

# *2006 Federal IT Security Survey*

## *Summary Results*

Market Connections, Inc.

October 2006



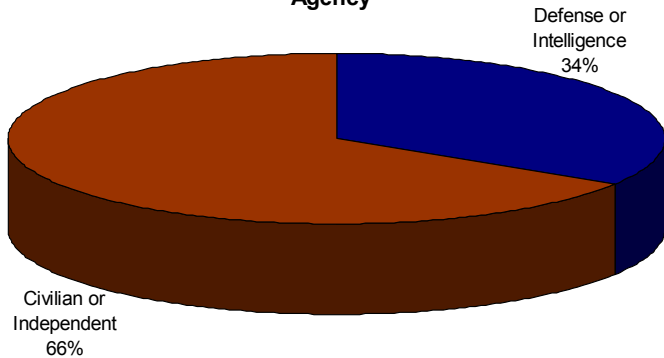
# *Background*

---

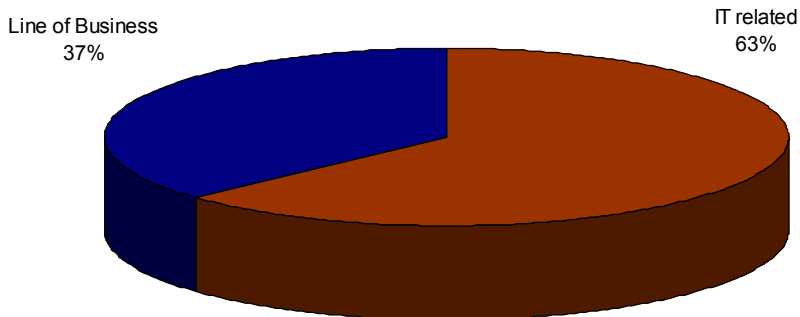
- **In August 2006, 200 federal IT decision makers drawn from various trade publication subscriber lists and federal employee databases were interviewed about their main security efforts and issues, progress and concerns with Federal initiatives, and perceptions of vendors.**
- **Respondents represented more than 45 Federal agencies and all branches of the military.**

# Overall Sample Population: Agency, Job Function and Involvement

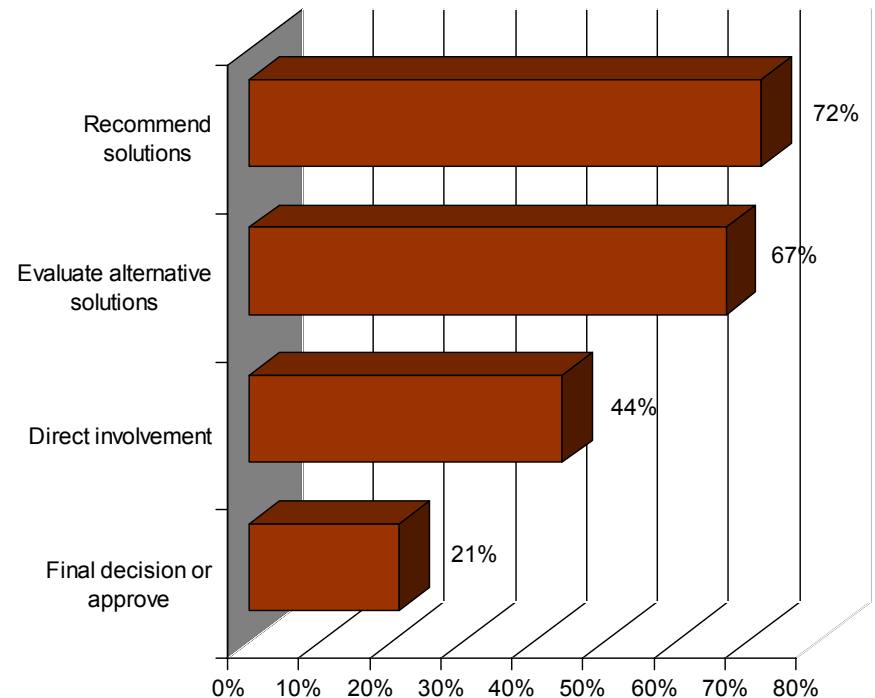
Agency



Primary Job Focus



Involvement in IT/network solutions



You are an employee of which of the following?

Are you mainly involved in the daily business operations of your agency or more specifically, IT related functions?

Please indicate the scope of your involvement of IT and network solutions for your agency or organization.

