



# Cybersecurity

Full strategic report at:

[www.FCW.com/Cybersecurity2010](http://www.FCW.com/Cybersecurity2010)



## **Inside:**

Modernizing Cybersecurity to Better Manage Risks, s2

Catalyst for Transformation: The U.S. State Department, s4

FISMA Update: Tracking the Renovation, s5

In Terms of Human Capital, A Cybersecurity Crisis Looms, s7

Advice for Government Organizations Implementing Continuous Monitoring, s8

# A Work in Progress: Modernizing Cybersecurity to Better Manage Risks

The sheer complexity of federal IT systems and networks, along with a shortage of skilled technical talent, a lack of coordinated leadership and legislation have all contributed to creating complex and perilous federal cybersecurity challenges.

As that complexity has grown, so to have the risks to securing vital resources and information. Threats now range from misguided employees to sophisticated attacks led by governments, terrorists and organized crime, each putting federal IT organizations into the bull's eye.

This is largely why the current federal IT cybersecurity landscape is under renovation to streamline cumbersome, costly security operations and help senior federal officials gain greater visibility, along with more precise information that will be used to improve risk-based decision-making. Industry observers maintain the complexities involved are often oversimplified. And because computing has been so individualistic for so long, the discipline required to control access to information and resources simply hasn't been fully implemented.

But that's all changing. There are multiple 'tools' now being used for the first time to help renovate federal cybersecurity. A greater use of automation, continuous monitoring, a lockdown of configurations and an intensified focus on finding and educating skilled technical talent, as well as building security into products 'from the start,' are all important elements that are beginning to take hold.

To improve risk management and security in federal enterprises, both the Consensus Audit Guidelines (CAG) and the Security Content Automation Protocol (SCAP), are considered critically important. "SCAP in particular, is now being 'baked' into new products and operating systems such as Windows 7, to automatically scan for vulnerabilities," said Alan Paller, director of research for the SANS Institute.

Meanwhile, the appointment of Howard Schmidt, to Cybersecurity Coordinator, will provide White House leadership to federal cybersecurity efforts, working in partnership with the Office Management and Budget and the Office of Science and Technology Policy to update cybersecurity measures across government and ensure security protections are made a central component of operational policies.

And additional new initiatives, such as the National Strategy for Trusted Identities in Cyberspace (NSTIC), are

being rolled out nearly each week. NSTIC is a plan for secure, voluntary, privacy-enhancing credentials that the public can choose to use to securely authenticate their identities in cyberspace. Simultaneously, the National Cyber Incident Response Plan, which is currently under development by the Department of Homeland Security (DHS), will be exercised as part of Cyber Storm 3 in September to ensure

---

*"Cyberspace touches nearly every part of our daily lives. It's the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses, and the massive grids that power our nation. It's the classified military and intelligence networks that keep us safe, and the World Wide Web that has made us more interconnected than at any time in human history. We must secure our cyberspace to ensure that we can continue to grow the nation's economy and protect our way of life."*

*— President Obama,*

*from the White House Cybersecurity web site.*

---

there will be a coordinated national response to significant cyber incidents. Simultaneously, new performance metrics for the Federal Information Management Security Act (FISMA) will help move federal agencies from static, paper-based reports to more efficient and effective continuous monitoring.

And a newly combined legislative effort, The Protecting Cyberspace as a National Asset Act of 2010, sponsored by Senators Tom Carper (D-DE), the chairman of the Federal Financial Management Subcommittee, Joe Lieberman

(ID-CT), the chairman of the Homeland Security and Governmental Affairs Committee and Susan Collins (R-ME), the ranking member of the same committee, seeks to modernize, strengthen and coordinate the security of federal civilian and select private sector critical infrastructure cyber networks.

The current presidential administration is also highly focused on building collaboration to address cybersecurity challenges. “We’re going to need all of you to keep coming together – government, industry, academia, think tanks, media and privacy and civil liberties groups – to work together, to develop the solutions we need to keep America safe and prosperous in cyberspace,” said President Obama in a May address on the progress of recent cybersecurity initiatives.

Another big change taking place is a sharp drop in demand for security personnel without strong technical skills. “There were more than 700 federal jobs listed in January for certification and accreditation personnel [contractor jobs, largely responsible for writing FISMA compliance reports, for example]. There are well under 150 such jobs posted now,” Paller said.

