Federal Government Concern for IT Security Exceeds that of the Private Sector.

AUTHORS:

Gibson Trub, Managing Partner

Laurie Olski, Managing Director

TOPIC:

Current State of IT Information Security in Federal Government

DATE:

July 27, 2009

Publishing Information

GMG Insights provides analysis, research, and strategy services to companies with complex B2B sales. Publication headquarters, marketing, and sales offices located at:

GMG Insights
95 Nason Hill Rd.
Sherborn, Mass. 01770
Phone: 508-545-1095
Fax: 866-725-7059
Internet: info@gmginsights.com

Methodology

This study focuses on IT security officers in U.S. government agencies with responsibility for security software initiatives. It includes a quantitative survey and in-depth interviews and focus groups in Washington, D.C. The study was conducted in March 2009 and carries a +/- 5 percent margin of error at the 95 percent confidence level.

The quantitative analysis was conducted by Beacon Technology Partners, Maynard, Mass. James McLeod-Warrick, president of Beacon Technology Partners, collaborated on the analysis and reporting of the findings.

This study was sponsored by CA.

Table of Contents

Gibson Marketing Group • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-655-5617 | F: 508-259-7962
www.gibsonmarketinggroup.com

Synopsis

This study examines IT security efforts and implementations in U.S. government agencies at a time when the economic meltdown and changing regulatory compliance mandates are focusing more attention on IT security practices. This report provides an IT perspective on the state of federal IT security, current attitudes, plans for the future, and market maturity. It also compares federal IT security plans and perspectives with those of worldwide private enterprises.

In the vast majority of U.S. federal agencies, overall IT spending is in a forced decline, resulting from tightening budgets. However, budgets devoted to IT security initiatives remain constant or are growing. Several factors contribute to this counterintuitive trend:

- First, the fear of internal threats (whether malicious or benign) has overtaken the fear of external threats.
- Second, the need to comply with ever-increasing regulations and satisfy auditors and Congress continue to fuel IT security investments.

It would be reasonable to expect that large agencies have automated internal security processes and adopted technology solutions such as identity and access management (IAM) to handle internal threats. Surprisingly, that is not the case, but there is increasing interest in new solutions, particularly among Department of Defense (DoD) agencies. Data-loss prevention, provisioning, log management, single sign-on and other solutions to handle manual tasks are top-of-mind and top-of-wallet.

Despite the mandate to reduce spending, necessity dictates that for the foreseeable future, new IT security software solutions will be broadly adopted throughout the federal government.

For a report on the state of IT security worldwide, see Economic downturn drives increased spending in IT security worldwide, a GMG Insights report published April 17, 2009.

Gibson Marketing Group • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-655-5617 | F: 508-259-7962
www.gibsonmarketinggroup.com

Federal agencies see critical gaps in their approach to information security

Virtually without exception, federal agencies have a common need to get the IT security "house" in order across their spectrum of IT initiatives. And, almost without fail, DoD's sense of urgency is even greater than that of civilian agencies. Many in the focus groups (as well as experts quoted and writing in recent publications) cite the Obama Administration's emphasis on openness and its desire to deliver greater levels of public access and transparency as driving a re-evaluation of security needs.

"The Web 2.0 stuff, we have hard deadlines now where we're supposed to be able show transparency and openness with the public, sharing of data. There is a working group at the White House level that's dealing with Web 2.0, everything from Twitter to blogs to using Facebook. You know, you can totally get bitten in the ass… when I met with my deputy director today, you know, I said, 'We, as an organization, first have to decide what do we want to do so that we can then figure out how we're going to do it.'"
- Federal IT executive

"(The White House said) do it, but figure out how to do it securely. They still want you to do it. So those are explicit marching orders that the federal agencies already received from this administration."
- Federal IT executive

"For leaders... it's really important to be connected to [social networking tools] and understand it," said Navy Adm. Mike Mullen, chairman of the Joint Chiefs of Staff, noting that he has his own Facebook page. "I think communicating that way and moving information around that way—whether it's administrative information or information in warfare — is absolutely critical."
- Government Computer News, June 22, 2009

Federal IT executives believe they have a great deal of catching up to do.

Gibson Marketing Group • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-655-5617 | F: 508-259-7962
www.gibsonmarketinggroup.com