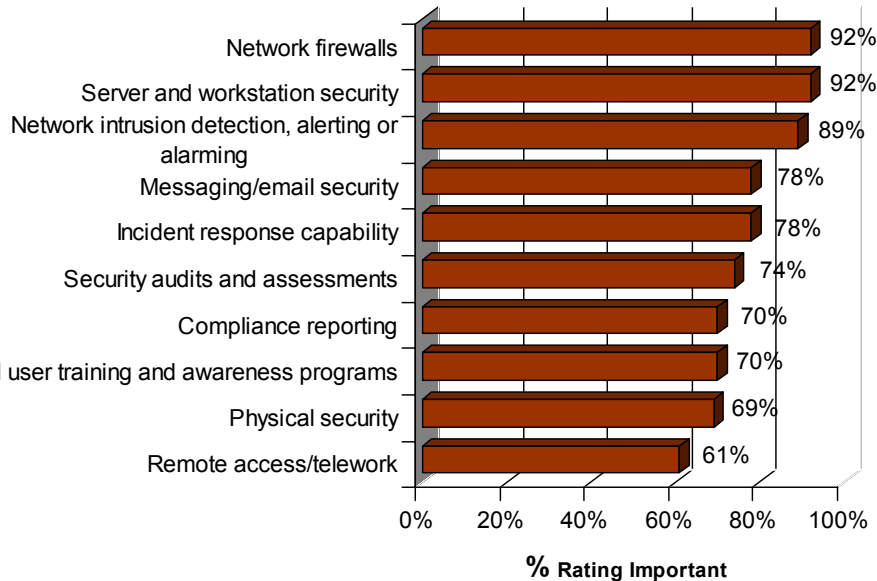


# *Security Issues*

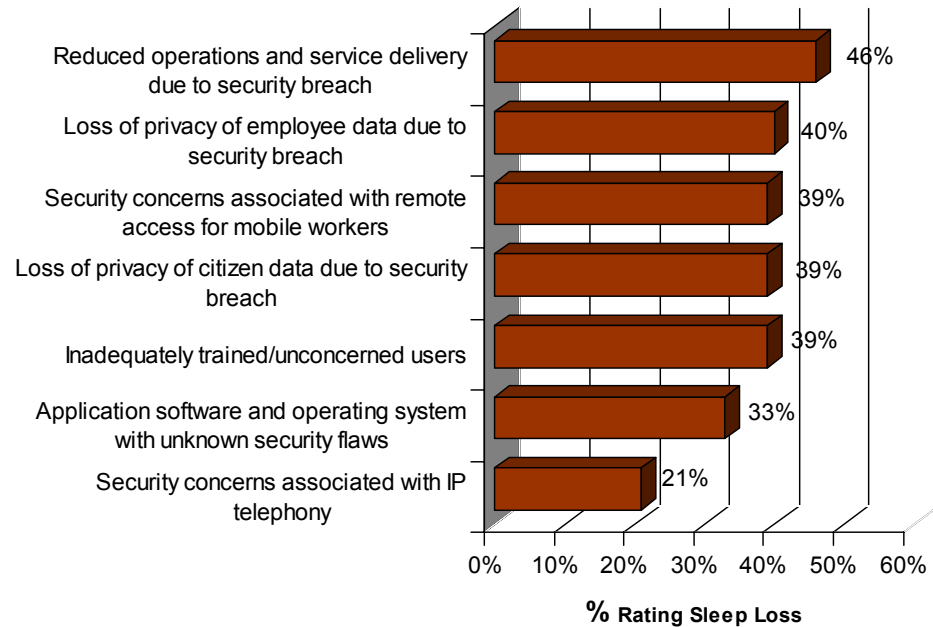
# Importance of Security Efforts and Issues

- Network firewalls, and server and workstation security, were considered more important to overall security efforts. The largest number of respondents reported losing sleep over the possibility of reduced operations and security delivery due to security breaches.

Importance of Components to Security Efforts



Extent to Which Security Issues Keep you Up at Night



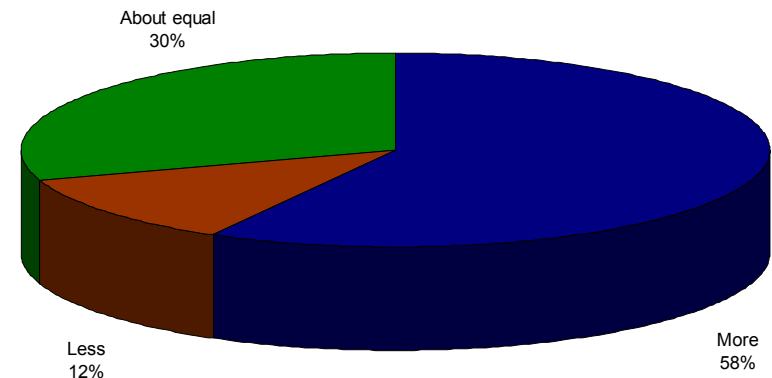
On a scale of one to five where one is "not at all important" and five is "very important", how important are the following security components and activities to your agency's total security efforts?

