Government IT Security Survey Analysis

Prepared for GTRA and Tripwire

January 2014

In the following report, Hanover Research presents the results of the Government IT Security GTRA Member survey. The goal of the survey was to better understand how government IT security and compliance employees feel about the state of Federal IT security.

HANOVER RESEARCH

Table of Contents

FOREWORD

RESOURCE IMPACTS

The survey respondents identified funding as the biggest issue but the salience of funding what areas was not detailed. One critical shortfall that exists is in funding for on-going cyber education, training and certifications. Budgetary reductions and economic impacts cause a tradeoff between training and education and day to day work. Over 2012-2013 sequestration and budgetary reduction impacts had direct implications on reduction in training and educational resources available. The ability for our political leaders to collaborate with outcome focused objectives is essential in meeting policy and compliance requirements.

Within the Federal Government personnel face a trade-off between increased compulsory reporting requirements and executing tasks and activities to remediate deficiencies. This is directly related to executing actions that improve information assurance and protection. Increased reporting requirements shift work to gathering status and what-if analysis information and away from taking actions correct or remediate. As resources are reduced and compulsory reporting requirements either remain the same or increase the workforce is compelled to accomplish mandatory reporting requirements over and above performing what-if-analysis associated with potential resource (budget and personnel) reductions. The on-going challenges of making progress and implementing actionable plans (execution) from strategy to tactics, detracts from establishing and managing strategies and available resources. Agency CIOs and IT leaders continue to be challenged with the dynamics associated with compression of budgetary outlays and the ability to adjust outcomes based upon resources available. Both this study and fiscal year reductions in funding should provide a compelling catalyst to close the gap between the ability to take actionable steps to strengthen the future cyber security environment, inclusive of workforce and integrated information technology solutions, and lawmaker's actions for satisfactory funding and support to Federal Agencies and Departments. This collaboration is paramount to realize the Comprehensive National Cybersecurity Initiative (CNCI: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative).

EDUCATION, TRAINING AND METHODOLOGIES

The overall categories and responses in Appendix A point to some compelling issues and challenges. A major concern is lack of satisfactory education, training and development of the Federal workforce. This is and has been a resonating theme for over the past decade from leadership to technical expertise. Recent reports on cyber leadership expertise from the Pell Center for International Relations and Public Policy; recent media reports such as Federal Computer Week, "Is there a cyber-security workforce crisis?", October 2013; U.S. Government reports, professional publications and reports from Cutter, Gartner, GTRA studies continue to cite the need for increased leadership, management and technical acumen. What has not caught up, based upon my experiences, are actions and execution of planned strategies to close this gap.

The increased acumen and competencies of the Federal workforce is critical. The Federal workforce is the essential human capital investment that must continue to have the necessary training and application (applied learning) necessary to implement lessons learned, good practices and continuous improvement. While one respondent cited increased contractor support that is a short term perspective. The Federal Government executives and leaders must focus strategically on career-long learning and enhancement of the organic workforce. There has been a focus of educational institutions to increase and improve cyber security educational tracks in higher education, non-profit Certification bodies, U.S. Government and Military Department schools and curriculums. Questionable is whether the Agencies and Departments have a planned and executable strategic and tactical approach for the workforce. We must move from lessons observed to implementable lessons learned.

Recruiting college and university graduates with positive education and position requirements, and establishing a pipe line for on-going workforce replenishment is yet another essential component. Higher education is turning out graduates with requisite degrees which the U.S. Government must leverage. The challenge to the aforementioned is also linked to budget challenges. With budget decreases (such as sequestration impacts), Departments and Agencies cuts on size of workforce, and the nature of the U.S. Government personnel practices and inflexibilities, the younger workforce, which is the future, can often be in jeopardy of being let go. Of all the initiatives under the CNCI, initiative number six, "expand cyber education" is a corner stone. Not only must we have a cyber-workforce for today's challenges, we need them for our future, we must have a workforce that can leverage the tools and technologies and exploit methodologies from strategy to actionable tactics. These are the human resources that we must invest in and with an on-going plan for continuous educational and training improvement as threat sources continue to morph and seek vulnerabilities and exploitations.

Craig McComb,
Former Deputy CIO, Lifecycle Management Center, U.S. Department of Defense

EXECUTIVE SUMMARY AND KEY FINDINGS

INTRODUCTION

In October 2013, Hanover Research (Hanover) conducted a survey among GTRA members and contacts provided by Tripwire. By asking questions about Federal IT policies, security issues and progress, and challenges in implementing policies and solving problems, this survey aims to understand what government IT security officials think about the state of Federal IT security.

To qualify, respondents must be involved in a government security and compliance program. Hanover collected a total of 111 complete responses. This section presents a summary of key findings from the study, and the following sections contain response and segmentation breakdowns for each question in the survey. Hanover segmented the following categories:

- Are you an employee or contractor?
- Organizational role (Senior management, security, IT)
- Program role (Implementing programs, other)
- Does your agency have a sufficient budget? (Top 2 box, other)
- Has your agency made progress since 2012? (Top 2 box, other)
- Is your agency currently making progress? (Top 2 box, other)
- Contact source (GTRA or Tripwire)

SUMMARY

Government security and compliance employees feel insufficient funding is the biggest issue facing their agencies. Overall, those in management or oversight positions tend to be more optimistic about the state of Federal IT security than those in program implementation, security, or IT roles. IT security officials who believe their agency has sufficient funding or has been making progress are also more positive about their agency and overall Federal IT security. Security and compliance employees believe more funding, better informed leaders, and a more clearly defined strategic planning process are necessities. There is a widespread belief that the dysfunctional congress exacerbates these problems. Despite these challenges, in general, respondents think their agencies have done an “Average” or “Above Average” job of addressing security issues and managing risk.

KEY FINDINGS[1]

- Overall, the biggest complaint among government IT security and compliance employees is a lack of funding. Forty-five percent of respondents believe it is the greatest challenge their agency faces to successfully implementing cyber security programs, only 37 percent believe they have adequate resources to properly implement policy, and "More Funding" is the second most popular response to "What is the one thing Federal Security leaders should do to connect security to the agency mission?"
- Many IT security and compliance employees see the dysfunctional congress and poor governance in general as a major problem. Fully 43 percent agreed this is "the biggest security threat we face."
- The majority of IT security and compliance employees consider their agency's progress since 2012 in addressing IT security issues "Average" (41 percent) or "Above Average" (34 percent). Forty-five percent consider their agency's current cyber security risk management "Average", and 37 percent consider it "Above Average".
  - Over half (55 percent) of respondents believe government IT security has improved due to the administration's policies, 60 percent believe the new NIST framework will improve security, and 46 percent say they have seen reductions in risk due to continuous monitoring efforts.
- While almost half (47 percent) of GTRA members believe their agency cares more about compliance regulations than improving security, a majority (65 percent) still believe their agency follows industry standards and best practices.
- Most respondents' agencies (74 percent) have been affected by sequestration.

SEGMENTATION ANALYSIS

Organizational Role

- Senior Management
  - Most likely to believe continuous monitoring has succeeded in reducing their agency's risk (60 percent) and security has improved due to their agency's policies/actions. (75 percent)
- Security
  - More likely to give their agency's progress a poor grade
  - More likely than senior management to believe their agency cares more about meeting regulations than actually improving security (72 to 40 percent)
  - Most likely to have been impacted by sequestration (81 percent)
  - Least likely to believe continuous monitoring has succeeded in reducing their agency's risk (34 percent)

[1] For all questions with a Likert scale, the top two responses (aka "top 2 box") are counted.

- IT
  - Least likely to believe the NIST framework will result in improvements (36 percent)

Program Implementers (Compared to program overseers, definers, and reporters)

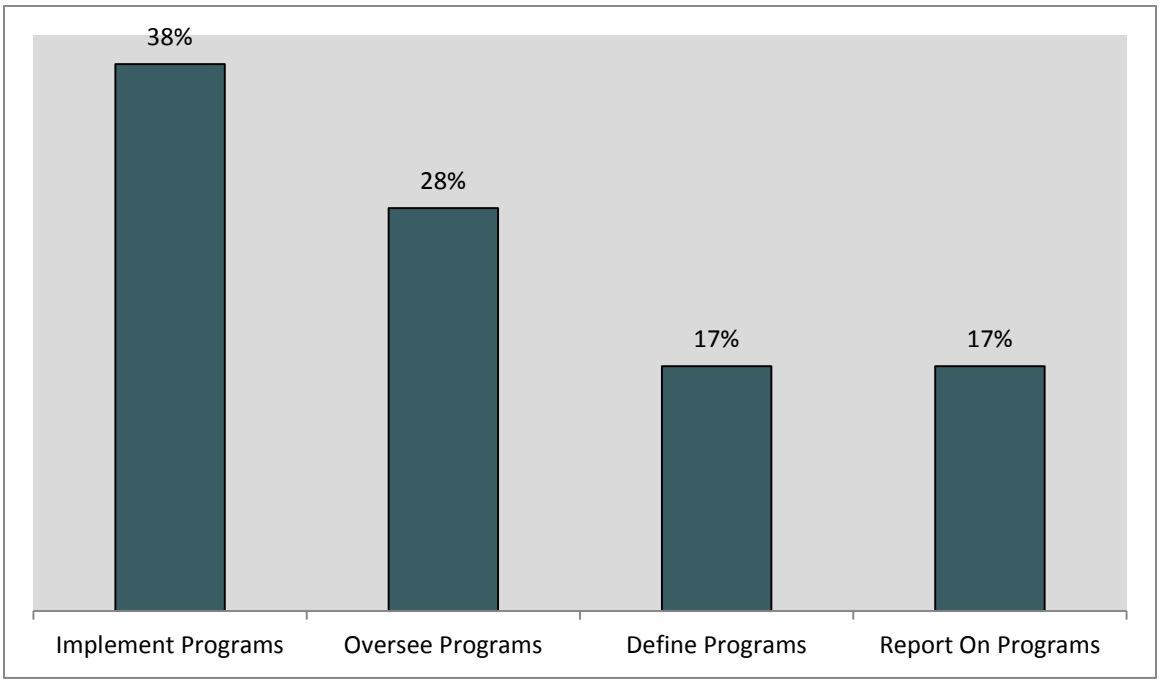
- Most likely to believe more qualified security employees are needed (28 to 11 percent)
- Less likely to believe security has improved due to their agency's policies/actions (36 to 65 percent)

GTRA Contacts (Compared Tripwire Contacts)

- More likely to believe in success of NIST framework (69 to 51 percent), continuous monitoring (52 to 40 percent), and overall success of government policies (69 to 37 percent).
- Less likely to believe agency cares more about compliance regulations than security (34 to 60 percent).