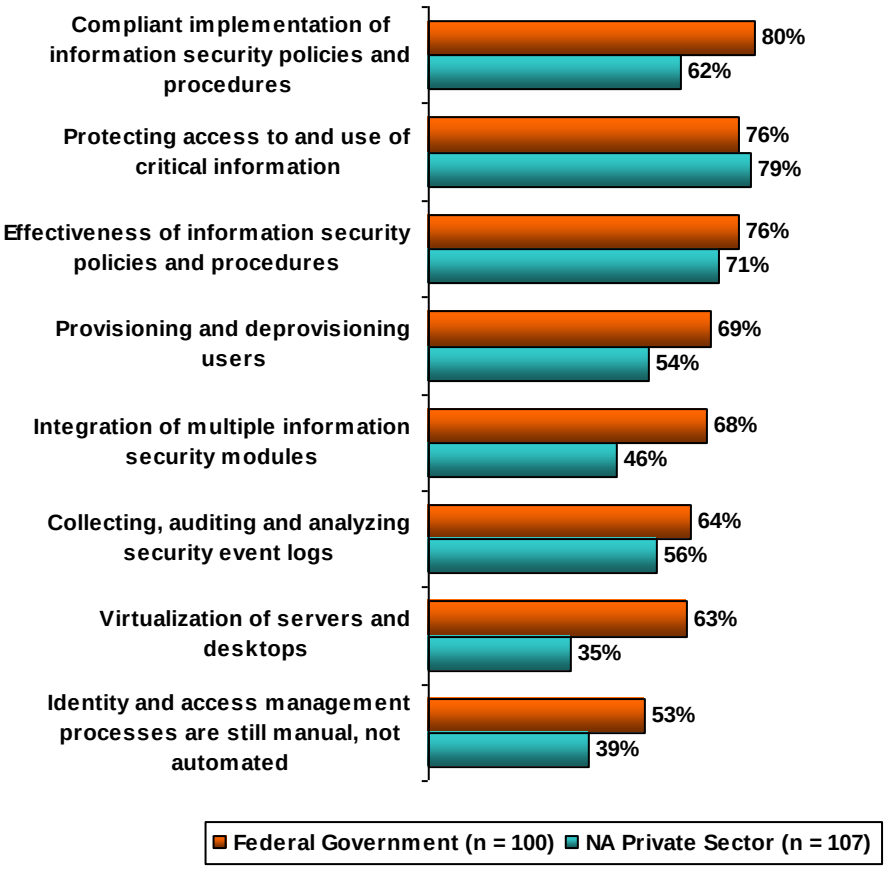

Fig. 1 - ***Percentage of agencies viewing initiatives as critical for information security.***

The need to comply with a vast array of regulations is compelling both civilian and defense agencies to spend security dollars

The myriad of regulations may affect one federal agency more than another, but the net effect is that spending is clearly dictated by regulations. Federal IT security executives are very conversant with these regulations and can rattle them off quickly from memory. And they are well aware of likely future additions.

"Presidential Directive 63 that President Clinton signed states that all critical information infrastructure components - and that almost touches everything that interfaces with the government - [are] considered critical parts of that infrastructure [and have] to be certified and accredited through FISMA."
- Federal IT executive

The number of regulations for security can be mind-boggling.

Gibson Marketing Group • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-655-5617 | F: 508-259-7962
www.gibsonmarketinggroup.com

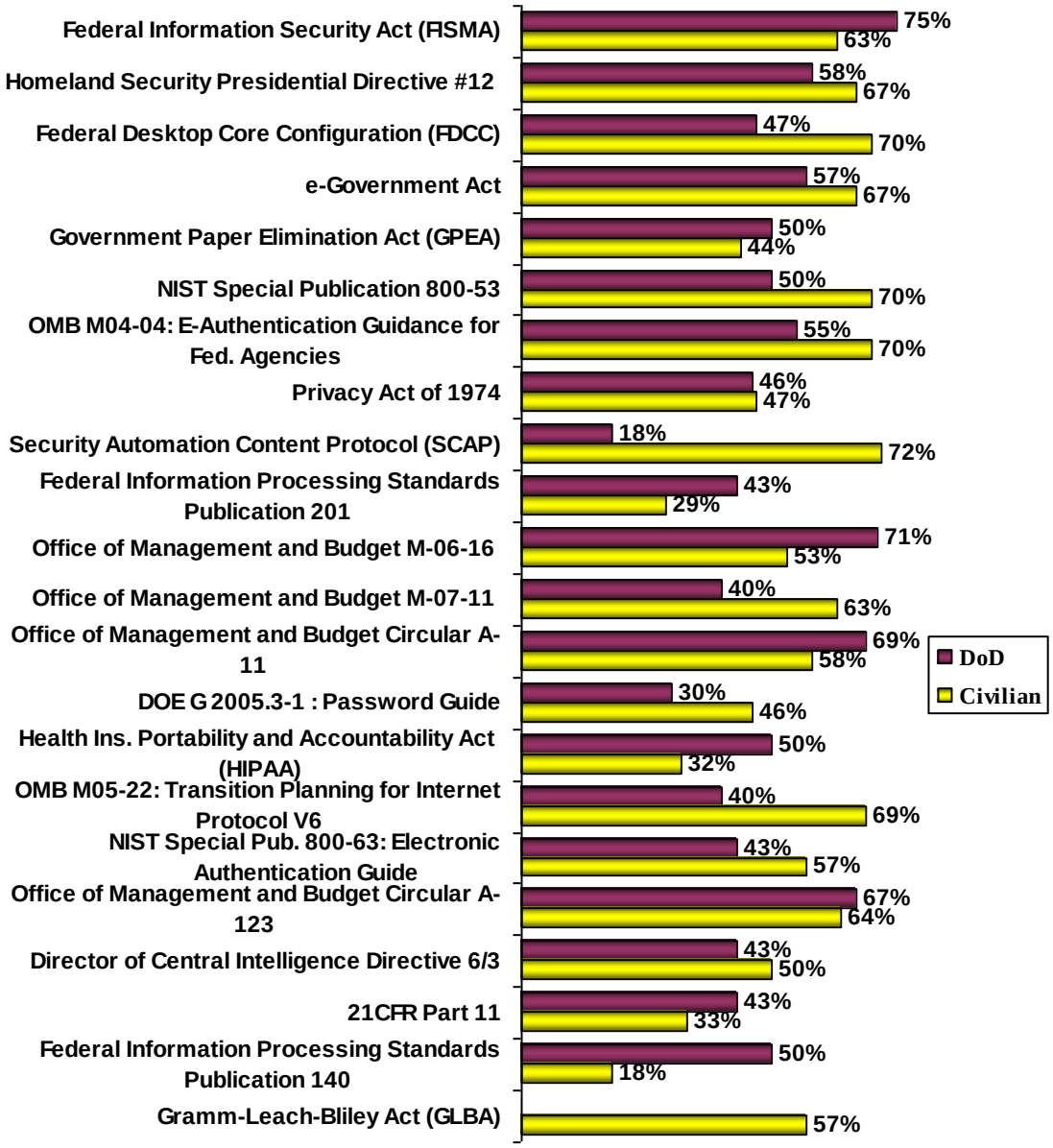

Fig. 2 - ***Percentage of information security dollars spent, by regulation.***

Gibson Marketing Group • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-655-5617 | F: 508-259-7962
www.gibsonmarketinggroup.com

