices have hundreds or even thousands of entries on the access control list, this can take some time to complete.”

In addition, Refense can also analyze firewall rules to ensure a particular rule is in place to block an IP range that is prohibited access to DoD computers and systems. “There are multiple STIG requirements that network managers restrict RFC 1918 IP addresses on the network,” said Pompliano. “An engineer would need to review all firewall rules and access control lists to ensure that statements are present that block these IP addresses.”

RFC 1918 IP addresses are those that have been designated for private use.

In addition to these STIG-compliance activities, Refense can also scan networks for newly announced vulnerabilities. “With each of these examples, Refense not only completes the audit task much more quickly than a human could, but also does so with greater accuracy,” said Pompliano. “In large organizations such as military branches that have tens of thousands of network devices deployed, searching out these vulnerabilities and ascertaining configuration postures would otherwise be akin to looking for a needle in a haystack.”

## MOBILE GUIDES

DISA’s STIG for Windows Mobile Messaging, which provides guidelines for DoD for the installation, configuration and operation of non-BlackBerry mobile e-mail systems, was recently updated to include device support for Microsoft Windows Mobile 6.0. Requirements in the STIG include standards for Bluetooth security, authenticated login procedures, and standards for required actions in case of the loss of the device.

Trust Digital, a company that provides mobile phone security products and services, has developed mobility management software specified for compliance with the wireless STIG. In addition, Trust Digital’s Bluetooth smart card reader, which enables access to mobile devices using the DoD common access card, was also recently certified

for two-factor authentication.

Developing a STIG for Windows-based smartphones allowed DoD a secure alternative to the formerly exclusive use of BlackBerry devices within the department for mobile e-mail and messaging applications, according to David Goldschlag, Trust Digital’s executive vice president for corporate strategy and technology.

“What DoD needed was a system that would provide enterprise control and visibility,” Goldschlag said. “Because there is no third-party network operations center,” as is the case with BlackBerry messaging, “and messages stay within a native network operations center, classified message incidents are mitigated, giving DoD and other federal agencies tighter control of information, as well as enhanced auditing capabilities.”

The STIG for mobile devices provided guidance on how to deploy and use mobile Windows devices. “What the STIG did is to provide a blueprint for DoD buyers. It goes to a level of detail on what implementation of smartphones looks like and how they are to be configured,” said Goldschlag.

Among other things, the STIG requires that only phones with up-to-date software and operated by the authorized individual be allowed access to the network. It also provides standards for synchronizing the e-mail available on smartphones with the command’s Exchange e-mail server. “One of the required components is the Trust Digital mobile security management system,” said Goldschlag.

The tools used to help organizations comply with the STIGs are designed to evaluate compliance and diagnose problems, but not to fix them with the application of software. DISA does issue software fixes aimed to do just that. Tripwire’s Sherman cautions against jumping to actually running those scripts, however.

“The DISA utilities can be used to harden a server for you,” he said,



Tony Pompliano

[apompliano@retense.com](mailto:apompliano@retense.com)



Josh Shaul

“but in the real world the STIG is a baseline prescriptive standard.”

The reality of information systems is that they are complex, and configuring a server by running a DISA script could have unintended consequences. “It is possible to configure an operating system so that applications won’t run,” said Sherman. “If you blankly apply the scripts as produced by DISA you might find yourself in an uncomfortable position. Our product goes in and checks server systems to see if it matches what the DISA checklists prescribe. That is where our product makes its play.”

Trusted Computer Solutions takes a different approach, by also providing the fix to the operating system configuration problems it covers. “From feedback from customers, we understand that they want to know exactly what we are fixing,” said Adams. “Our product provides them with that information.”

But Adams agreed with Sherman that the impact of the STIG fixes on applications is unknown, until they are actually tested. That is why the Trusted Computer product comes equipped with an “undo” function that restores all the configuration fields and values to where they were before. “If you can’t get your applications to work with the STIG configurations, you have to apply for a waiver,” Adams noted.