The reason? What federal agencies need now are personnel and tools to help them gain better forensics, log monitoring and deep packet analysis to better understand exploits, along with secure coding and better risk/security management, Paller explained. “Unless you can perform actual cybersecurity forensics, analysis, and/or secure coding, those formerly important report-writing skills are no longer required,” Paller said.

A newly published report from the Center for Strategic and International Studies (CSIS) further underscores the cyber-skills challenge, underscoring a dire lack of technical cybersecurity skills available and offering suggestions to help grow training in the U.S. (See related article in this Snapshot report.)

At the same time, federal security regulation is also under renovation. FISMA has been widely criticized as an unnecessary paper chase. But it’s quickly being revamped to improve agency protections by tying compliance to actual security protection measures. (See separate article on FISMA in this Snapshot report.) “By using automated tools and advanced analytics to more closely align both compliance and security, government organizations will address gaps and focus valuable resources on high-value projects that meet both compliance requirements and provide a significant reduction in security risk,” Paller said.

Despite the many changes and initiatives currently under way to streamline cybersecurity, some industry observers maintain that the situation has morphed into too many initiatives, with none being adequately completed. “In our

surveys, we continue to find that agency executives express a sense of being overwhelmed, unsure about what to do, so personnel are ‘staying the course’ for now,” said Deniece Peterson, manager of industry analysis for INPUT, although this situation varies by agency. “There are pockets of progress and delayed or slow acceptance among others,” she explained.

The problem may simply boil down to a lack of change management. “As the personnel and governance have been quickly put in place, additional stakeholder buy-in may now require additional effort,” she explained.

While the lack of federal leadership and/or coordination was addressed earlier this year by the appointment of Howard Schmidt, other decisions, such as putting DHS in charge of enforcing compliance to FISMA has received mixed reviews as a step toward improving coordination among federal agencies. Administration officials maintain new guidance from NIST and other federal oversight organizations emphasizing risk management and real-time monitoring will assist federal agencies in implementing the measures needed to improve security protections. In its evolving role as guidance provider, NIST is also undergoing change. Sen. Barbara Mikulski (D-Md.) is seeking \$10 million in funding to establish a national cybersecurity center of excellence to help accelerate training and education.

For now, the administration’s focus on federal cybersecurity renovation continues at a breakneck pace, determined to leverage automation, enhance legislation and incorporate continuous monitoring, as well as trying to set up better information-sharing and a more rapid evolution of guidance. Much of the current changes taking place now can be traced to the State Department’s success in automating monitoring, adding new tools, figuring out how to score risks, and interacting with personnel and other organizations to work through cultural and change management issues. “Where in previous years, most federal defense and intelligence agency officials were unconvinced by the State Department’s efforts, in the last several months, ‘it has become clear everyone now supports and is advancing the State Department’s work to improve cybersecurity,’” Paller said.

Ultimately, while challenges (particularly those related to change management) remain, and new cybersecurity threats continue to emerge daily, it’s becoming increasingly clear that by implementing CAG controls, increasing automation and continuously monitoring networks, federal IT organizations can make enormous strides toward achieving greater protection against a wide range of cybersecurity threats. ■

# Catalyst for Cybersecurity Transformation: The U.S. State Department

In the two years since the U.S. State Department deployed a digital security dashboard to monitor a key unclassified network of 5,000 routers and 40,000 host computers that support 285 foreign posts, automated data collection has enabled the department to implement risk-based scoring, reducing risk on the network by 93 percent.

The State Department now scans its worldwide network at least every 36 hours to identify vulnerabilities. Via continuous monitoring, risk is assessed 100-300 times more frequently than with traditional FISMA methods. Throughout the State Department, John Streufert, Chief Information Security Officer and Deputy CIO for Information Security said in an interview that the goal now is to implement as many as possible of the 20 Most Critical Controls set by the Consensus Audit Guidelines (CAG).

The Department's Risk Scoring Program, for example, leverages best practices from the CAG, which are mapped against the way the department is attacked. The tools perform functions that include:

- Confirming what's connected to department networks;
- Assuring that computers, network and software are in the safest configuration setting;
- Locating system vulnerabilities that need correction; and
- Collecting evidence for cybersecurity investigations.

In July, the State Department also signed contracts to integrate Boundary Defense (from CAG #5) and some initial asset management data (from CAG #1, 2) into the daily recalculation of risk on its security dashboard. In each of these cases, Streufert explained, "the goal is to take information already available for review from the output of specific tools, and instead place those results into a security data warehouse, from which, across our enterprise the worst problems can be called out for attention and fixed first each day."