Agencies recognize likely deficiencies in handling future security requirements

Just as we heard from private enterprise, the overwhelming majority federal government IT executives believes that the regulatory burden will only increase. The self-assessment of where they are today regarding practices and controls suggests that there is much more to be done to meet the current state of IT security requirements. Most believe that processes are still far too manual to be effective and efficient. And there is a lack of visibility into organizational compliance.

"I mean, I work for DoD and you have X amount of directives that are coming down from DoD. And there's more and more of them coming down."
- DoD IT executive

"[We see new mandates brewing.] They're coming - like a hurricane."
- Federal IT executive

Federal IT executives see the regulatory burden growing quickly.

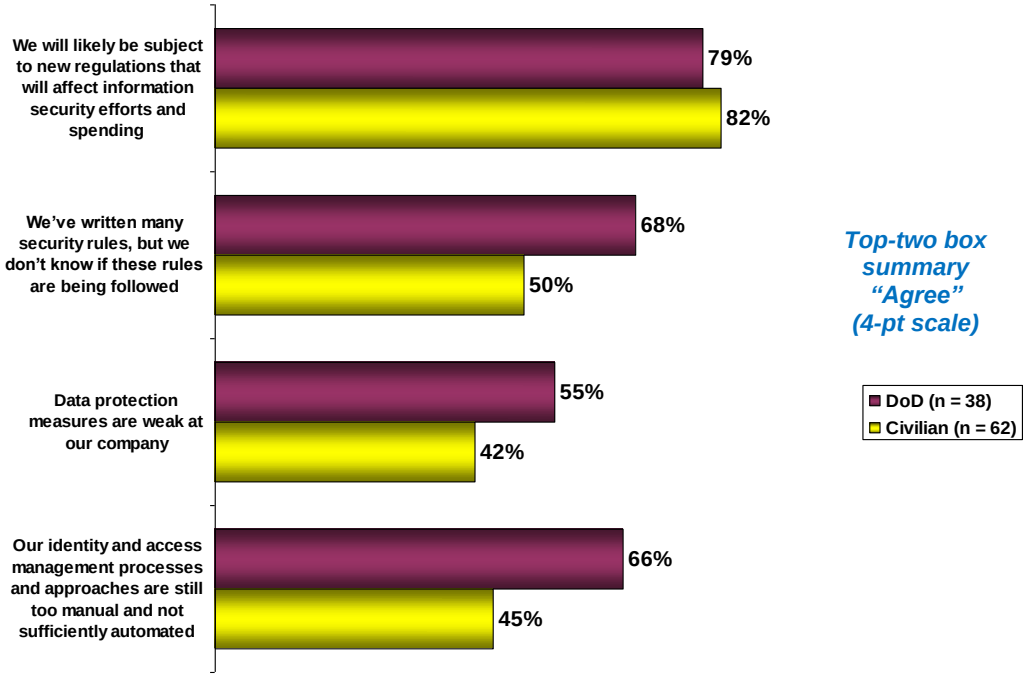

Fig. 3 - *Percentage by respondents agreeing that their agency condition matches the description given.*

Gibson Marketing Group • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-655-5617 | F: 508-259-7962
www.gibsonmarketinggroup.com

Awareness of security shortcomings explains 2009 IT security budgets

In stark contrast to other categories of federal IT spend, security spending is, at minimum, flat. For about half of the agencies surveyed, that line-item is growing over 2008 levels. Where spending is flat, security spending represents a larger percentage of the overall budget as these agencies find other places to economize on their IT spend. Both IT and non-IT leadership place a higher priority on security and compliance. These days, hardware is often the place IT looks to economize.

"And if you're looking for the increase in budget to cover it, it's not there. If you're looking at what our requirement is in our money in that area, the money is going down as requirements are going up. ..It's not meeting the requirements that are coming on top of us."
- DoD IT executive

"I think it would operate differently in private industry because it would be cost savings that would drive the initiative. And I don't think they're concerned about the cost savings that would occur if the Department of Homeland Security developed compatible systems across the board."
- Federal IT executive