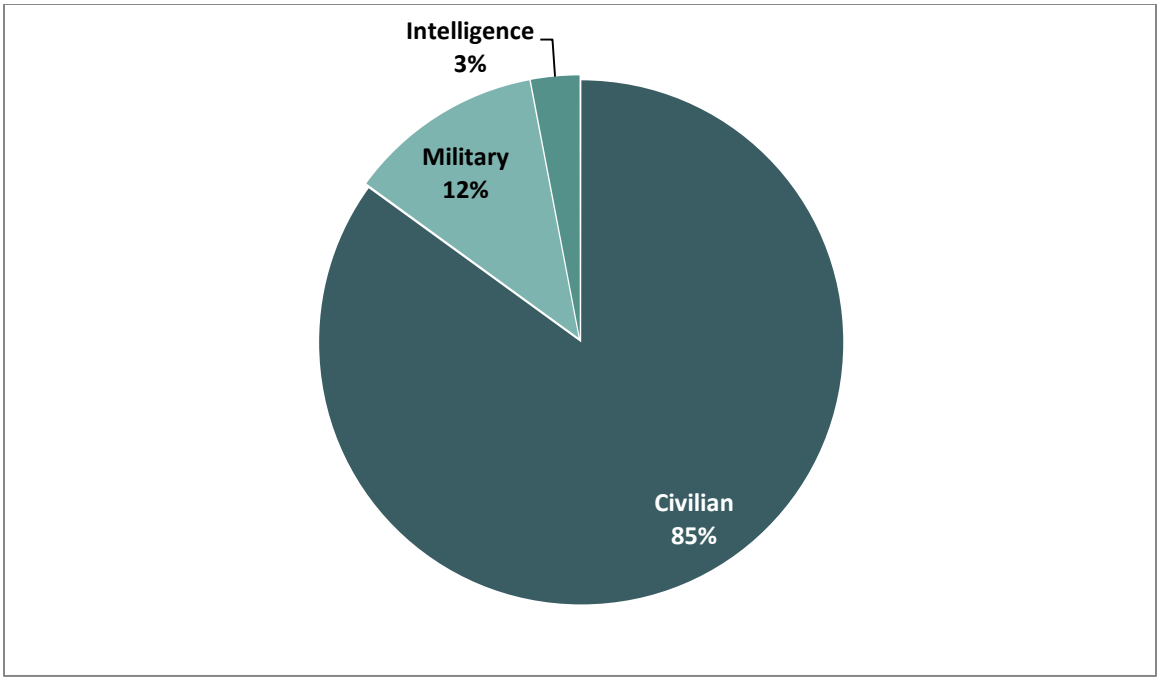
SECTION I: RESPONDENT CHARACTERISTICS

Figure 1.1: Please indicate your involvement in security and compliance programs in your agency.



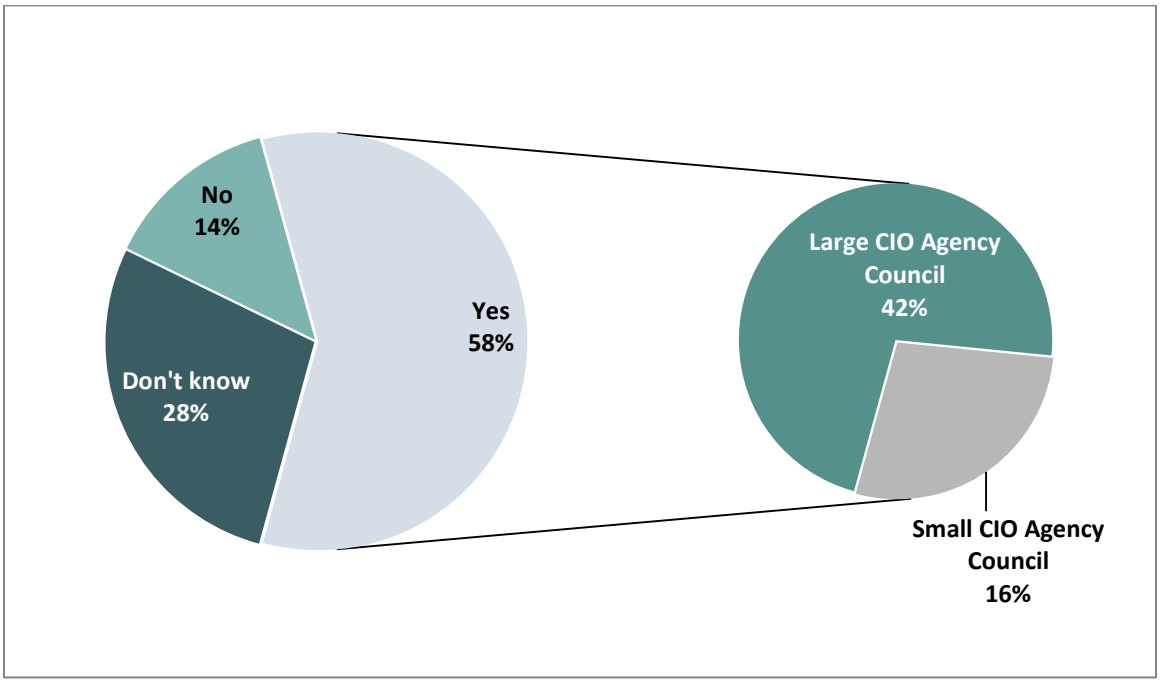
n=111

Figure 1.2: What part of the U.S. government do you work for?



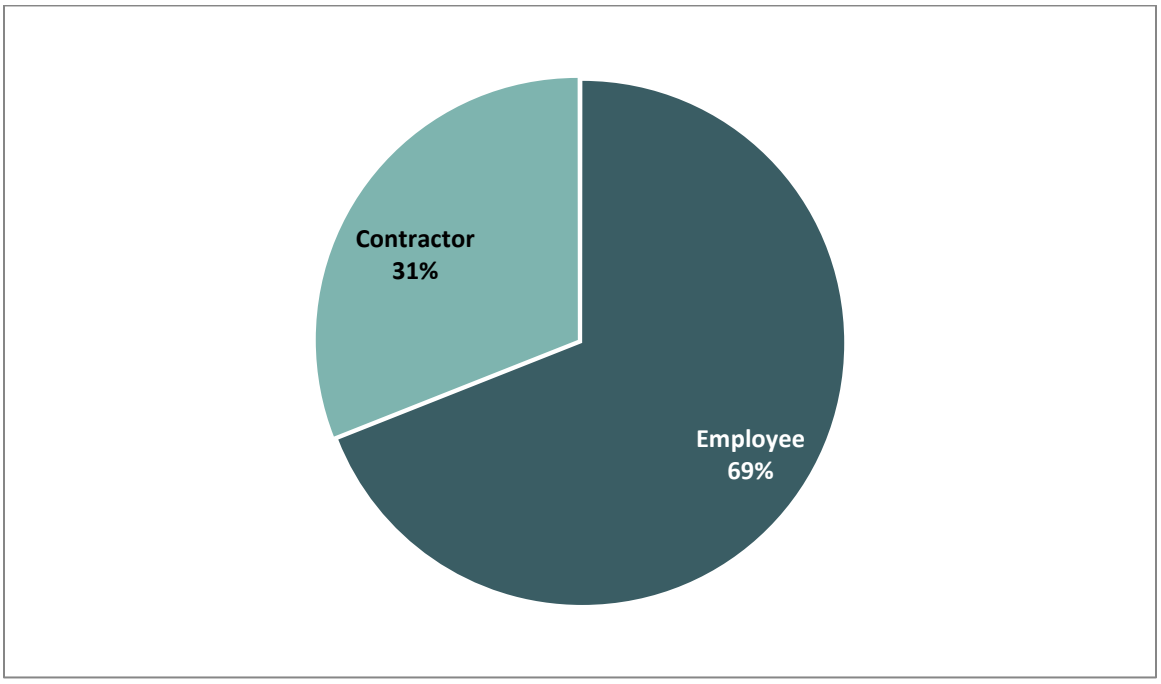
n=109

Figure 1.3: Is your agency represented on the Federal CIO council?