On a scale of one to five where one is "sleep like a baby" and five is "do not sleep a wink", to what extent do the following security issues or concerns keep you up at night?

# Agency Security: Progress Being Made

- **Most respondents cited feeling more secure with their agency's security than they did two years ago.**
- **More DOD respondents than Civilian respondents indicated that they felt better about their agency's security.**

Do You Feel More or Less Secure than Two Years Ago?

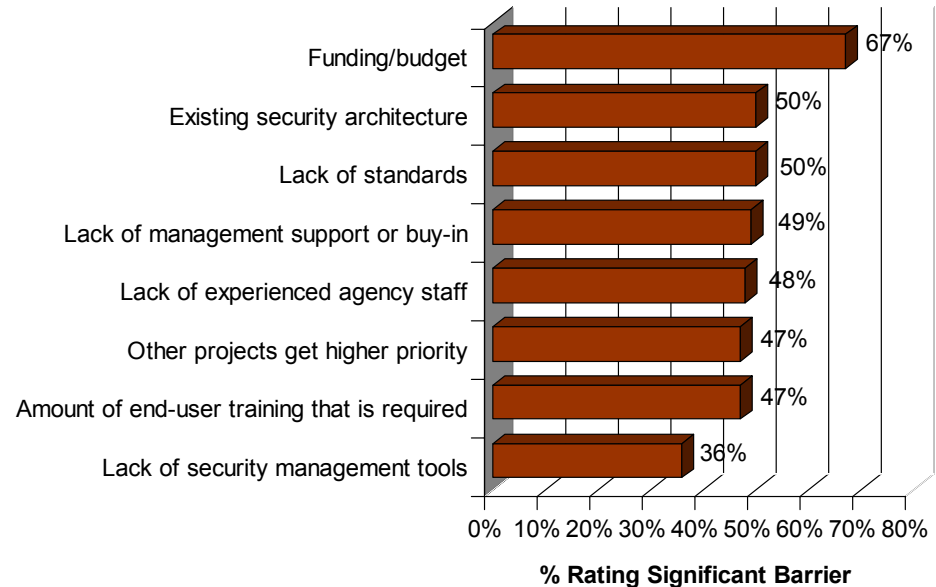
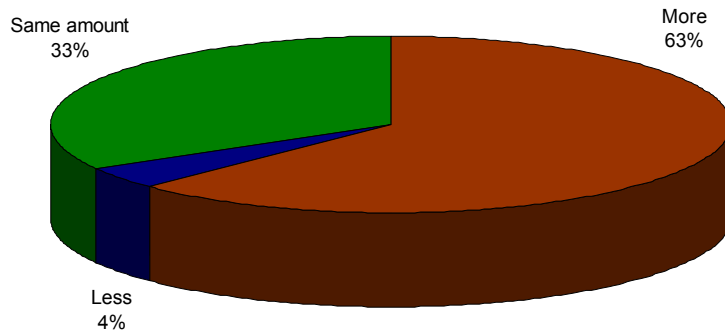


Regarding your agency's security, do you feel more, less, or about equally secure now than you did two years ago?

# Security Requirements and Barriers to Security Improvement

- Respondents spent more time this year dealing with mandated security requirements than last year. Funding was the top barrier to improving network security capabilities, though many others were still evident.

Compared to Last Year, Amount of Time Spent Dealing with Security Requirements



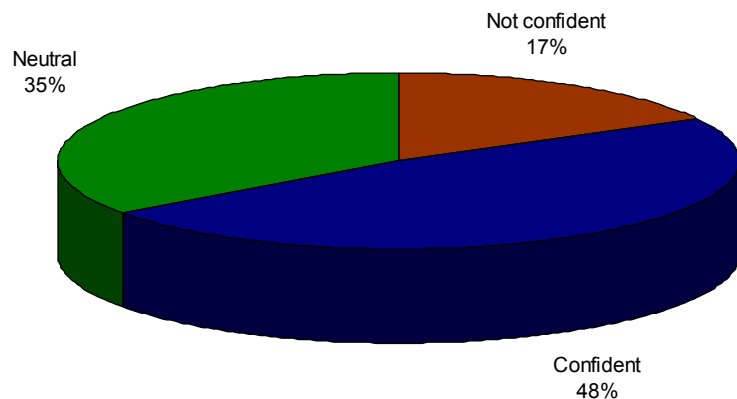
Compared to one year ago, do you spend more, less, or about the same amount of time dealing with mandated security requirements?