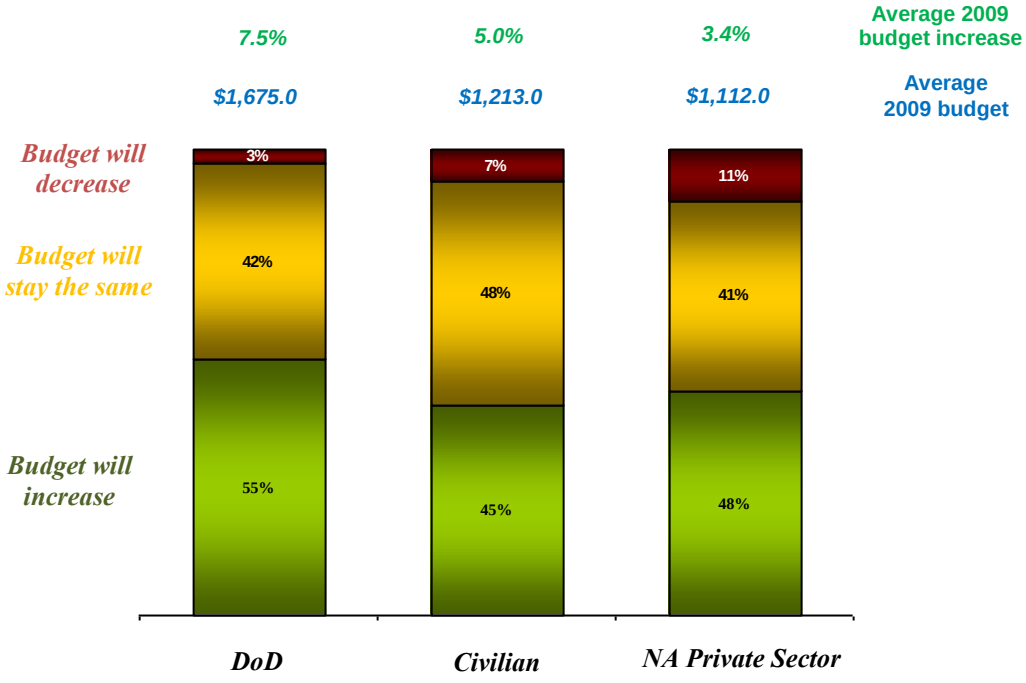

Fig. 4 ***- Projected IT security budgets with comparison between federal agencies and large North American private companies.***

IT spend on security is becoming an even greater piece of the overall IT effort.

Gibson Marketing Group • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-655-5617 | F: 508-259-7962
www.gibsonmarketinggroup.com

Compliance drives much of the IT security spend, particularly for DoD

The long list of regulations federal agencies comply with has a direct impact on budgets. And if their expectations of even more regulatory burden prove accurate, the allocation rates will inevitably rise as well. Responders expressed an added concern: the recognition that existing regulations are always open to new interpretations by auditors, resulting in additional remediation.

Agencies are forced to spend a significant portion of their IT security budgets on regulatory compliance.

"So NIST, which is the National Institute of Standards and Technology - they've written standards that kind of build guidelines, if you will, on how to protect your infrastructure. And you kind of pick and choose which is best for you based on the sensitivity of your information, mostly - and criticality."
- Federal IT executive

"And DoD has its own, because we don't follow some of the regulations that are going out to the civilian agencies… we have this Defense Information Systems Agency, which basically directs most of security or minimum security for your network and so forth. You know, we have to have our systems accredited every time there's a change. If there's a change to an application or a system, it has to get re-accredited by DISA…"
- DoD IT executive

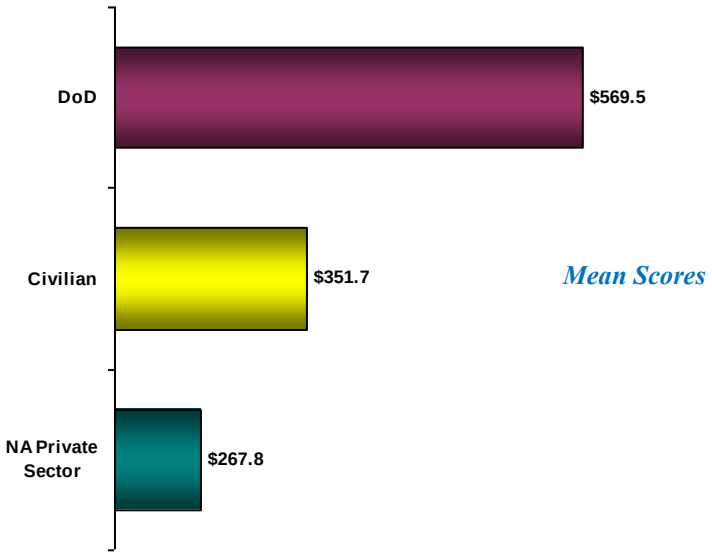

Fig. 5 – *Amount, in dollars, of information security budget allocated to regulatory compliance.*

Gibson Marketing Group • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-655-5617 | F: 508-259-7962
www.gibsonmarketinggroup.com

The impact of information security incidents can be measured in dollars and cents

A large percentage of internal and external security incidents lead to substantial monetary losses. In addition to the mean reported out-of-pocket costs of more than $400,000, the time lost identifying and remediating the damage suggests the real cost is likely far greater.

"Well, I think in large part it's the environment that we face. We're seeing more and more attack factors. The threats are going up."
- Federal IT executive

"We're reactive. So if an incident occurs, we apply resources to it to make sure that whatever happened to the other guy doesn't happen to us."
- Federal IT executive

The federal government finds incidents end up with associated costs more often than private enterprise.