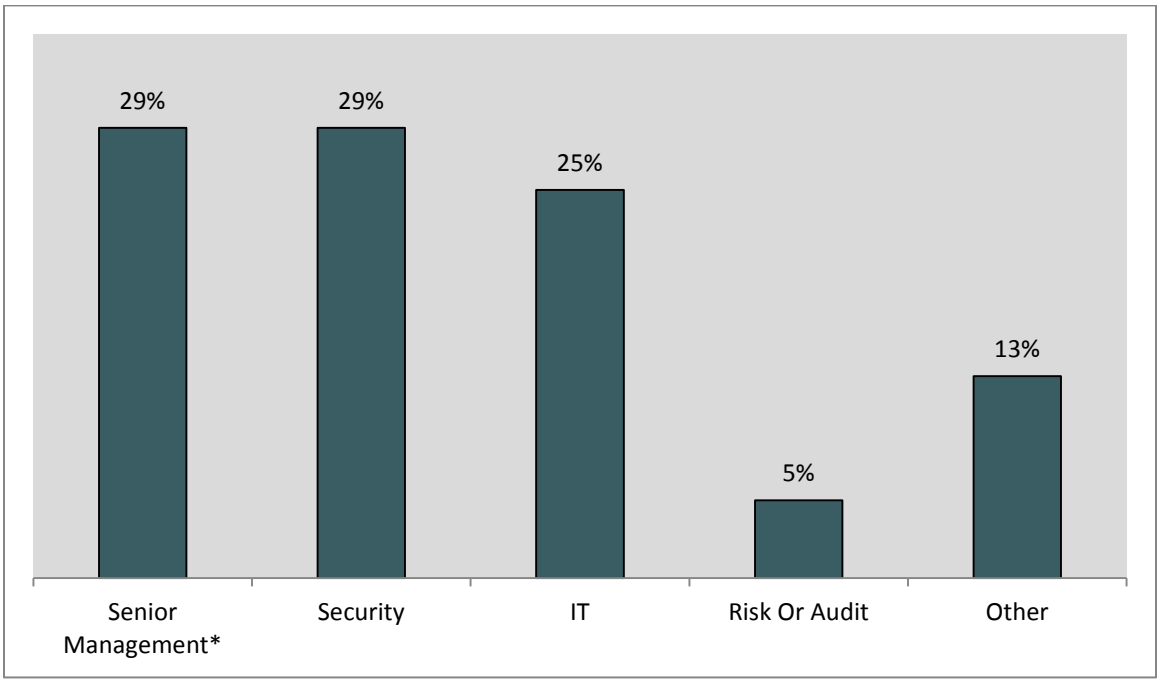
n=111

Figure 1.4: Are you an employee or a contractor?



n=110

Figure 1.5: What is your role within your organization?



n=111

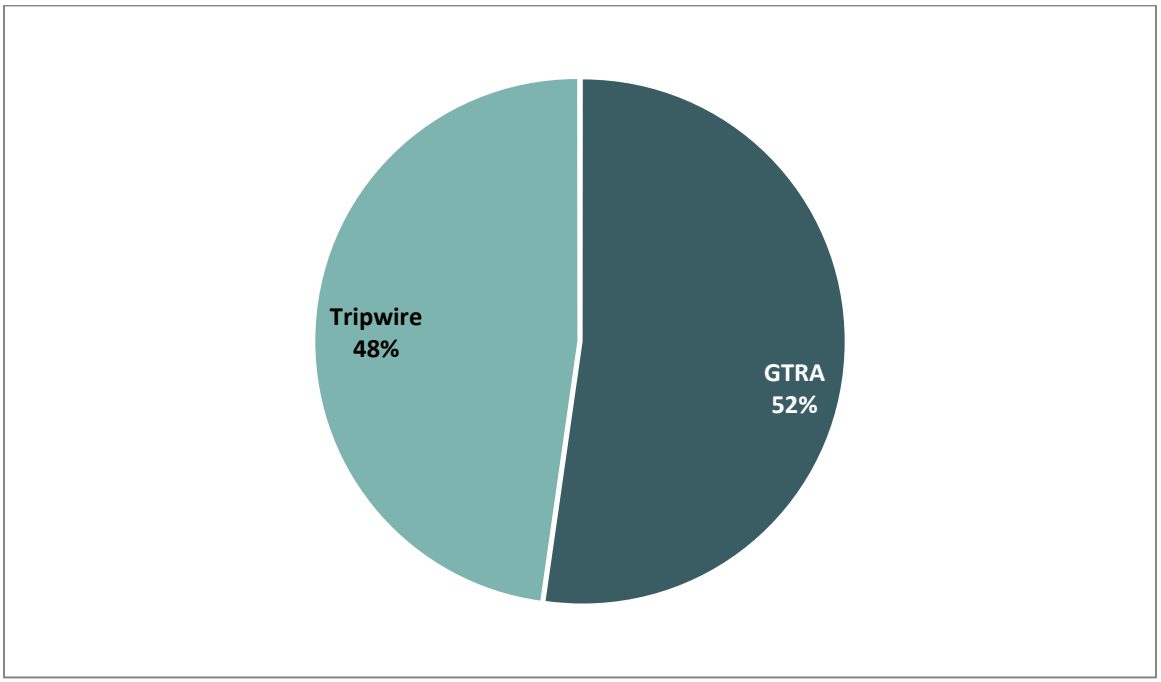
Figure 1.6: What is your role within your organization? Other

RESPONSE
CTO
Cybersecurity Workforce Development & Training
Developer
Enterprise Architect
Enterprise Architecture
General Management
IT Operations And Security
Privacy Officer
Program Manager
Program Office
Senior Advisor - Technology
Senior It Consultant
SSO
Staff, Work On Cybersecurity Education

n= 14

*CIO, CISO, Security operations council

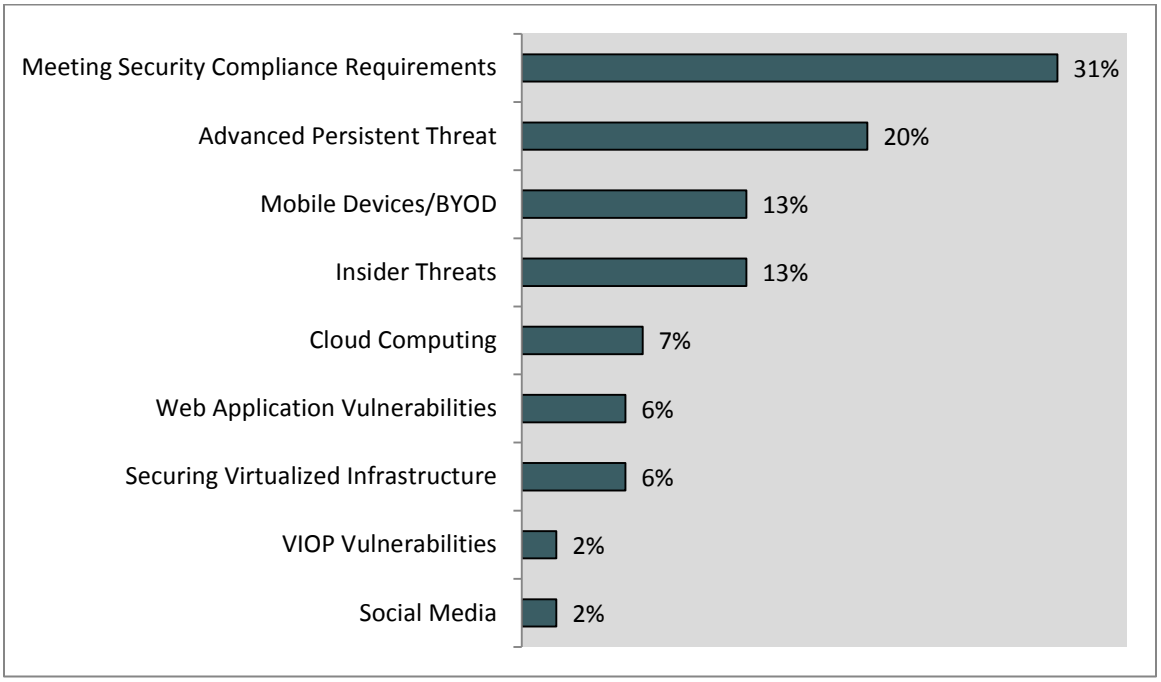
Figure 1.7: Contact Origination



n=111

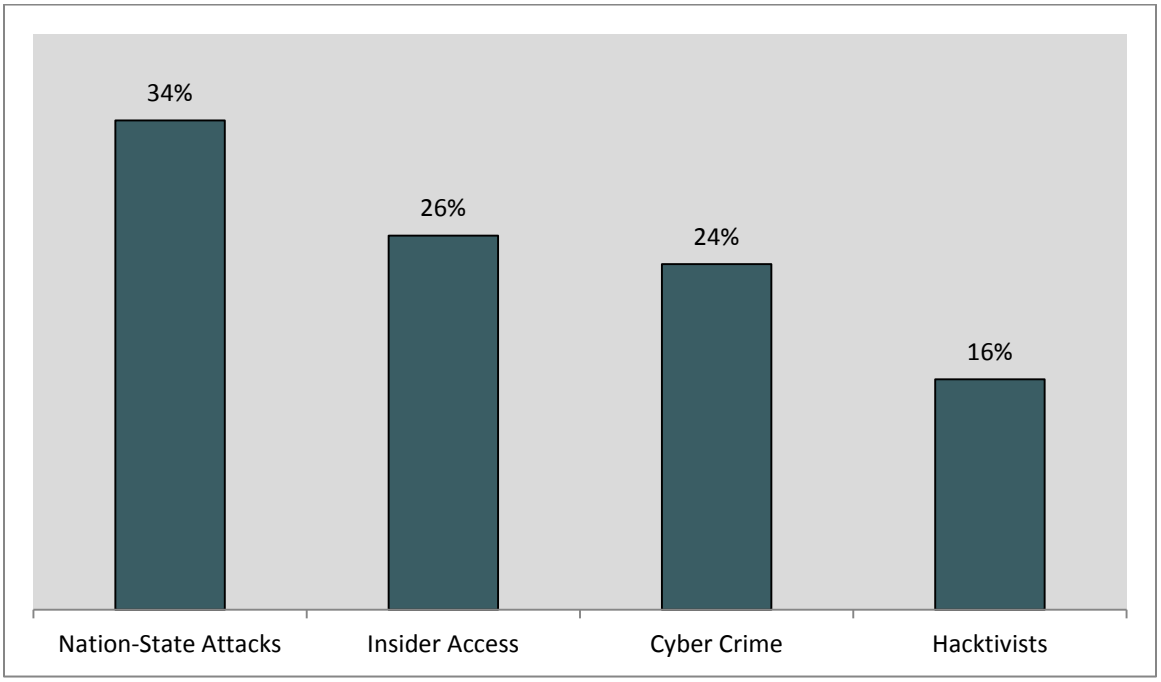
SECTION II: RESPONSE BREAKDOWN

Figure 2.1: What is your biggest security concern for FY 2014?