Using a scale of one to five, where one is "not at all significant" and five is "very significant", how significant are the following barriers to improving your agency's network security capabilities?

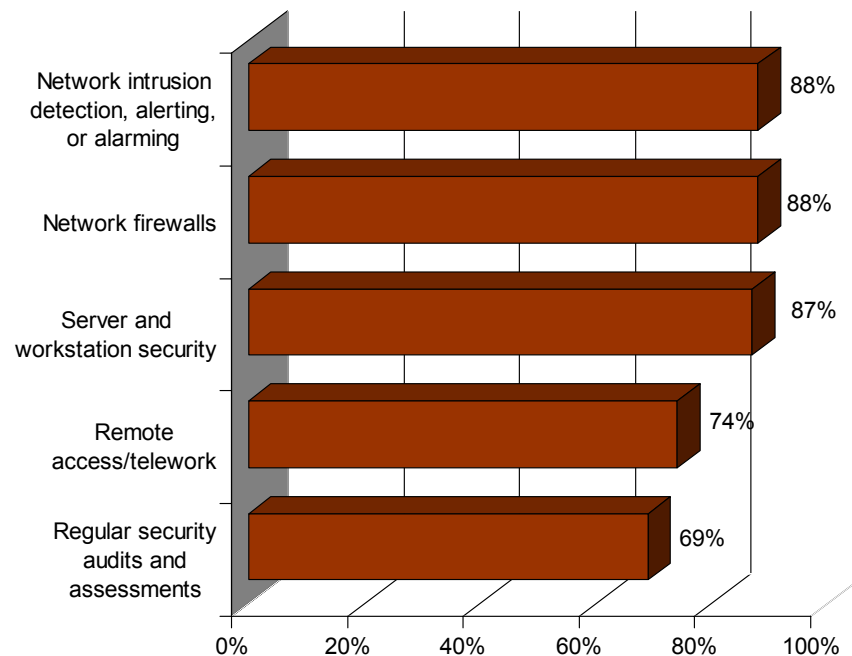
# Thoughts on Software Automation Tools

- Nearly half of respondents (more from DOD than Civilian agencies) felt confident that software automation tools will address their agency's security issues in the future. These software automation tools will specifically address network intrusion detection, firewalls, and server security.

Level of Confidence in Software Automation Tools



Areas to be Addressed by Software and Other Automation Tools



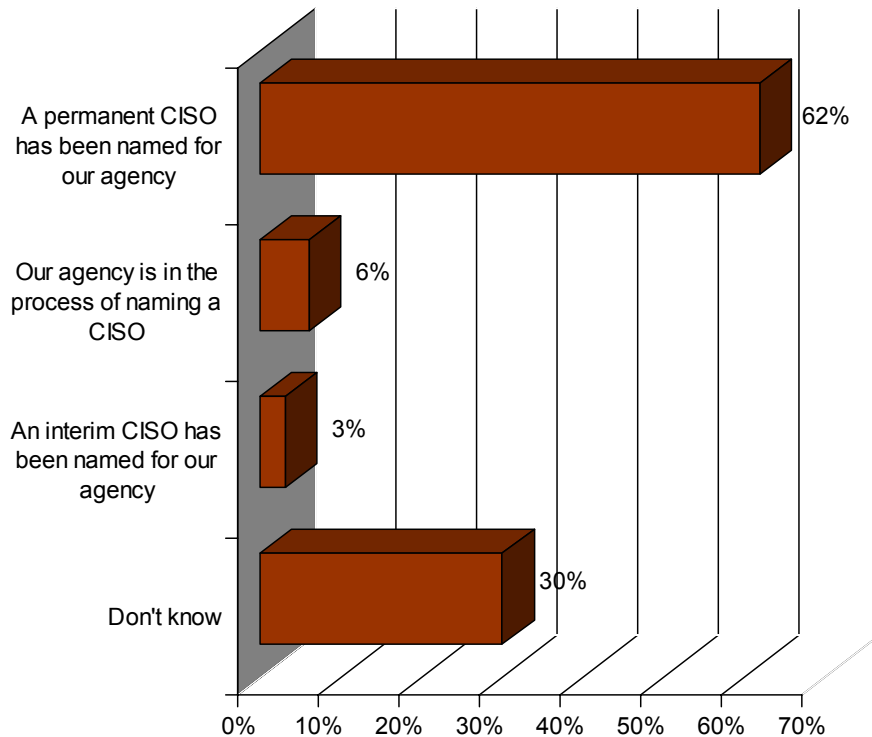
On a scale of one to five, how confident are you that software automation tools will adequately address the majority of your agency's security issues?  
Which of the following security areas do you envision will be primarily addressed by software and other automation tools in the future?