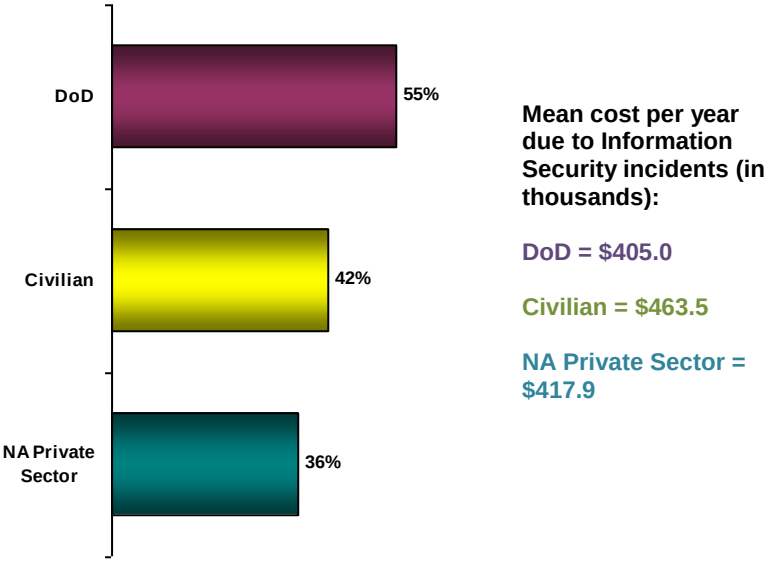

Fig. 6 - ***Percentage of internal and external security incidents resulting in financial costs or losses.***

Gibson Marketing Group • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-655-5617 | F: 508-259-7962
www.gibsonmarketinggroup.com

Internal threats equal or exceed external threats as a concern

External threats have long received primary attention, but while the risk is every bit as real, most agencies have mature systems and processes to address these problems. However, internal threat management is far less mature and constitutes a greater concern for many agencies. While layoffs drive increased concern about internal threats in private enterprise, the federal government does not experience layoffs in the same way. Instead IT reports a need to protect against innocent mistakes and overcome the "but our employees wouldn't do that" mentality to varying degrees.

"Typically a threat will come out of a vulnerability. So we have a very stringent USB drive policy and writing to removable media. If we allow somebody to do some things to circumvent that control, then we have a vulnerability in our control that has introduced a threat to our environment."
- Federal IT executive

"The point (is), if you lose a handgun, you have 24 hours to report it. If you lose a computer that has PII data on it, you have one hour to report it."
- DoD IT executive

About 10 percent of agencies reported more internal and external incidents over the previous year.

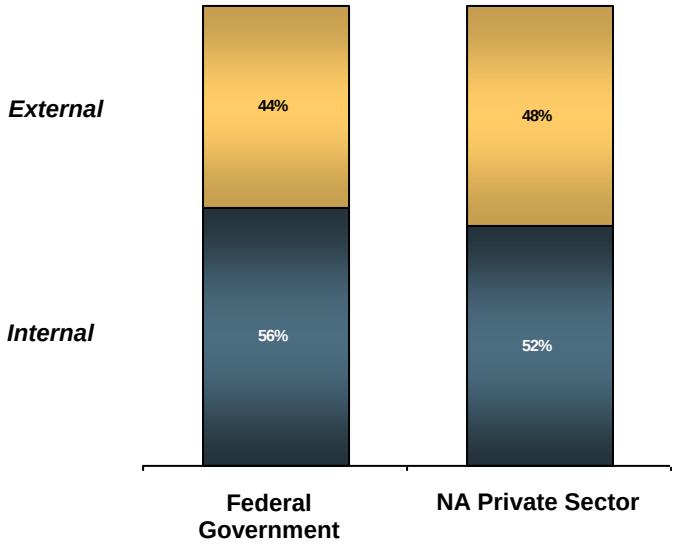

Fig. 7 - ***Agencies and companies reporting the percentage of greater perceived threat from internal or external incidents.***

Gibson Marketing Group • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-655-5617 | F: 508-259-7962
www.gibsonmarketinggroup.com

Budgets increase with the rate of incidents

Increases in security breaches force greater spending on prevention and remediation. All agencies privately acknowledge that there are constant internal and external threats.

Respondents who reported an IT security budget increase also reported a higher number of internal and external incidents than respondents whose budgets stayed the same.

"I've been getting very sizeable increases both in staffing and budget, and owe a lot to the VA and their incident. Even though it caused us a lot of pain, it also opened a lot of eyes."
- Federal IT executive

Those with increasing security budgets have three times more incidents than those whose budgets are decreasing.

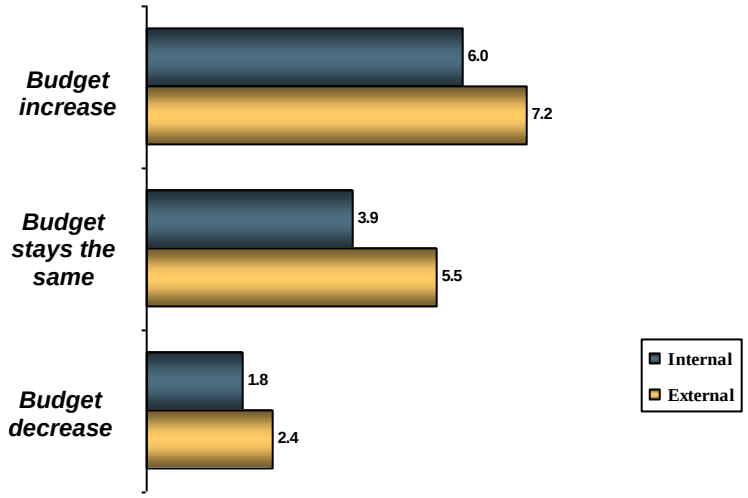

Fig. 8 – *Mean number of internal and external incidents correlates with IT security budget plans.*

Most agencies have experienced audit failure for IT security issues

IT executives express a great deal of frustration with the time and work associated with audits and the increasing prospect that, despite those investments, remediation will surely follow. Between internal and external audits, failure has occurred for more than 50 percent of the agencies surveyed (See Fig. 9). The external failures are striking because internal auditors are charged with preventing the possibility of external audit issues.