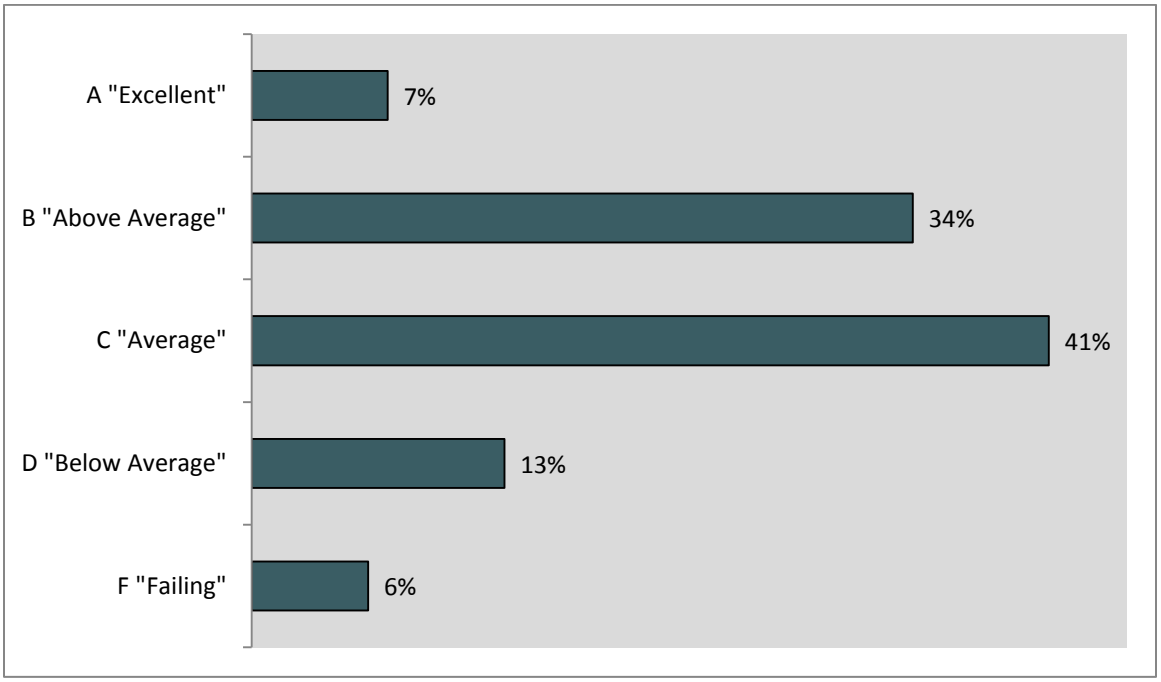
n=109

Figure 2.2: What is the most significant threat category you face?



n=106

Figure 2.3: How would you grade your agency's progress since 2012 in addressing these issues?



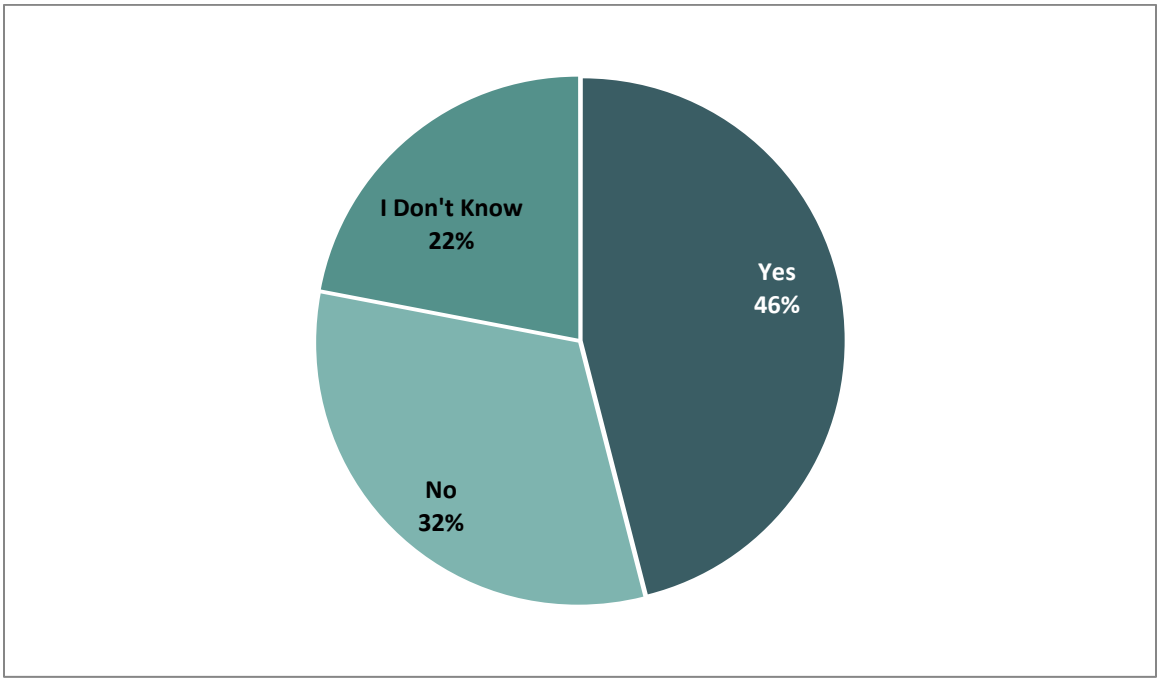
n=107

Figure 2.4: You said failing, can you please comment on why?

RESPONSES
Everything is broken. And, open to the whole world!
Insufficient resources. Inadequate skill sets.
No
No DoD policy regarding cyber securing ICS
Successful ATP attacks are escalating
Top Leadership feel and act as if it is not important

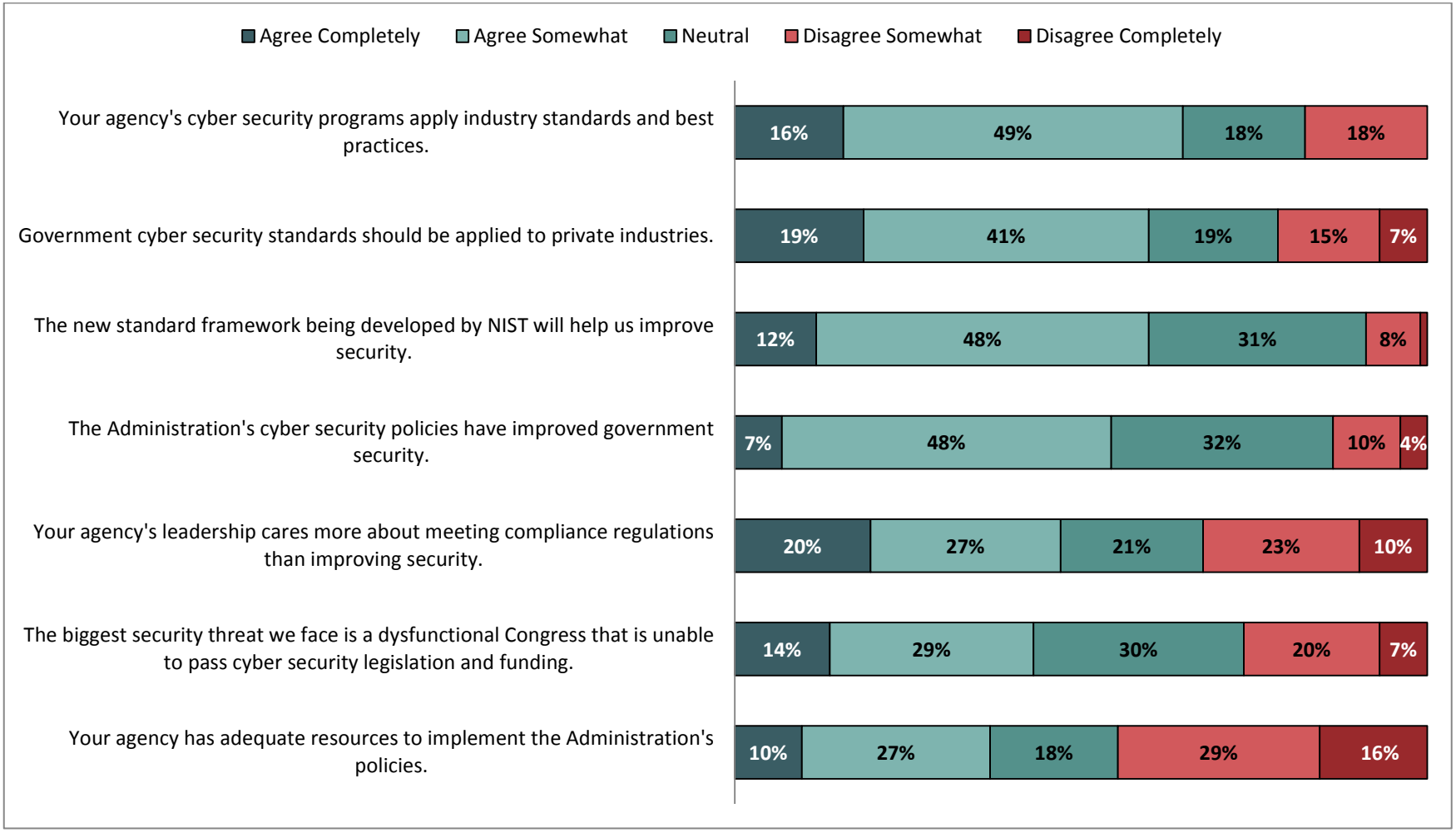
n=7

Figure 2.5: Have you seen measurable reductions in your agency's risk based on continuous monitoring efforts to date?



n=109

Figure 2.6: Rate your level of agreement with the following statements.



n=103

Figure 2.7: The Administration's cyber security policies have improved government security. You said you disagree; please comment on why.