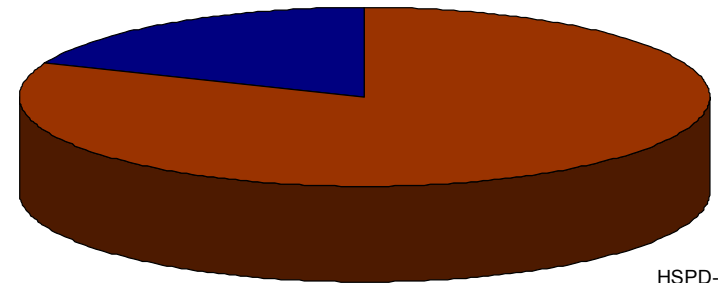
*Progress and Concerns  
with Federal Requirements*

# Status Check: Naming a CISO and Completing HSPD-12

- **Most respondents work in agencies where a permanent CISO has been named and expected to complete their HSPD-12 requirements on time.**



HSPD-12 requirements not completed on time  
19%



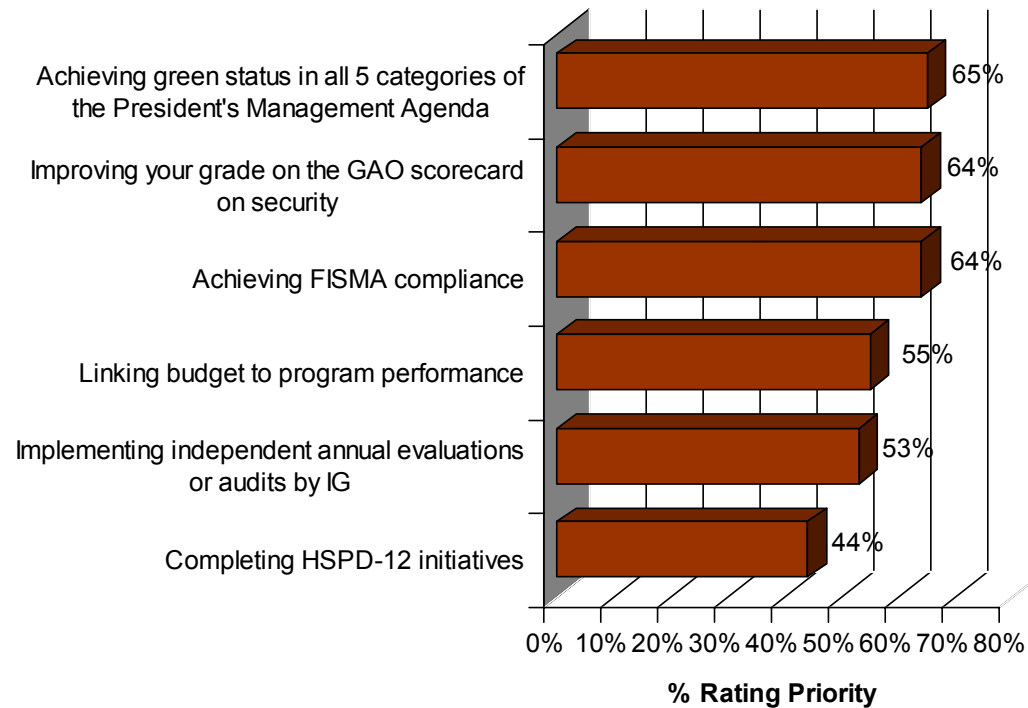
HSPD-12 requirements completed on time  
81%

What is the status of naming a Chief Information Security Officer (CISO) to your agency?

Do you expect to complete your HSPD-12 requirements on time?