## A Little History

In 2008, the State Department decided its aging compliance requirements based on manual processes and annual compliance checks didn't meet its need to securely implement

web-based technologies and services. Instead, the organization launched a pilot test to see if automation and monitoring would make a difference. Now, "every day is really regarded to be a pilot proof of concept for continuous monitoring," Streufert explained.

In fiscal 2009, the State Department began supplementing FISMA compliance reports with a Risk Scoring Program that scanned every computer and server connected to its network not less than every 36 hours, on eight security factors, and twice a month for safe configurations of software.

In a typical week, the State Department blocks 3.5 million spam e-mails, intercepts 4,500 viruses and detects over a million external probes to its primary non-classified network. Since 2008, the number of security related tickets more than doubled, while malicious code attacks increased by 47 percent. And the volatility of changes to security sensitive settings has also been problematic. Cyber attacks are evolving faster than they can be counteracted. And penetration tests showed 80% of the successful attacks used known vulnerabilities.

The new monitoring methods have allowed a critical piece of the State Department's information security program to move from a snapshot in time previously available under FISMA, to a program that continuously scans for weaknesses on servers and PCs, identifies weak configurations every 15 days, recalculates the most important problems daily to fix in priority order, and issues letter grades (A+ to F) monthly to senior managers tracking progress within their organizations.

As for costs associated with the compliance program, Streufert said most can be covered by redirecting resources that would have been spent on one-time compliance testing efforts. There have even been a few cost reductions achieved. For example compliance and audit costs were lowered by 62%.

With pilot testing completed, the State Department is in the process of fully automating security monitoring now and is adding new data to its dashboard, to help others within the State Department to purchase the tools, using financing previously required for paper-based FISMA compliance reports. ▀

# FISMA Update: Tracking the Renovation

The ongoing upheaval in federal cybersecurity, especially the Federal Information Security Management Act (FISMA), has led to a shift in oversight management, designed to help clarify key roles and avoid confusion.

In a July 6 memo from the Office of Management and Budget (OMB) and White House Cybersecurity Coordinator Howard Schmidt, the Department of Homeland Security (DHS) will take primary responsibility in the executive branch for operational aspects of security in civilian agency federal systems covered by FISMA. OMB, meanwhile will be responsible for reporting to Congress on FISMA each year, for developing and approving cybersecurity portions of the budget and for coordinating with the cybersecurity coordinator on all related policy issues. Meanwhile, the cybersecurity coordinator will have visibility into DHS programs to ensure FISMA compliance and will be the primary White House official to coordinate interagency cooperation with DHS cybersecurity programs, according to the joint memo.

In all, DHS will now be responsible for:

- Overseeing government-wide and agency reporting on cybersecurity policies and guidance;
- Assisting government-wide and agency efforts to provide adequate, risk-based and cost-effective cybersecurity;
- Overseeing agencies' compliance with FISMA and to help OMB develop the FISMA annual report;
- Annual reviews of agencies' cybersecurity programs;
- Overseeing agencies' cybersecurity operations and incident response, as well as helping with appropriate assistance.

This new area of responsibility for DHS will be built into a robust program within the coming year. DHS and White House officials have publicly stated that putting DHS in charge of federal agency compliance furthers the administration's overarching effort to move away from FISMA's previous annual paper-based exercise, certification and 'check box compliance' to operational monitoring and making sure each agency is accurately measuring the actual state of security on a continuing basis.

And while DHS will handle compliance enforcement, the National Institute of Standards and Technology (NIST) will continue providing guidance to help agencies move forward. NIST recently rolled out SP 800-53A, Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations. This latest guidance is aimed at helping agencies implement continuous monitoring of IT systems under new compliance rules for FISMA. NIST also released a separate guidance document in June that provides

answers to frequently asked questions about continuous monitoring for federal IT executives. Continuous monitoring is part of a broader push from the current administration to improve risk management in federal agencies. New guidance to be released in NIST SP 800-137 this summer, will focus on NIST's broader approach for implementing network security configurations and controls using risk-based management principles.

NIST also plans to continually post new guidance and other updates on FISMA to its FISMA Implementation Project website, at: <http://csrc.nist.gov/groups/SMA/fisma/index.html>.