CATEGORY	RESPONSES
No Tangible Difference Or Change	Don't see where there has been a difference
	Ineffectual
	Just more boxes to check and hoops to jump through. Very little in the way of real security progress.
	No measurable, real progress. Reporting is unreliable and shows successes that are not rooted in reality.
	No tangible impact thus far.
Not Addressing Correct Threats	Cyber IT policy not addressing cyber ICS
	Inconsistency and not focused on the problem
	It seems that we are always playing catch-up on threats that seem to be coming which are more advanced than we are.
	Recent events of PII being compromised.
Polices Are Too Vague	Vague policy. Needs to be requirement driven and adequately resourced. Can't pass comprehensive Cyber Laws.
	Vague, unfunded policy guidance is useless.
Too Much Bureaucracy/Red Tape	Many Bills sit in Congress and not passing. There has been no progress in the last 3 years.
Other	Focus is on
	It's all a false truth!

n=14

Figure 2.8: The biggest security threat we face is a dysfunctional Congress that is unable to pass cyber security legislation and funding. You said you agree; please comment on why.

CATEGORY	RESPONSE
Lack Of Necessary Funding And Regulation	Agencies know what needs to be done to improve security across their enterprises; agencies lack funding.
	Congress' failure to pass scty leg and to do budgets increases uncertainty about how to act and what funds will be available now and in the future. This uncertainty means we can't contract for support as contractor support is essential to obtaining the needed advanced IT skills. When we can't contract until CR is over often in the middle of the year and don't know if we will have funds in the following year due to the do nothing congress we end up not doing or doing poorly what we could do well
	Delay in Security funding and policy will be the shortfalls for which Cyber security will be attempting to overcome.
	Focus is on checking boxes for compliance while funding is lost for real world persistent threats.
	Funding/manpower
	Inadequate funding; politics getting in the way of good decision making
	Lack of funding to harden infrastructure
	Legislation and funding are essential. Senate has not passed a budget. How many crs have we been working under?
	Perennial problem with legislators not tying enough funding to address issues of oversight. They recognize the problem but are often unwilling to pay for it...
	Resources are required to investigate the ICS scope and mitigate vulnerabilities

	Sequestration; budget delays; furloughs and funding tied to unpassed legislation
	There is never enough resources expended on infrastructure
	Uncertainty if funds and personnel will be available to carry out security mission
	We have been waiting for years for legislation to help the issue.
	We have smart people in agencies who can implement -- they need the legislative & regulatory framework, plus dependable funding sources
Congress Is Ineffective and Ill-Informed	This congress is useless in getting anything done
	Bi-partisan politics have replaced effective government
	Congress can't get it together
	Congress has not fulfilled its role in government and has ignored the Constitution.
	Congress is ineffective
	Congress is owned by lobbyists
	Good security begins with good governance
	Ignorant of IT!
	Infrastructure attack is going to happen and Congress can get its act together
	Politicians do not understand Cyber Security to an adequate level
	The current congress is focused on party politics.
	The fact is, they are not passing anything - cyber related or otherwise
	There seems to be a need to create legislation without getting it passed. Too many laws say the same thing but accomplish little.
	They seem to be unable to do agree on anything, except how to take for themselves.
	They waste time and money arguing rather than doing something meaningful and haven't passed an actual budget for years.
	Government Shutdown....need I say more
Other	Congressional Laws would be policy drivers. Should be tied to Trade Law.
	Government want's cloud, yet won't provide us with the solutions to make it happen quickly.
	Investment in providing training environments to improve skills, lack of accountability for malicious actors and failure to punish companies that practice poor hygiene. No mandate requiring secure coding of critical information systems
	It is a huge threat, but not the biggest.
	Many organizations will not implement security without directives dictating them.
	Needs to be bigger than just the U.S.
	Only obvious answer provided
	Past behavior as a predictor of future
	The need for Congressional Laws to protect Cyber security is needed.
	What level of experience do they have to do so ??? Are they working together?

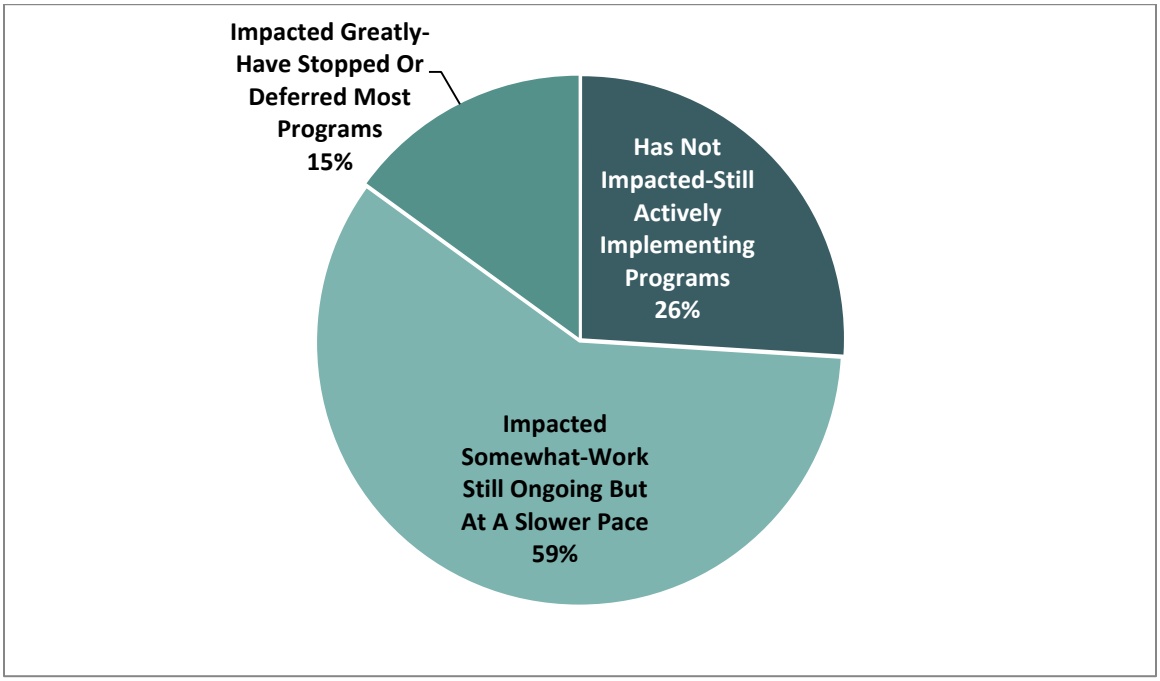
n=41

Figure 2.9: The new standard framework being developed by NIST will help us improve security. You said you disagree; please comment on why.

CATEGORY	RESPONSE
Will Not Actually Address Issues	I see no relation of NIST compliance to security improvements.
	It has no teeth
	NIST = bloat w/ little added value.
	NIST updates are becoming like new product updates and are not significantly addressing real risk since the auditors still are stuck on compliance more than they are on true risk. Also, the overall FISMA process has created an undue burden on the agencies that distracts us from concentrating on real risk - instead, we have an annual compliance audit that is becoming increasingly time consuming.
Lack Of Standard Framework Not The Biggest Issue	People are the biggest risk, not standards or frameworks
	The new framework will simply create a new compliance regimen
	There is no one-size-fits-all solution.
	Tools/frameworks by themselves don't improve security
	We do not need more regulations
Other	Has it been tested? New s

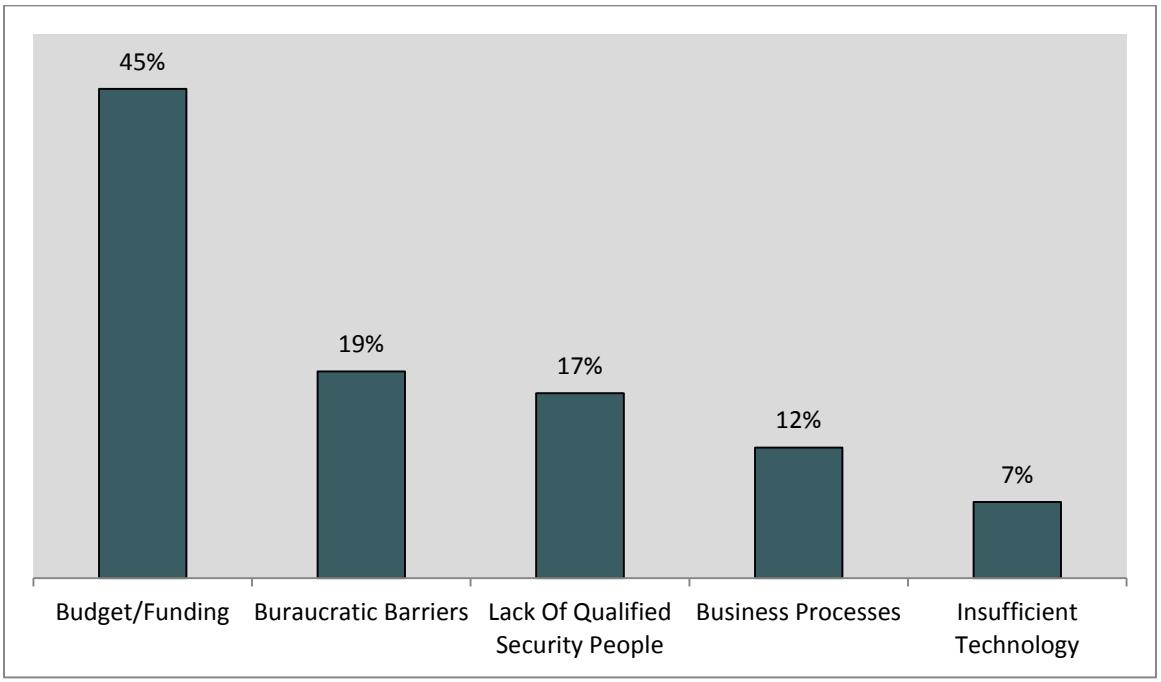
n=10

Figure 2.10: How much impact has sequestration had on implementing cyber security programs in your agency?