# Priorities for the Upcoming Year

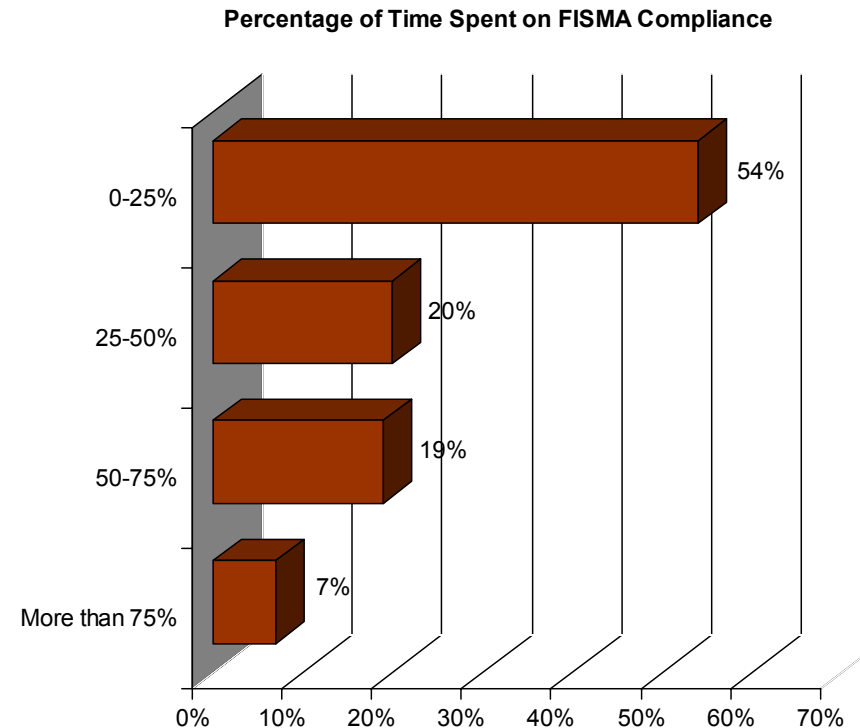
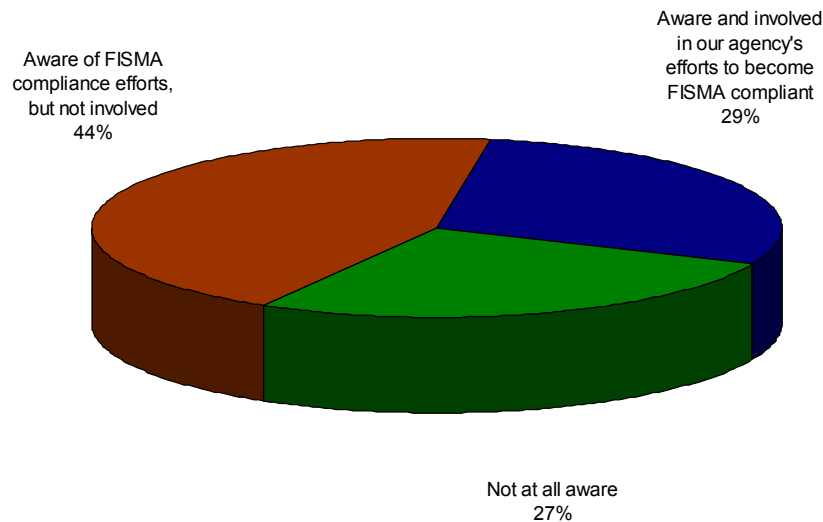
- **Three Key Priorities: (1) Achieving green status in every category of the PMA, (2) Improving security grades on the GAO scorecard, and (3) achieving FISMA compliance all compete for personnel time and funding.**
- **Linking budget to program performance has increased as a priority since 2005.**



On a scale of one to five, where one is an "extremely low priority" and five is an "extremely high priority", please indicate your agency's level of priority over the next 12 months for the following initiatives:

# FISMA Compliance Efforts

- **Half those who are aware and involved in compliance spent at least a quarter of their time committed to exclusively FISMA compliance matters.**