Gibson Marketing Group • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-655-5617 | F: 508-259-7962
www.gibsonmarketinggroup.com

Those failures (shown in Fig. 10) have a direct impact on increased IT security budgets.

"[We answer to] the OMB. If we don't have our systems certified (by them) we don't get funding. They will shut us off if we do not have a system. [They] do not accredit it. They will not fund." - Federal IT executive

"Every year, we file annual reports and then a Congressional committee compiles those reports and issues a report card for every agency, usually in the Spring. And several of the CIOs of the lower-ranking organizations are summoned up to Capitol Hill for a sound beating, a public beating. Nobody wants to be the guy in the barrel." - Federal IT executive

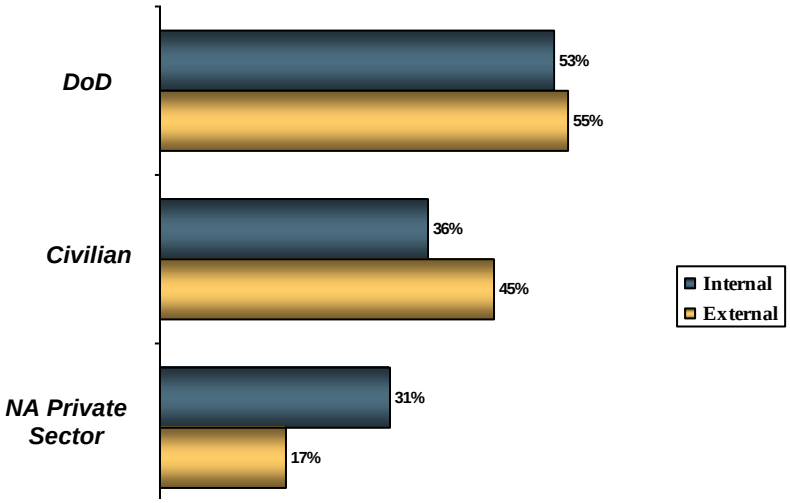

Fig. 9 - ***Percent of agencies failing an internal or external security audit over the last three years.***

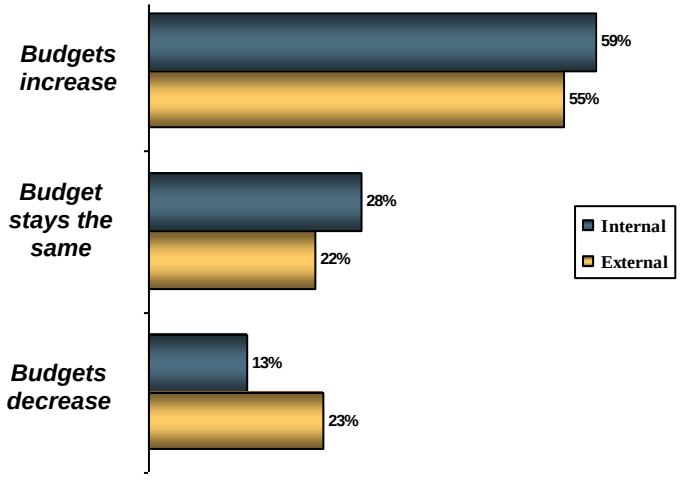

Fig. 10 – *Budgets correlated with failure of internal and external audits.*

Gibson Marketing Group • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-655-5617 | F: 508-259-7962
www.gibsonmarketinggroup.com

Strong demand for information security systems in the next 12 months

The drivers for federal interest in procuring automated solutions are many and explain the wide array of options being considered for immediate or near-term implementation. Data-loss prevention is top-of-mind. “Thumb” or flash drives are a particular concern for security in all agencies. Some report a desire to disable USB drives as a way to combat their use, although it is unclear how that would be accomplished.

Automated log management is on the list because IT can find no other way to perform the systematic reviews necessary to spot aberrant behavior before it becomes an irrevocable issue. IT (in particular IT audit) looks for security information management solutions that can produce compliance reporting from logs throughout the infrastructure.

Areas of strong interest include single sign-on, role-based provisioning, and Web security. Single sign-on and role-managed access are goals for all agencies.

“We’re all interested in making those solutions more rigid and more trustworthy. HSPD-12 is going to do a lot when it’s fully implemented in making agencies trust one another as to somebody’s identity. [That’s when] I can go to Homeland Security and they can trust the information that’s embedded in my HSPD-12 card, which it certainly wouldn’t do today.”
- Federal IT executive

“(Employees) are either promoted or they’re transferred, but they go from, say, our Economic Directorate to our Demographic Directorate. Having something that could track them as they move within our organization to ensure that they don’t retain access rights that they should not have when they’re moved is a key benefit.” - Federal IT executive

There is great interest in all categories of IT security solutions.