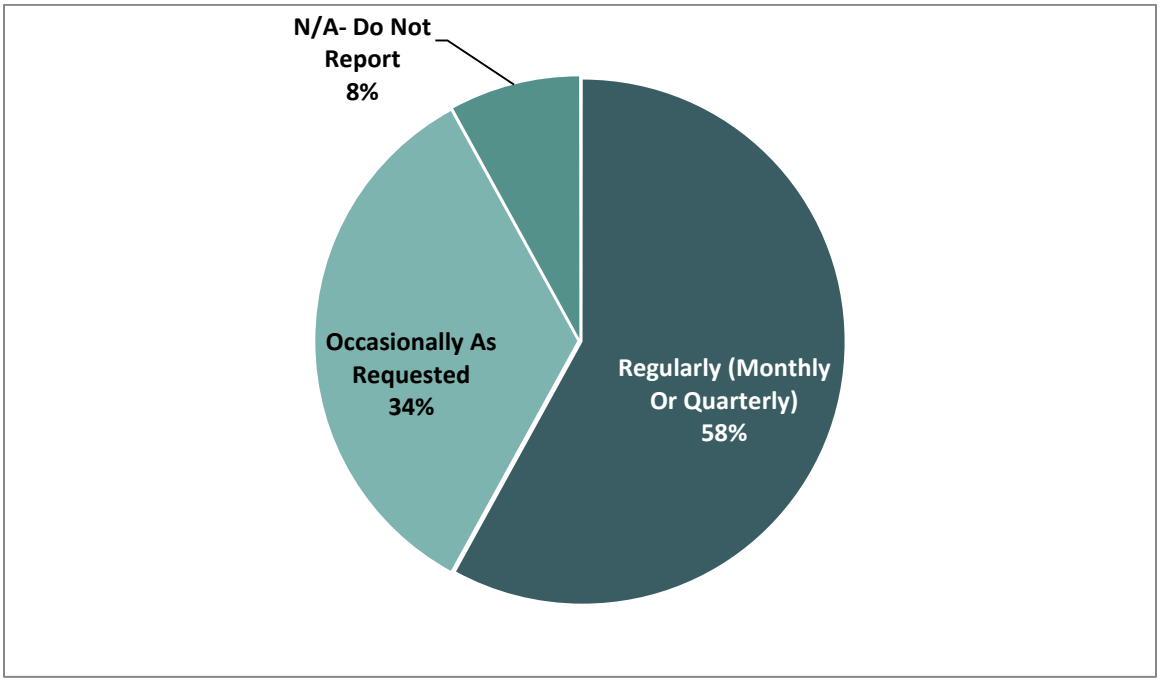
n=103

Figure 2.11: What is your agency's greatest challenge in implementing cyber security programs?



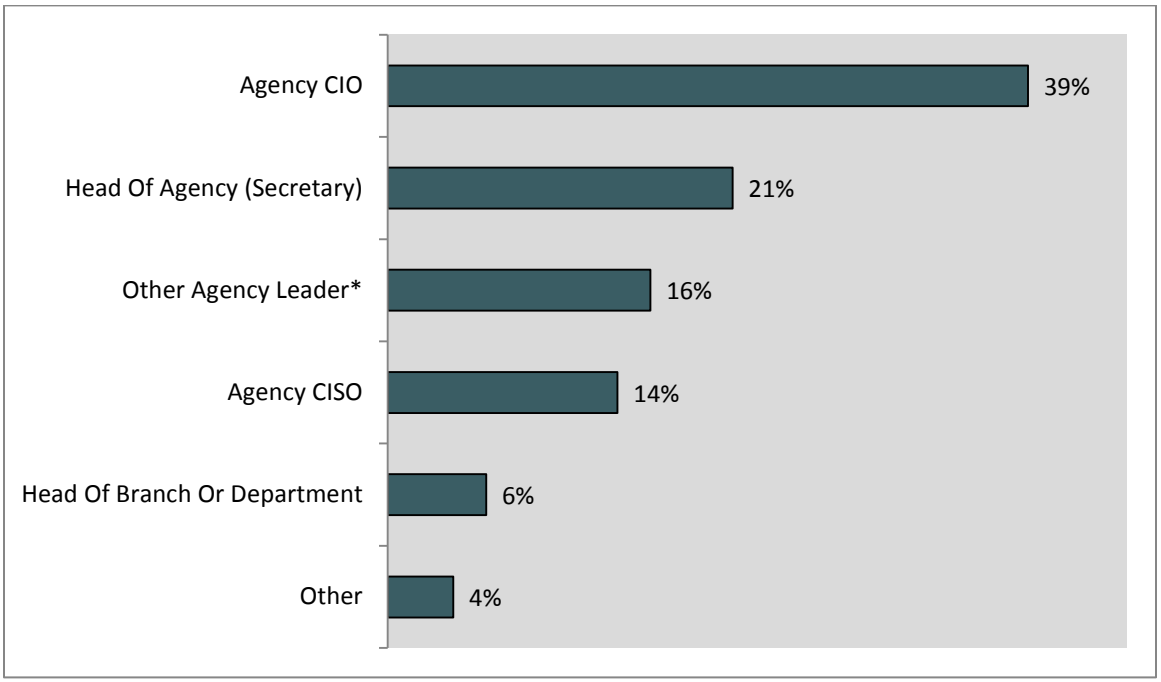
n=103

Figure 2.12: How often does your agency report to its executive leadership about cyber security?



n=101

Figure 2.13: What is the highest management level in the agency that receives regular reports on cyber security?



n=100

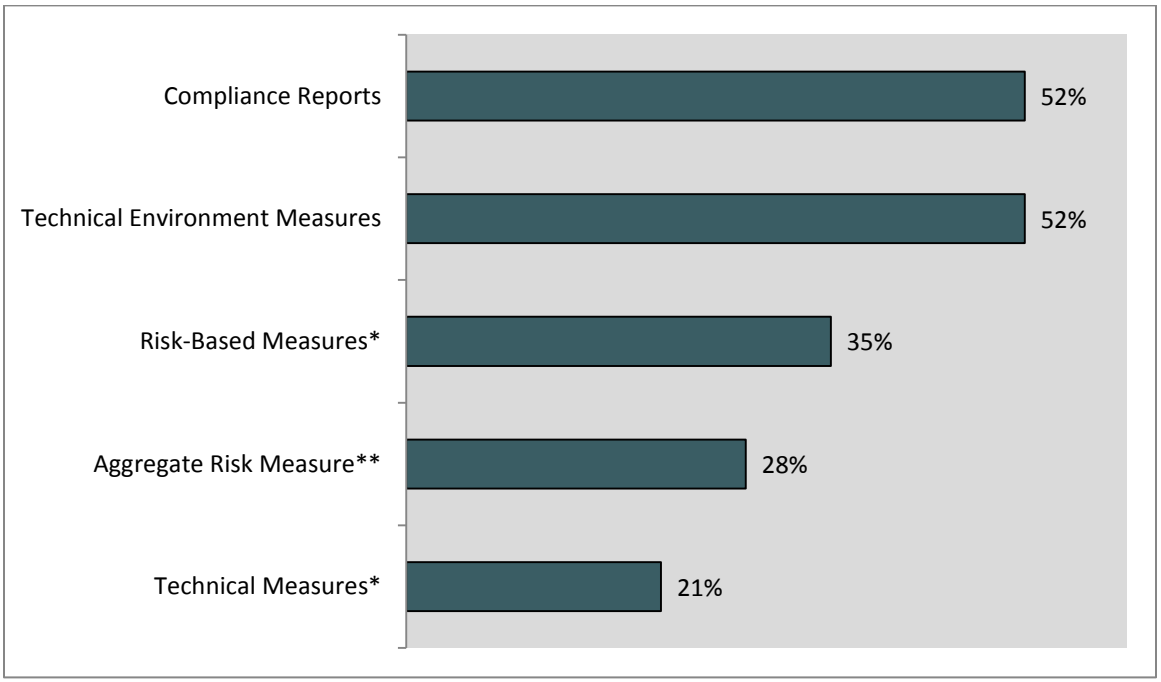
Figure 2.14: What is the highest management level in the agency that receives regular reports on cyber security? Other

RESPONSES
Authorizing Official
I don't know
It is not reported
No real reporting

n=4

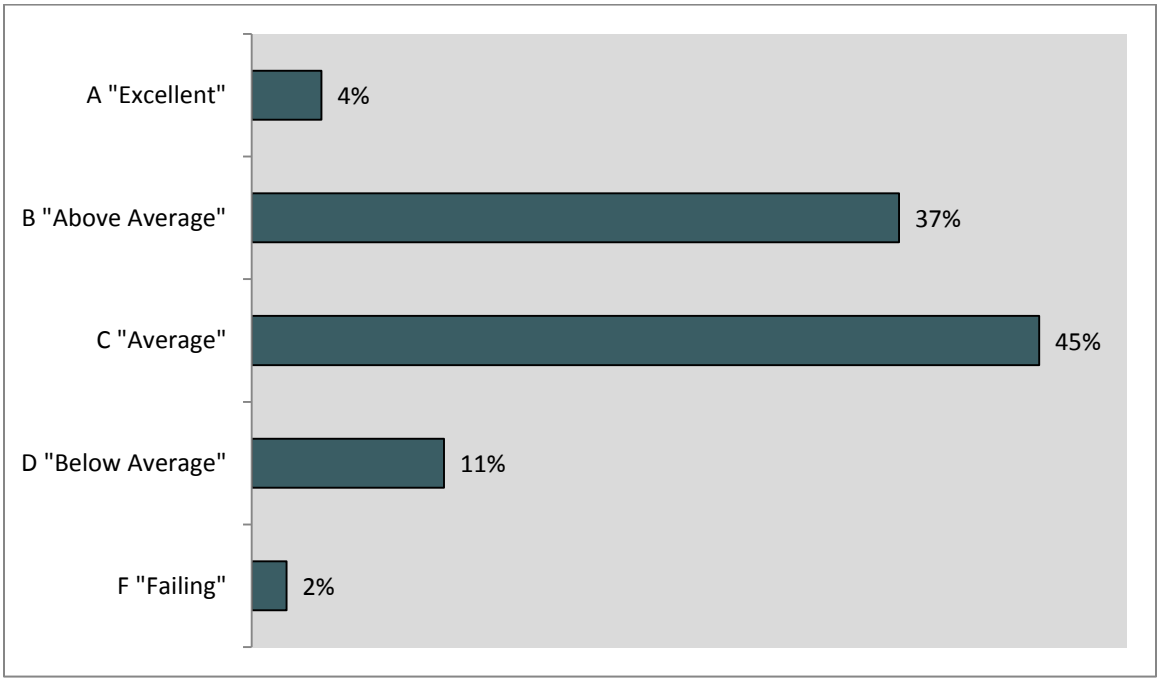
* Assistant Secretary, Under Secretary

Figure 2.12: Which types of measures do you use most often to communicate to executives? (May select multiple answers)



n=99

Figure 2.13: How would you grade your agency's average cyber security risk management at this time?