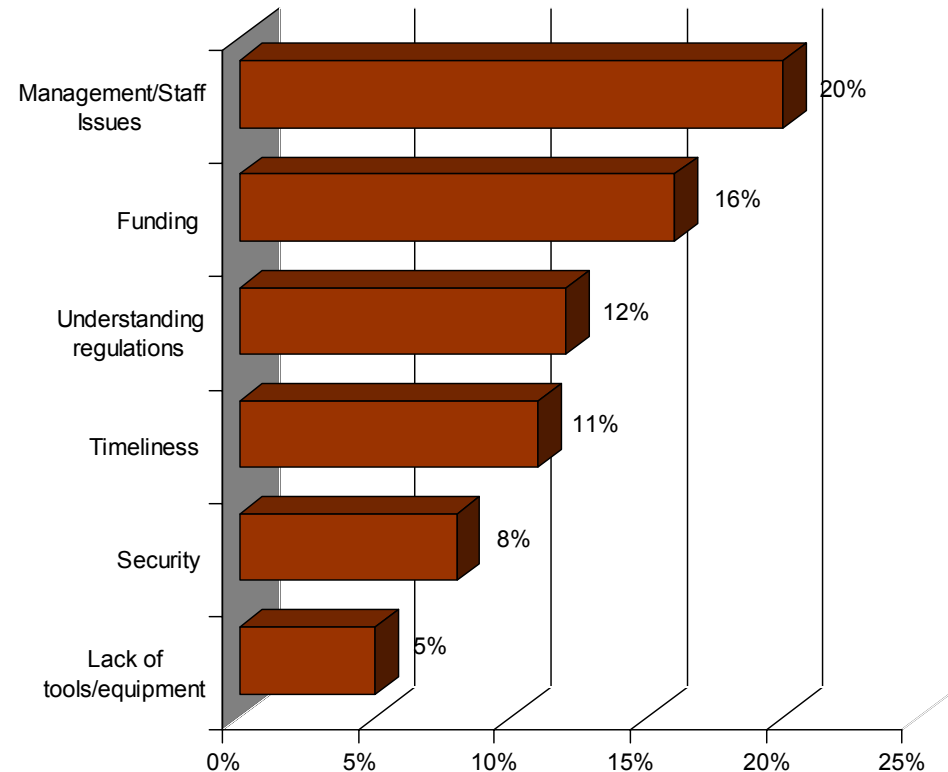


*How aware are you of your agency's efforts to achieve FISMA compliance?*

*What percentage of your time do you approximate is committed to achieving FISMA compliance?*

# FISMA Compliance Challenges

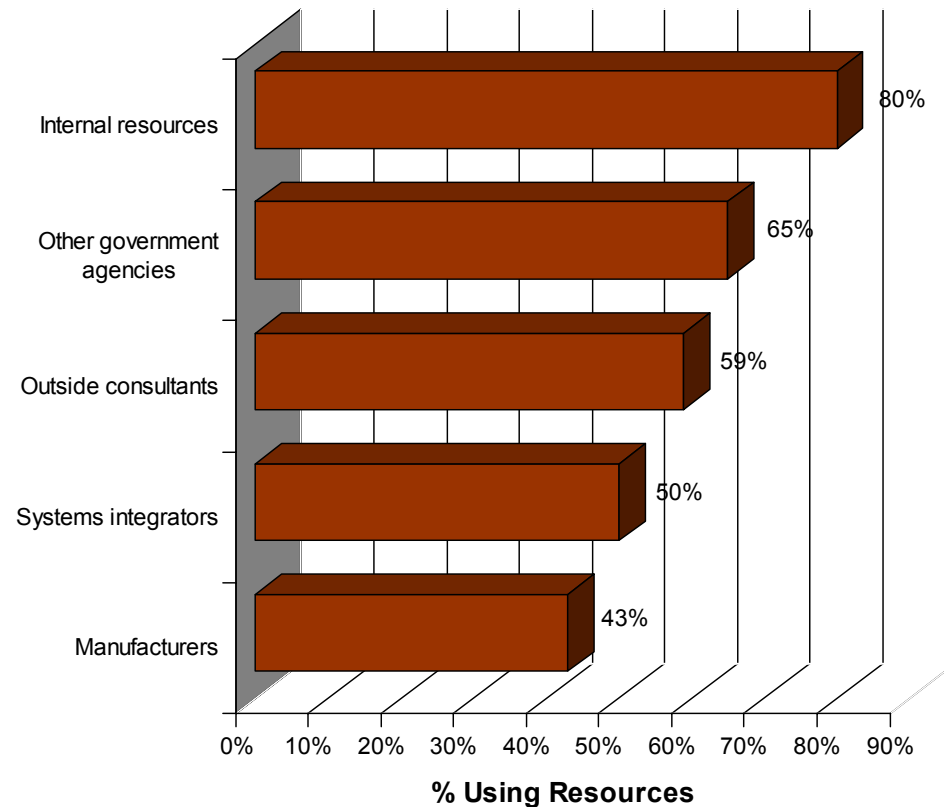
- **Management/staff issues, such as training and capacity, and funding were top of mind challenges for respondents.**
- **Specific examples of management/staff issues include:**
  - “management awareness”
  - “employee/management participation”
  - “lack of personnel”
  - “getting agreements between management”
  - [lack of] “manpower”
  - “training”



(UNAIDED) What are your top two challenges in achieving overall FISMA compliance?

# Resources Used in Security Solution Implementation

- **Despite training and staffing barriers, internal staff is still most frequently relied on to develop and implement security solutions.**
- **When internal agency resources are not as available, many look toward other agencies to provide assistance.**



Which of the following resources do you use when developing and implementing security solutions?