From DISA’s perspective, the STIGs have made their marks and will continue to do so. “They have become the foundation to a lot of security processes within DoD,” said Keely. “They are foundational to our operations, and their importance continues to increase.”



David Goldschlag

[dgoldschlag@trustdigital.com](mailto:dgoldschlag@trustdigital.com)

The only current tools that DoD and DISA develop to automate the remediation of vulnerabilities are the Gold Disk and SCRI. In both cases there is published guidance encouraging the users to validate remediations in a lab environment prior to applying fixes to production systems.

## ACCESS CONTROL

The STIG addressing network access control (NAC) provides processes for identifying, authenticating and authorizing access to protected assets and presents a methodology for selecting and integrating access control solutions. The key feature of the NAC STIG is a multilayer approach that places great emphasis on controlling traffic at switch ports internal to the network rather than on perimeter control.

ForeScout Technologies offers a product called CounterACT CT-1000 to address the requirements for port-based access control outlined in this STIG. CounterACT is the only approved network access

control solution on the U.S. Army Information Assurance Approved Products List.

CounterACT is a switch-agnostic network appliance that provides real-time visibility and control over port-based access requests. It addresses the key criteria of the STIG, verifying that both the computer and the user have authorized access and that the computer configuration is compliant with security standards.

“When a device connects to the network, CounterACT will see and identify the device and the user,” explained Don Byrne, ForeScout’s federal director. “It will determine if the device is properly patched, whether its anti-virus is up to date and whether it is otherwise compliant with requirements.”

If CounterACT identifies a problem with a device, the system administrator can take appropriate action: update the anti-virus software, integrate with a patch management solution, or issue a command to shut down the switch port to prevent an unauthorized access to the network.

CounterACT works whether or not a network has implemented Protocol 802.1x, a network access standard promulgated by the IEEE. Few DoD systems have implemented this protocol, Byrne noted, although other network access solutions require 802.1x compliance in order to work.

“The requirement that the DISA STIG identifies is basically two-fold,” added Steve Cooper, a former chief information officer of the Department of Homeland Security who is currently a partner and founding member of Strativest. “First it says, ‘Network ports should be both physically and logically secured to prevent unauthorized access to the DoD enclave.’ It goes on to say, ‘Both unclassified and classified networks require the implementation of a logical network port security solution.’”

“Basically the requirement says device access must be controlled at the switch port. Not all NAC solutions are alike, so you need to be sure that if you are implementing an NAC solution, it meets this fundamental requirement outlined in the STIG,” Cooper said. ★

## STIGs for the Future

What kinds of Security Technical Implementation Guides (STIGs) are we likely to see in the future? As technology continues to develop, the Defense Information Systems Agency (DISA) plans on issuing STIGs to cover them.

Virtualization of everything from data centers to operations centers to applications will require the development of a new STIG to cover those, according to Dave Hoon, a contractor supporting the DISA IA standards branch for EDS, an HP company.

A STIG covering virtualization, streaming technologies and cloud computing will likely be “the thrust of DISA’s efforts in 2010 and 2011,” he said.

“We also need to look at platforms that provide applications as a service,” he added. “As data is increasingly stored in virtualized environments, we need to develop requirements for the separation, storage and transport of data as well as for access controls. We need to make sure that the commercial entities providing these services meet the same requirements as DoD in their own environments.”

Many of these requirements are already addressed in existing STIGs, such as the one addressing network infrastructure, but, as William Keely, DISA’s director of field security operations, noted, the increasing utilization and complexity of virtualized environments makes it necessary to refine the requirements and bring them together in a single document.

Contact Editor Harrison Donnelly at

[harrisond@kmediagroup.com](mailto:harrisond@kmediagroup.com). For more information related to this subject, search our archives at [www.MIT-kmi.com](http://www.MIT-kmi.com).