## A Little History

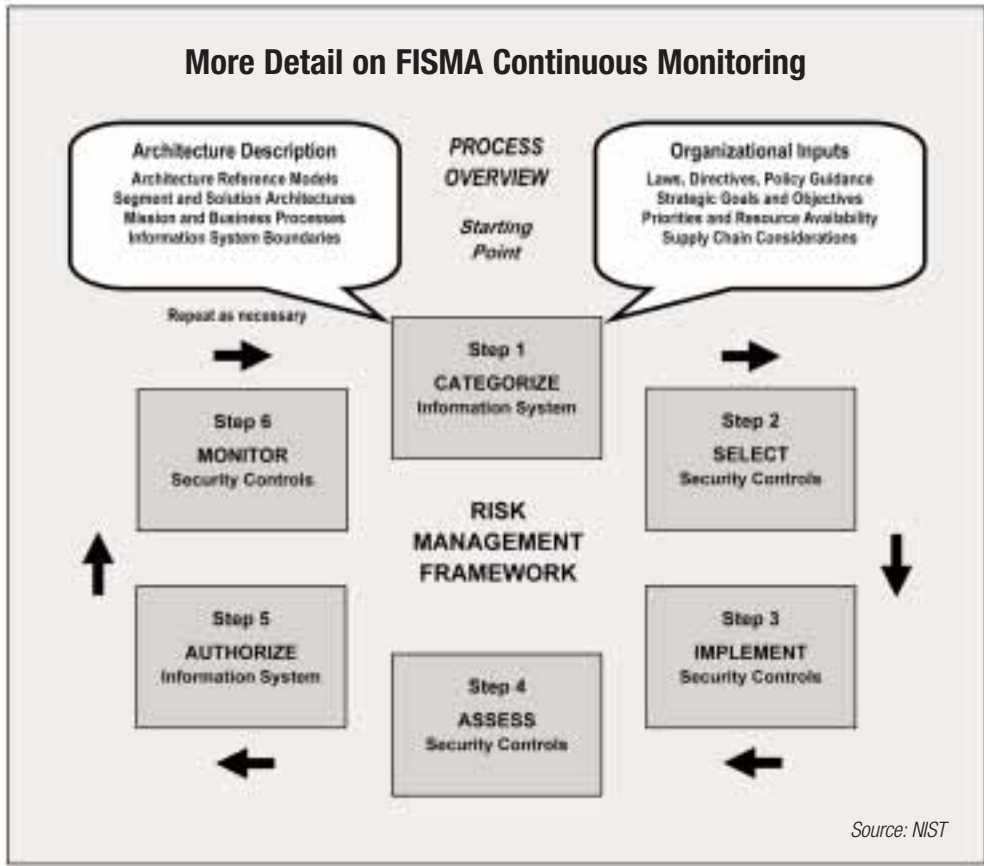
Until recently, federal IT security mandates, especially FISMA, remained largely focused on testing, evaluation and the accreditation of security solutions. This created a situation in which federal organizations spent time and effort on filing paperwork and providing documentation for compliance, without gaining any further security benefits in the process. In fact, the current certification and accreditation process required by FISMA has been estimated to cost approximately \$1.3 billion per year, and another \$1 billion is spent for agency inspectors general to audit FISMA compliance annually. In total, the government is estimated to have spent \$40 billion on FISMA compliance since its enactment in 2002.

This is also why the White House, with OMB's guidance, issued a memo in April instructing federal departments and agencies to use an online data collection tool to file fiscal year 2010 reports by Nov. 15, as required by FISMA. This single step reverses the compliance requirements, eliminating paper filings and documentation, and further underscores the administration's efforts to drive continuous monitoring and automation into federal IT organizations.

To continuously monitor security-related information from across the enterprise, "agencies need to automate security-related activities, to the extent possible, and acquire tools that correlate and analyze security-related information," according to the White House memo. In addition, federal agencies must "develop automated risk models and apply them to the vulnerabilities and threats identified by security management tools."

Within the electronic filing process, a team of government security specialists will quiz agencies on their security posture. The aim of the electronic and in-person questioning is to build cybersecurity profiles of each agency.

It was a year ago that the Office of Management and Budget also launched CyberScope, a secure, data collection



coming weeks, NIST is also due to publish new guidelines aimed at helping federal organizations build enterprise-wide risk management strategies. Continuous monitoring is only part of the solution, according to NIST officials. Agencies must focus on building a process for evaluating each organization's core mission, processes and critical information, and then decide what protections are most necessary.

