



Cisco 2008 Federal IT Security Survey **Top Line Summary**

In October 2008, Cisco commissioned Market Connections, Inc. to conduct a web-based survey of federal IT decision-makers. Respondents were asked about their main security efforts, issues, and concerns. Respondents represented more than 45 federal agencies.

I. Security Trends (2005-2008)

The security survey has been conducted annually since 2005. The following conclusions were reached after reviewing the survey data for each year:

- Issues related to security breaches, such as loss of privacy data or reduced operations and service delivery, have been top concerns from 2005-2008.
- Time spent managing security is not decreasing. Since 2006, more than 60% of respondents each year said they spent more time on mandated security requirements than in the previous year.
- Confidence in agency security grew from 2007 to 2008. The majority of respondents reported feeling more confident in their agency's security than they did four years ago – increasing from 51% in 2007 to 60% in 2008.
- Web 2.0 technologies remain a concern, with file sharing/peer-to-peer, remote access to secure data and social networking of greatest concern.

II. Demographics (2008)

- There were 223 survey respondents. Civilian respondents represented 60% of the sample, while defense represented 40%, mirroring the distribution of the overall federal population.
- Most respondents (71%) were involved in IT implementation, while 29% were involved in IT policies.
- All respondents were involved in IT security activities, ranging from applications or data security to Web 2.0 technologies.

III. Security Efforts and Issues (2008)

- In general, respondents were more concerned with one-time security issues, such as loss of privacy data or reduced operations and service delivery due to security breaches. Inadequately trained and unconcerned users also caused concern for respondents.
- The majority of respondents (60%) reported feeling more confident in their agency's security than they did four years ago.
- Eight of every ten respondents indicated that embedding or integrating security capabilities and safeguards into their agency's infrastructure is critical.



IV. Federal Initiatives and Requirements (2008)

- Consistent with previous years, nearly two-thirds of respondents reported spending more time on mandated security requirements than they did one year ago. More civilian respondents than defense indicated they were spending more time on mandated security requirements.
- Achieving FISMA compliance and complying with the Comprehensive National Cyber Security Initiative were the top two federal initiative priorities among respondents.
- Four in ten civilian respondents believed they will spend 25% or less of their time on tasks related to the National Cyber Security Initiative (NSPD 54/HSPD 23); while another 40% do not know how much time they will spend on the initiative.
- Nearly half of civilian respondent organizations intend to manage TIC entirely in-house, while one-third plan to outsource some aspects of TIC, with the remaining one-fifth planning to outsource TIC completely.
- One half or more of respondents indicated that service capability and physical (SOC/NOC) would be challenging aspects of TIC to improve in order to meet OMB guidelines.

V. Security Impact of Web 2.0 (2008)

- One in five respondents were involved in securing Web 2.0 technologies at their agencies.
- Web 2.0 services of greatest concern to respondents included peer-to-peer file sharing, remote access to secure data, and social networking.