Gibson Marketing Group • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-655-5617 | F: 508-259-7962
www.gibsonmarketinggroup.com

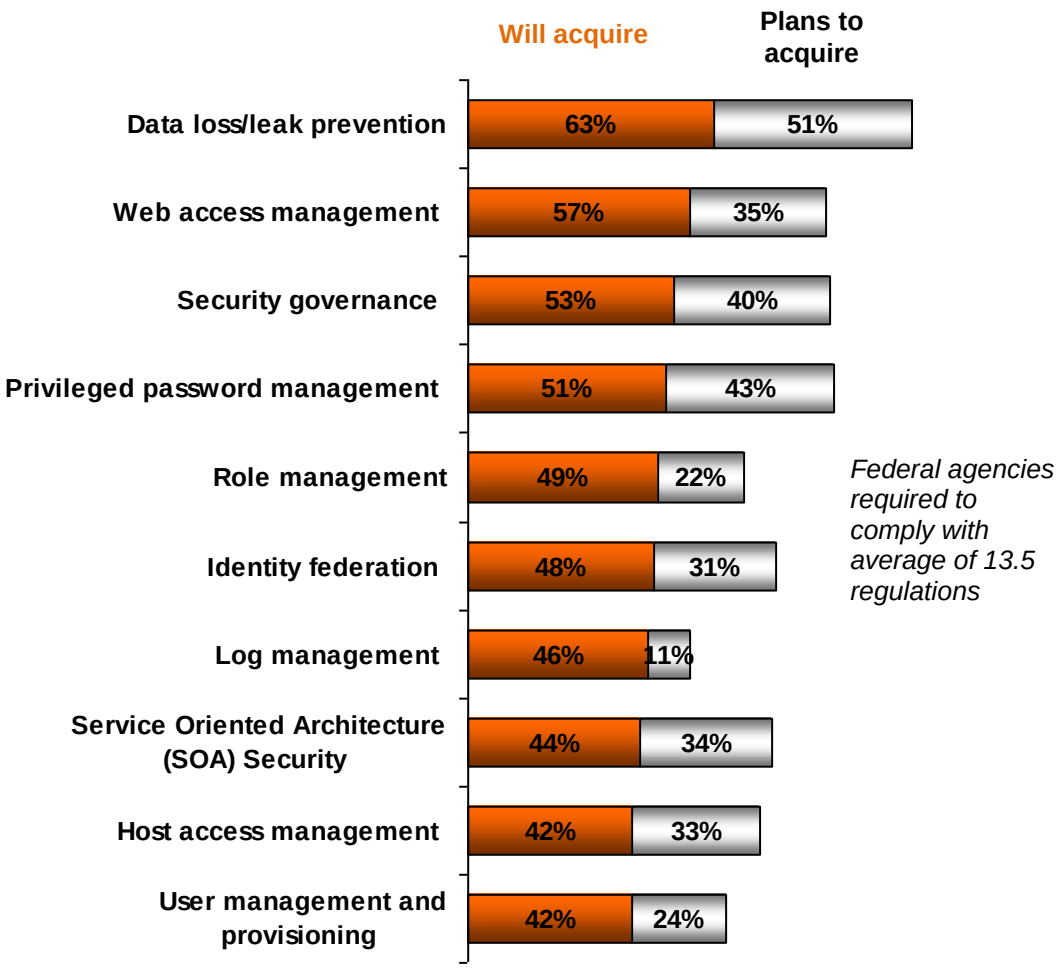

Fig. 11 – ***Percent of agencies looking to acquire automated information.***

Gibson Marketing Group • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-655-5617 | F: 508-259-7962
www.gibsonmarketinggroup.com

The federal government intends to acquire more security solutions than private enterprise will in the next 12 months

With the exception of log management, federal agencies cite a greater immediate intent to purchase the broad range of information security solutions available today. This may be explained by the perception held by federal IT execs that their groups lag those in private enterprise (see Fig. 12). While DoD has demonstrated a greater sense of need and is widely considered to be better-funded, the actual rate of purchase is very similar with some notable exceptions (see Fig. 13). For example, DoD's plans to buy identity federation, SOA security, and data-loss prevention solutions are significantly higher.

"The economy doesn't really drive us that much. What really drives us are the appropriations. So, in our half of the federal government that's been operating under a continuing resolution for the last six months at greatly reduced levels, that impacts what we've been able to do or not do. But now, alternatively, the appropriations was passed… There's going to be buckets of money flowing downhill that we have six months to execute."
- Federal IT executive