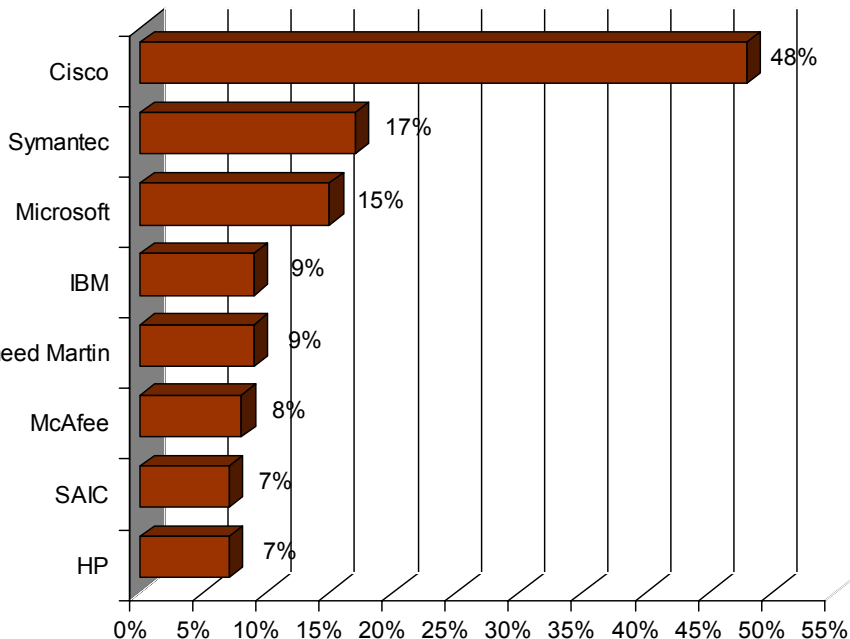


# *Perceptions of Vendors*

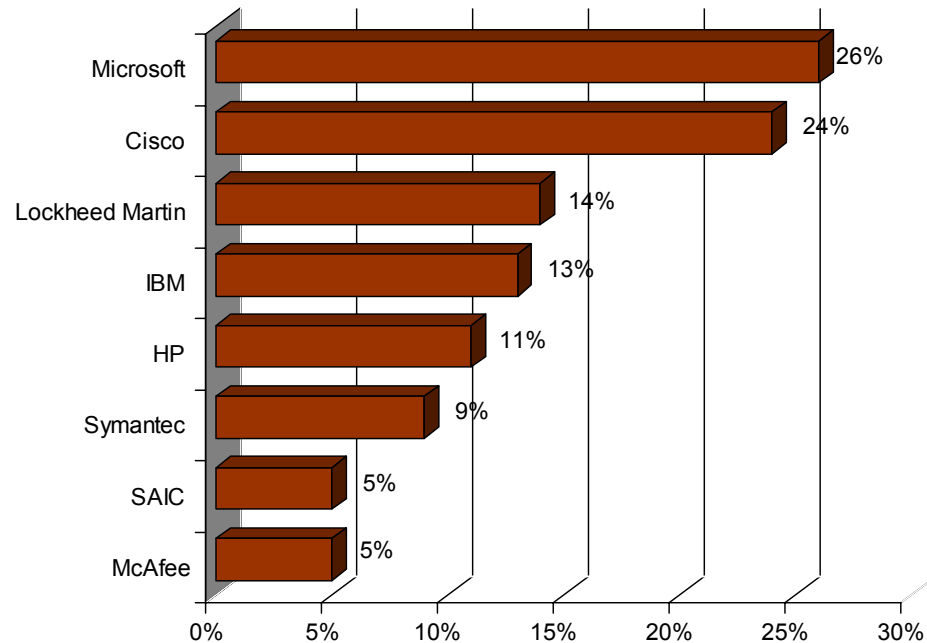
# Leading Providers of Network and Information Security

- Unaided, Cisco was named a leading provider of network security by nearly half of respondents. Microsoft and Cisco were listed as the main players in providing information security solutions to the federal government.

Leading Providers of Network Security



Leading Providers of Information Security



(UNAIDED) What companies do you consider as the leading providers of network security to the federal government?

(UNAIDED) What companies do you consider as the leading providers of information security solutions to the federal government?

# *Contact Information*

---

**Market Connections, Inc.**  
13135 Lee Jackson Memorial  
Hwy, Suite 380  
Fairfax, VA 22033  
703.378.2025

[www.marketconnectionsinc.com](http://www.marketconnectionsinc.com)