Also on NIST's primary publication schedule are systems and security engineering guidelines and a separate set of guidelines for application security, along with additional guidelines for continuous monitoring. Further continuous monitoring guidelines will focus on managing risk and change in a dynamic environment. NIST is

platform for reporting that allows research and analysis across federal agencies. CyberScope is the primary online tool to be used by federal agencies in completing fiscal 2010 FISMA requirements. And federal chief information officer Vivek Kundra formed an interagency task force to develop new metrics for information security. Meanwhile, the National Institute of Standards and Technology revised its certification and accreditation Special Publication 800-37 to increase emphasis on continuous monitoring, including a recommendation for the use of automation to obtain timely, cost-effective, and efficient monitoring results. The OMB is also working on a cybersecurity dashboard much like the one used by the State Department to further unlock the real-time monitoring value of security information currently housed in federal IT environments.

Industry observers maintain cybersecurity must become a top priority in all IT purchasing decisions. Sometime in the

working to lay the foundation for helping agencies to build a risk management framework for cybersecurity, but there's still much heavy lifting to be done to complete the renovation. "This is likely why DHS was brought into assist in ensuring compliance across all federal agencies, said Deniece Peterson, manager of industry analysis for INPUT.

While in the last few years, there have been more than a dozen pieces of legislation related to improving cybersecurity bouncing around in Congress, none have been signed into law yet. And a new combined piece of legislation called Protecting Cyberspace as a National Asset Act of 2010 will be further promoted to help drive greater understanding of the need for better cybersecurity protections across all organizations. "Legislation, education, training and awareness, more secure products and more discipline in the deployment and use of technology are all required to improve cybersecurity," said INPUT's Peterson. ▀

# In Terms of Human Capital, A Cybersecurity Crisis Looms

According to a newly published report from the Center for Strategic and International Studies, “the current professional certification regime [for cybersecurity professionals] is not merely inadequate, it creates a dangerously false sense of security.”

The report’s authors, both former leaders within the Office of Management and Budget, Karen Evans, the former administrator of the Office of Electronic Government and Information Technology, and Franklin Reeder, former founder and chairman of the Center for Internet Security, maintain the current trend has emerged because:

- Individuals and employers are spending scarce resources on credentials that don’t demonstrably improve the ability to address security-related risks; and
- Credentials are currently focused on demonstrating expertise in documenting compliance with policy and statutes, rather than expertise in actually reducing risk through identification, prevention and intervention.

These U.S. security officials maintain the country’s cyber-defenses are not up to the challenge. In part, it’s due to a severe shortage of computer security specialists and engineers with the skills and knowledge necessary to do battle against would-be adversaries. While it’s critical, according to the report, to have “the right people at every level to identify,

build and staff the defenses and responses,” unfortunately, that’s precisely where the U.S. federal government is considered weakest.

“There are about 1,000 security people in the U.S. who have the specialized security skills to operate effectively in cyberspace. We need 10,000 to 30,000,” said Jim Gosler, Sandia Fellow, NSA Visiting Scientist, and the founding Director of the CIA’s Clandestine Information Technology Office, in the CSIS report.

According to Evans and Reeder, there simply aren’t enough highly technically skilled people required to operate and support systems already deployed. And there’s an even more “desperate shortage of people who can design secure systems, write safe computer code, and create the ever more sophisticated tools needed to prevent, detect, mitigate and reconstitute from damage due to system failures and malicious acts,” the report said.

Industry observers agree. “What we have today are many skilled professionals who can write reports, while what we really need are technically skilled professionals who can perform actual cybersecurity forensics, analysis, and/or secure coding,” said Alan Paller, director of research for the SANS Institute. ▶

---

## How to Resolve the Skills Challenge

The four key elements needed to deal with the critical skills challenge, according to Evans and Reeder, include:

- Promote and fund the development of more rigorous curricula in schools. (This is happening now, according to the report, though the U.S. reportedly lags behind other nations, including China, in finding and developing young talent.)
- Support the development and adoption of technically rigorous professional certifications that include a tough educational and monitored practical component.
- Use a combination of the hiring process, the acquisition process and training resources to raise the level of technical competence of those who build, operate and defend governmental systems.
- Ensure there is a career path as with other disciplines like civil engineering or medicine, rewarding and retaining those with the high-level technical skills.