n=99

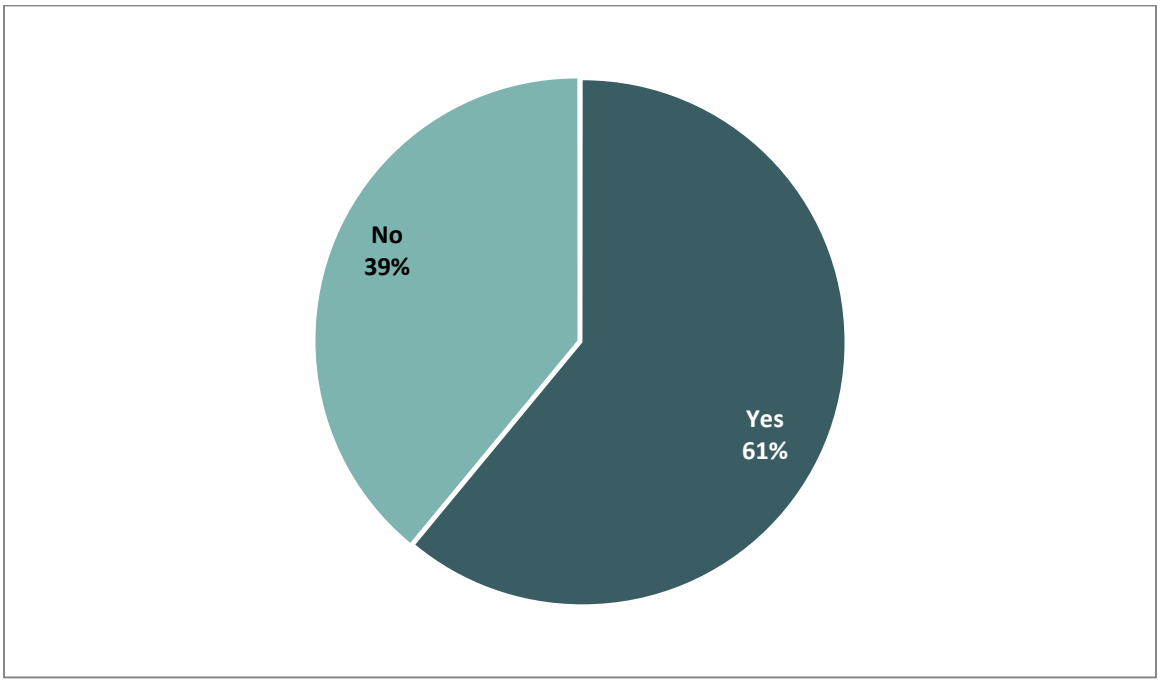
* By department or functional area
** For agency

Figure 2.14: Can you please comment on why you said failing?

RESPONSES
It is seen as not important
Risk is increasing and agency's ability to respond to threats is decreasing.

n=2

Figure 2.14: Does your executive reporting relate current cyber security risk to potential impact on the agency's mission?



n=96

Figure 2.15: In your opinion, what is the one thing Federal Security leaders should do to connect security to the agency mission? (Coded, top responses only)

n=87

SECTION III: SEGMENTATION[6]

Figure 3.1: What is your biggest security concern for FY 2014?

	Contractor	Employee	Organizational Role			Program Role		Sufficient Budget[7]		Progress[8]				Website	
			Senior Management	Security	IT	Implementation	Other	Top 2	Other	Since 2012		Current		Tripwire	GTRA
										Top 2	Other	top 2	Other		
N=	34	74	30	23	28	41	68	38	65	43	64	41	58	53	56
Advanced persistent threat	21%	20%	30%	28%	7%	20%	21%	29%	17%	12%	27%	20%	22%	19%	21%
Cloud computing	6%	8%	7%	3%	4%	5%	9%	11%	5%	9%	6%	7%	7%	4%	11%
Insider threats	12%	14%	27%	13%	4%	7%	16%	11%	14%	19%	9%	20%	9%	11%	14%
Meeting security compliance requirements	35%	30%	20%	34%	32%	32%	31%	13%	40%	28%	33%	22%	36%	36%	27%
Mobile devices / BYOD	9%	15%	7%	13%	21%	22%	7%	13%	14%	9%	16%	10%	16%	11%	14%
Securing virtualized infrastructure	9%	3%	3%	0%	11%	2%	7%	8%	5%	5%	6%	2%	7%	4%	7%
Social media	0%	3%	0%	0%	7%	5%	0%	3%	2%	2%	2%	2%	2%	4%	0%
VOIP vulnerabilities (Vishing)	3%	1%	0%	0%	7%	2%	1%	3%	0%	2%	0%	2%	0%	2%	2%
Web application vulnerabilities	6%	7%	7%	9%	7%	5%	7%	11%	5%	14%	2%	15%	2%	9%	4%

[6] Segmented results were tested for significant differences at the 95% confidence level. Segmentation tables display these differences through the use of cell shading. Within each segment, cells with dark blue shading are significantly higher than cells with light blue shading. (E.g., Senior management is significantly more likely than IT to be concerned about insider threats (27 to 4 percent)). Orange shading simply displays relative value (i.e., the darker the cells are, the higher the value is).
[7] Top 2 refers to the top 2 responses, "Agree Completely" and "Agree Somewhat".
[8] Top 2 refers to the top 2 responses, "A 'Excellent'" and "B 'Above Average'".

Figure 3.2: What is the most significant threat category you face?

	Contractor	Employee	Organizational Role			Program Role		Sufficient Budget		Progress				Website	
			Senior Management	Security	IT	Implementation	Other	Top 2	Other	Since 2012		Current		Tripwire	GTRA
										Top 2	Other	top 2	Other		
N=	33	72	29	31	28	40	66	38	62	42	62	39	58	51	55
Cyber crime	21%	25%	17%	19%	29%	20%	26%	24%	19%	26%	21%	18%	22%	25%	29%
Hacktivists	9%	19%	17%	16%	14%	15%	17%	18%	15%	14%	16%	26%	10%	16%	15%
Insider access	30%	25%	28%	23%	29%	33%	23%	24%	29%	38%	19%	31%	26%	26%	24%
Nation-state attacks	39%	31%	38%	42%	29%	33%	35%	34%	37%	21%	44%	26%	41%	34%	33%

Figure 3.3: How would you grade your agency's progress since 2012 in addressing these issues?

	Contractor	Employee	Organizational Role			Program Role		Sufficient Budget		Progress		Website	
			Senior Management	Security	It	Implementation	Other	Top 2	Other	Current		Tripwire	GTRA
										Top 2	Other		
N=	33	73	30	32	27	40	67	38	64	40	58	53	54
A "Excellent"	6%	7%	10%	3%	7%	5%	7%	13%	3%	18%	0%	7%	7%
B "Above Average"	33%	34%	33%	31%	37%	35%	33%	34%	31%	53%	19%	34%	33%
C "Average"	36%	42%	40%	38%	41%	35%	45%	39%	42%	25%	53%	41%	43%
D "Below Average"	15%	12%	10%	22%	11%	18%	10%	8%	17%	3%	21%	8%	11%
F "Failing"	9%	4%	7%	6%	4%	8%	4%	5%	6%	3%	7%	3%	6%

Figure 3.4: Have you seen measurable reductions in your agency's risk based on continuous monitoring efforts to date?

	Contractor	Employee	Organizational Role			Program Role		Sufficient Budget		Progress				Website	
			Senior Management	Security	IT	Implementation	Other	Top 2	Other	Since 2012		Current		Tripwire	GTRA
										Top 2	Other	top 2	Other		
N=	34	74	30	32	38	41	68	38	65	43	64	41	58	53	56
Yes	50%	45%	60%	34%	46%	41%	49%	53%	40%	70%	28%	63%	33%	40%	52%
I Don't Know	12%	26%	10%	16%	32%	24%	21%	16%	26%	14%	28%	17%	24%	21%	23%
No	38%	30%	30%	50%	21%	34%	31%	32%	34%	16%	44%	20%	43%	40%	25%

Figure 3.5: What is your agency's greatest challenge in implementing cyber security programs?

	Contractor	Employee	Organizational Role			Program Role		Sufficient Budget		Progress				Website	
			Senior Management	Security	IT	Implementation	Other	Top 2	Other	Since 2012		Current		Tripwire	GTRA
										Top 2	Other	top 2	Other		
N=	32	70	28	32	25	39	64	38	65	40	62	41	58	52	51
Budget/funding	44%	44%	50%	31%	56%	44%	45%	37%	49%	48%	42%	41%	48%	40%	49%
Bureaucratic barriers	19%	20%	14%	28%	20%	21%	19%	18%	20%	10%	26%	17%	19%	21%	18%
Business processes	9%	13%	14%	13%	4%	5%	16%	16%	9%	8%	15%	15%	10%	13%	10%
Insufficient technology for the task	9%	6%	14%	3%	0%	3%	9%	13%	3%	13%	3%	10%	5%	6%	8%
Lack of qualified security people	19%	17%	7%	25%	20%	28%	11%	16%	18%	23%	15%	17%	17%	19%	16%

Figure 3.6: How would you grade your agency's average cyber security risk management at this time?

