

## The State of Federal Government Information Security, 2007

Federal IT decision makers are more concerned about information security than they were in 2006, despite spending more time on security requirements, according to a Cisco® survey conducted in September 2007. Respondents included 202 federal IT decision makers representing more than 30 federal agencies and all branches of the military. The survey was written and conducted by the e-Gov Institute and interpreted by Market Connections, Inc., a federal information technology market research firm.

### Top Concern: Bots and Spyware

Respondents said that what kept them up at night, despite their increased security efforts, were bots and spyware. This finding could reflect the large number of highly publicized spyware and cybersecurity attacks against federal agencies over the last 12 months, according to David Graziano, manager of federal security, Cisco. "Bots and spyware have been increasing in importance, and now they are the number-one concern," he says. Federal agencies can reduce risk with Network Access Control (NAC) solutions that check PCs and laptops to ensure they are not infected and have current antivirus software, patches, and configuration settings required by agency security policy. The Cisco Network Access Guardian solution performs automatic remediation, when necessary, without any effort from the employee or agency IT group.

### IPv6: Valued for Security Benefits

Regarding IPv6, nearly 60 percent of respondents said they expect it to improve their agency's security architecture. And yet, only a little more than one-third of respondents reported that their agency is developing, or has developed, an IPv6 security architecture—a surprising finding given the June 2008 deadline for using IPv6 on agency infrastructures. Agencies that want assistance with any aspect of the transition, from planning to deployment and optimization, can take advantage of the Evolv6 service from Cisco and its partner Command Information.

### Existing, Fractured Security Architectures Actually Impede Overall Security

Asked about barriers to improved information security, respondents cited funding first. Significantly, the next biggest barrier, mentioned by half of respondents, is the agency's existing, unintegrated security architecture. "Over the past decade, federal government agencies have purchased standalone security devices such as firewall and intrusion detection systems [IDS] from different vendors," says Graziano. "The devices usually work great independently, but they cannot work together, which limits their value for providing earlier awareness of threats or identifying false positives." Agencies that regard their standalone security products as a barrier to overall security have two remedies. One is to deploy routers and switches with embedded security capabilities—regarded as a critical capability by 80 percent of survey respondents. The other is to use software that can gather and correlate information from an agency's existing standalone security products to provide actionable information. An example is Cisco Security Monitoring, Analysis, and Response System (MARS), which correlates information from nearly any vendor's security products as well as from Cisco network devices.

## Progress on User-Based Security Issues

Some of the survey results underscore recent security progress by federal government agencies. For example, 30 percent no longer consider remote access as important or very important to their agency's security efforts. "This is not to say that agencies do not think that remote access is important, but rather that they now perceive it as being under control," says Graziano. "The previous problem of users spreading an infection from their laptops has largely been solved because of NAC solutions that enforce agency policy for antivirus software and settings."

To read the survey results, visit

[www.cisco.com/web/strategy/docs/gov/cisco\\_security\\_report\\_11\\_1\\_2007.pdf](http://www.cisco.com/web/strategy/docs/gov/cisco_security_report_11_1_2007.pdf)



**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
Tel: +65 6317 7777  
Fax: +65 6317 7799

**Europe Headquarters**  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: +31 0 800 020 0791  
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)