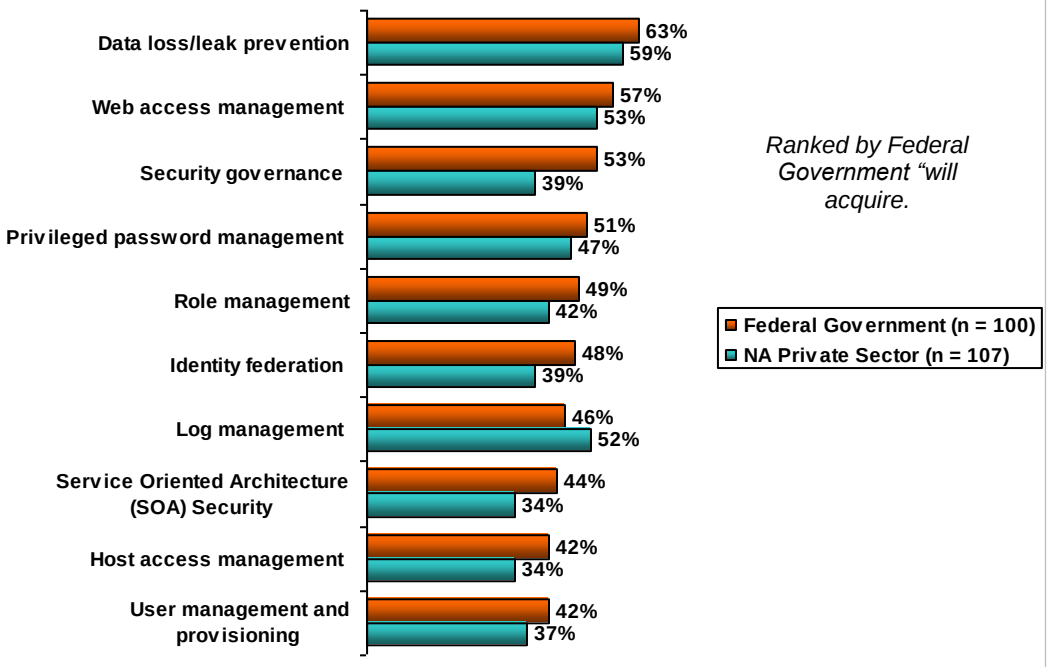

Fig. 12 - ***Comparison of federal agencies and North American companies looking to acquire automated information security solutions.***

Gibson Marketing Group • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-655-5617 | F: 508-259-7962
www.gibsonmarketinggroup.com

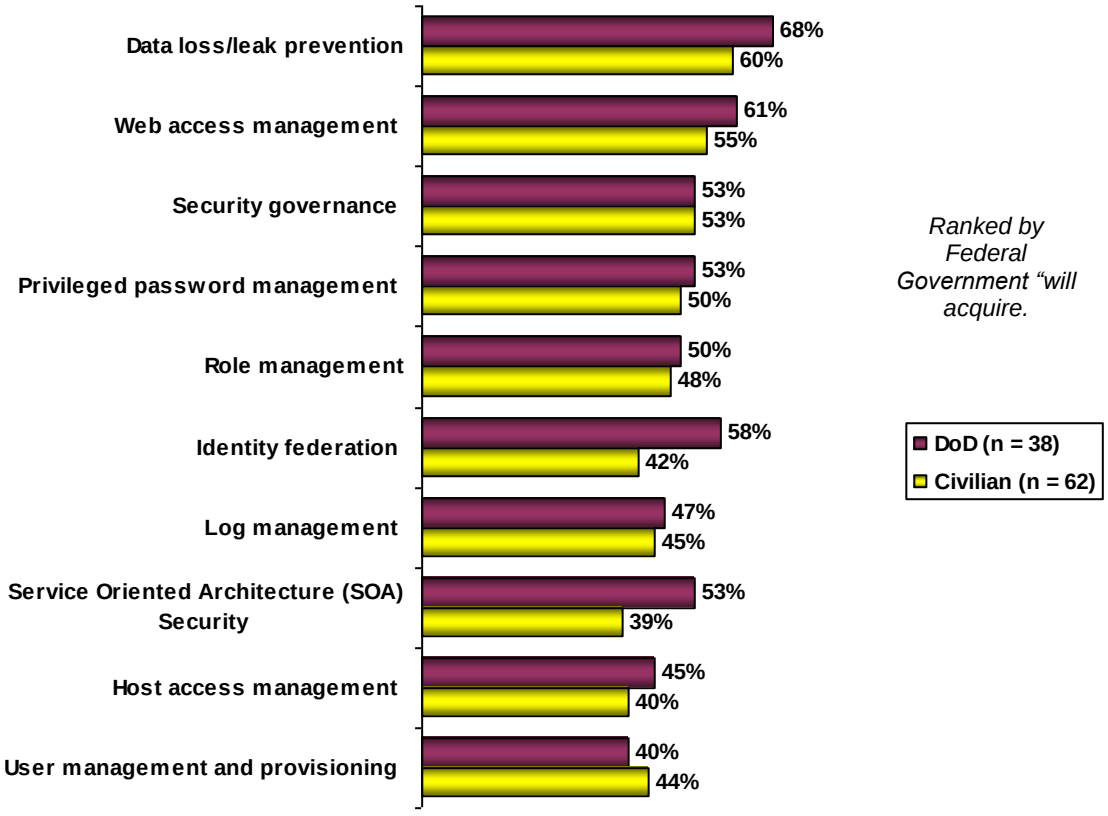

Fig. 13 - ***Comparison of planned acquisitions by civilian and DoD agencies.***

Increased regulatory burdens and perceived vulnerability will continue to drive adoption of new information security solutions, outpacing even the needs in the private sector

In this current economic cycle, it takes imperative need or a definitive return on investment to gain budget support for IT initiatives - whether in the federal government or private enterprise. Information security passes the needs test for all federal agencies. And the need can be generally categorized as improved automation of processes to handle the increased level of internal threat and/or to improve regulatory compliance.

The comparative differences in need and spending intent between DoD agencies and commercial organizations is consistent and comports with the nature of their missions and funding. And it is clear that all agencies

anticipate the needs will grow unabated. Both DoD and civilian agencies are less likely to see decreases in security budgets compared to private corporations.

A broad range of security management tools will receive increased scrutiny as the push to remove manual processes and the need to perform more sophisticated security management prevail. Data-loss/leak prevention, user management and provisioning, single sign-on, role management, Web access management, and more will all see interest and adoption outpacing the rate of corporate IT (with log management being the lone exception). Despite the ever-present IT mandate to “do more with less,” security tools companies will see solid growth from their federal clients.

Gibson Marketing Group • 95 Nason Hill Road • Sherborn, MA 01770 P: 508-655-5617 | F: 508-259-7962
www.gibsonmarketinggroup.com