More information on this report’s findings are available at: <http://csis.org/publication/prepublication-a-human-capital-crisis-in-cybersecurity>

---

# Advice for Government Organizations Implementing Continuous Monitoring

To help government organizations striving to incorporate automated, continuous monitoring, John Streufert, Chief Information Security Officer and Deputy CIO for Information Security for the Department of State offers the following advice:

**1) Narrow the aim of any security monitoring program** to begin addressing the worst specific attack vectors for each organization as opposed to trying to monitor all theoretically conceivable threats that are not in evidence or highly unlikely. At the State Department, primary attention was given to anti-malware defenses, other key vulnerabilities, configuration management weaknesses, and now coming soon, to boundary defenses and asset management.

**2) Set numerical standards** to assign known risks and apply extra emphasis to unique threats so the organization's focus is trained primarily on the worst cyber risks, first.

**3) Determine a small, manageable handful of initial systemic improvements** for the continuous monitoring program. No organization has enough resources 'to boil the ocean.' Instead, more focused attention by executives and managers will likely spell the difference between relative success and failure responding to known vulnerability and configuration management problems.

**4) Seek tools** that can provide timely, targeted and prioritized security information to organizational constituents. Don't make the mistake of treating all users as though they have identical security information needs.

**5) Pilot, pilot, pilot.** While most organizations will likely be able to conceive of a more comprehensive, complete continuous monitoring program, it's far less likely that the organization or its many users are ready to absorb more, until they walk through the necessary steps that will allow for basic security protection, local team cohesion, data quality and enterprise coordination for operational security.

**6) Determine the algorithm** to be used for each component to be scored. Begin with the raw Common Vulnerability Scoring System (CVSS) scores for vulnerability and determine how they should be transformed to be meaningfully added.

Determine the parameters for other scoring components by contrasting them with vulnerability scores.

**7) Establish a formal process** for requesting, reviewing and approving and/or rejecting scoring exceptions.

**8) Engage the owners** of the underlying data so the potential impact of tool upgrades on the scoring program can be analyzed. Having scores suddenly worsen across the board will generate trouble tickets, ill will and a feeling that the scoring program is unstable.

**9) Establish a team** to which scoring questions can be directed. Initially, there will be many questions due to misunderstandings, issues with the underlying data and concerns about the scoring program implementation. As much as possible, a pilot test's design should accommodate the addition of new scoring components and changes in calculations for certain components. Establishing this type of flexibility was one of the most difficult challenges for the Department of State.

## Additional Cyber Resources

Separately, the National Cyber Security Alliance (NCSA) has launched a new web portal that provides an enormous array of information, including news, tips, events and other resources for all kinds of computer users. NCSA sponsors National Cyber Security Awareness Month (NCSAM) in October. Each fall since 2004, NCSAM has become a national public awareness campaign to encourage everyone to protect their computers and the nation's critical cyber infrastructure. The Department of Homeland Security (DHS), National Cyber Security Alliance (NCSA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) are the primary drivers of NCSAM, which is designed to shed brighter light on how users, businesses and government organizations can better protect computers, children and data. While the campaign is set for October, cybersecurity requires vigilance 365 days per year. And the resources listed on this site can be useful to anyone seeking further information on topics related to cybersecurity, [www.staysafeonline.org/content/additional-awareness-resources-2010](http://www.staysafeonline.org/content/additional-awareness-resources-2010). ▀



# The only way to be prepared for anything is to prepare for everything.

Threats are constantly evolving — as is technology. Cloud computing and Web 2.0, for example, offer whole new security concerns. To address your challenges, CDW•G can help you design solutions combining everything from IP video surveillance to secure remote access and data loss prevention systems. We can even help with risk assessment and compliance. We'll ensure you find balance between security and your organization's preferences. Plus, we understand the contract, policy and purchase requirements unique to government. When anything happens, we'll make sure you're ready.

Citrix® NetScaler®  
CALL FOR PRICING



**CITRIX**

RSA SecurID® Authentication Manager 10 Users Promo

CALL FOR PRICING  
CDWG 799449



**RSA**  
The Security Division of EMC

McAfee® Total Protection for Data

**\$74.80**

101-250 user license¹  
CDWG 1389843



**McAfee**



Your preparation begins here. 800.767.4239 | [CDWG.com/federal](http://CDWG.com/federal)

¹Licensing requires a minimum purchase of 11 licenses; includes one-year Gold Support (24x7 technical support, upgrade protection and virus definition updates). Offer subject to CDW•G's standard terms and conditions of sale, available at CDWG.com. ©2010 CDW Government LLC