	Contractor	Employee	Organizational Role			Program Role		Sufficient Budget		Progress		Website	
			Senior Management	Security	IT	Implementation	Other	Top 2	Other	Since 2012		Tripwire	GTRA
										Top 2	Other		
N=	31	68	28	32	24	37	62	37	62	39	59	49	50
A "Excellent"	3%	4%	11%	0%	5%	5%	3%	8%	2%	8%	2%	2%	6%
B "Above Average"	39%	37%	43%	34%	41%	30%	42%	51%	29%	64%	19%	37%	38%
C "Average"	39%	49%	39%	41%	50%	43%	47%	35%	52%	26%	59%	45%	46%
D "Below Average"	13%	10%	7%	22%	0%	19%	6%	5%	15%	3%	17%	14%	8%
F "Failing"	6%	0%	0%	3%	5%	3%	2%	0%	3%	0%	3%	2%	2%

Figure 3.7: Your agency's cyber security programs apply industry standards and best practices.

	Contractor	Employee	Organizational Role			Program Role		Sufficient Budget		Progress				Website	
			Senior Management	Security	IT	Implementation	Other	Top 2	Other	Since 2012		Current		Tripwire	GTRA
										Top 2	Other	top 2	Other		
N=	31	70	28	32	24	38	64	38	64	40	61	40	58	51	51
Agree completely	13%	17%	25%	6%	13%	16%	16%	24%	11%	23%	11%	25%	10%	12%	20%
Agree somewhat	42%	53%	50%	50%	50%	39%	55%	58%	44%	63%	39%	53%	50%	49%	49%
Neutral	23%	14%	7%	22%	25%	21%	16%	13%	20%	8%	25%	13%	17%	22%	14%
Disagree somewhat	23%	16%	18%	22%	13%	24%	14%	**5%**	**25%**	8%	25%	10%	22%	18%	18%

Figure 3.8: Your agency's leadership cares more about meeting compliance regulations than improving security.

	Contractor	Employee	Organizational Role			Program Role		Sufficient Budget		Progress				Website	
			Senior Management	Security	IT	Implementation	Other	Top 2	Other	Since 2012		Current		Tripwire	GTRA
										Top 2	Other	top 2	Other		
N=	32	69	28	32	24	39	63	38	64	40	61	41	57	51	51
Agree completely	22%	19%	4%	38%	25%	26%	16%	24%	17%	13%	25%	20%	21%	29%	10%
Agree somewhat	31%	26%	36%	34%	17%	26%	29%	29%	27%	20%	33%	17%	33%	31%	24%
Neutral	19%	20%	21%	16%	33%	28%	16%	18%	22%	23%	20%	20%	19%	16%	25%
Disagree somewhat	22%	23%	18%	9%	13%	15%	27%	24%	22%	30%	16%	32%	18%	20%	25%
Disagree completely	6%	12%	21%	3%	13%	5%	13%	5%	13%	15%	7%	12%	9%	4%	16%

Figure 3.9: The new standard framework being developed by NIST will help us improve security.

	Contractor	Employee	Organizational Role			Program Role		Sufficient Budget		Progress				Website	
			Senior Management	Security	IT	Implementation	Other	Top 2	Other	Since 2012		Current		Tripwire	GTRA
										Top 2	Other	top 2	Other		
N=	32	70	28	32	24	39	63	38	64	40	61	41	58	51	51
Agree completely	19%	9%	14%	9%	17%	13%	11%	13%	11%	23%	5%	15%	10%	12%	12%
Agree somewhat	47%	49%	50%	56%	29%	44%	51%	53%	45%	48%	49%	46%	52%	39%	57%
Neutral	25%	34%	25%	25%	50%	38%	27%	26%	34%	28%	33%	32%	28%	41%	22%
Disagree somewhat	9%	7%	7%	9%	4%	5%	10%	5%	9%	3%	11%	5%	10%	8%	8%
Disagree completely	0%	1%	4%	0%	0%	0%	2%	3%	0%	0%	2%	2%	0%	0%	2%

Figure 3.10: The biggest security threat we face is a dysfunctional Congress that is unable to pass cyber security legislation and funding.

	Contractor	Employee	Organizational Role			Program Role		Sufficient Budget		Progress				Website	
			Senior Management	Security	IT	Implementation	Other	Top 2	Other	Since 2012		Current		Tripwire	GTRA
										Top 2	Other	top 2	Other		
N=	32	69	28	32	24	39	63	37	65	39	62	40	58	52	50
Agree completely	6%	17%	14%	13%	16%	10%	16%	11%	15%	15%	13%	20%	10%	15%	12%
Agree somewhat	19%	35%	25%	25%	28%	33%	27%	22%	34%	31%	27%	28%	33%	27%	32%
Neutral	34%	28%	29%	28%	36%	31%	30%	35%	28%	33%	29%	28%	31%	27%	34%
Disagree somewhat	28%	16%	21%	28%	16%	18%	21%	24%	17%	15%	23%	18%	21%	23%	16%
Disagree completely	13%	4%	11%	6%	4%	8%	6%	8%	6%	5%	8%	8%	5%	8%	6%

Figure 3.11: Your agency has adequate resources to implement the Administration's policies.

	Contractor	Employee	Organizational Role			Program Role		Progress				website	
			Senior Management	Security	IT	Implementation	Other	Since 2012		Current		Tripwire	GTRA
								Top 2	Other	top 2	Other		
N=	32	70	28	32	25	39	64	40	62	41	58	52	51
Agree completely	19%	6%	14%	9%	12%	10%	9%	13%	8%	17%	5%	12%	8%
Agree somewhat	16%	33%	21%	25%	28%	33%	23%	33%	24%	37%	21%	29%	25%
Neutral	34%	10%	11%	22%	32%	15%	20%	18%	19%	17%	17%	23%	14%
Disagree somewhat	22%	33%	39%	28%	16%	26%	31%	28%	29%	22%	36%	21%	37%
Disagree completely	9%	19%	14%	16%	12%	15%	16%	10%	19%	7%	21%	15%	16%

Figure 3.12: The Administration's cyber security policies have improved government security.

	Contractor	Employee	Organizational Role			Program Role		Sufficient Budget		Progress				Website	
			Senior Management	Security	IT	Implementation	Other	Top 2	Other	Since 2012		Current		Tripwire	GTRA
										Top 2	Other	top 2	Other		
N=	32	70	28	32	25	39	64	38	65	40	62	41	58	52	51
Agree completely	3%	9%	14%	3%	4%	8%	6%	11%	5%	15%	2%	10%	5%	4%	6%
Agree somewhat	53%	46%	61%	47%	24%	28%	59%	53%	45%	55%	42%	54%	47%	33%	63%
Neutral	34%	30%	18%	31%	64%	44%	25%	29%	34%	25%	37%	32%	31%	40%	24%
Disagree somewhat	9%	10%	4%	16%	8%	15%	6%	5%	12%	5%	13%	5%	12%	13%	6%
Disagree completely	0%	6%	4%	3%	0%	5%	3%	3%	5%	0%	6%	0%	5%	6%	2%

Figure 3.13: How much impact has sequestration had on implementing cyber security programs in your agency?

	Contractor	Employee	Organizational Role			Program Role		Sufficient Budget		Progress				Website	
			Senior Management	Security	IT	Implementation	Other	Top 2	Other	Since 2012		Current		Tripwire	GTRA
										Top 2	Other	top 2	Other		
N=	32	70	28	32	25	39	64	38	65	40	62	41	58	51	51
No Impact	41%	19%	32%	19%	28%	31%	23%	34%	22%	23%	27%	32%	21%	25%	27%
Impacted Greatly	3%	20%	18%	6%	12%	18%	13%	11%	17%	15%	15%	10%	19%	8%	22%
Impacted Somewhat	56%	61%	50%	**75%**	60%	51%	64%	55%	62%	63%	58%	59%	60%	67%	51%

APPENDIX A: RESPONSES TO "IN YOUR OPINION, WHAT IS THE ONE THING FEDERAL SECURITY LEADERS SHOULD DO TO CONNECT SECURITY TO THE AGENCY MISSION?"

CATEGORY	RESPONSES
Adapt To Changing Environment, Focus On Actual Issues	Start speaking in terms of risk to the mission, not compliance with regs
	Stop thinking about things as it's always been. Technologies and capabilities have changed, so has the threat environment. We need to look at this more holistically rather than at specific pieces and parts - then try to meld them together.
	Work on security rather than ensuring compliance with government regulations.
Additional Training	Engage employees in training and discussion about on-the-ground and insider threats
	More training
Better Informed Leaders	Educate themselves in cyber security or delegate this task to knowledgeable individuals.
	IT Security leaders must be able to clearly identify (in understandable terms) mission risk, what's at stake and solutions to mitigate. And sell it.
	Lead by example, manage by facts and measure by numbers, everything they do.
	Leaders need to truly understand the impact of security measures, instead blindly pushing compliance.
	Practice good leadership
	Put in agency leaders that understand security is at the core of every aspect of the agency business.
	Understand the mission and work with management top down
Better Strategic Planning Process	Apply resources (funding/manpower) consistent with policy
	Better compartmentalization
	Better manage the implementation of automated tools that have been approved for the enterprise.
	Create requirements that can be implemented
	Define budget.
	Have a step-by-step implementation and test plan developed for all agencies to follow.
	Include it in the mission statement.
	Involve when creating new projects, not as an after thought
	Make part of performance standards
	Mandate/directive
	Risk mgmt framework institution
	Staying on top of things
	Strong contingency management practices
	Understand the goals trying to be achieved and the processes that achieve those goals
Greater Accountability	Accountability
	Address the gaping lack of accountability for adhering security policies.
Greater Focus On IT Security	Make security as common as work instructions. Keep it in the news. Standing agenda item.
	More PR
	Provide awareness
	Publicize the number and the remediation cost of both attempts and successful security incidents.
	Recognize the threat and stop fooling themselves.

CATEGORY	RESPONSES
Hire More Experienced People	Awareness
	Hire cyber security people.
	Hire more consultants
	Hire more individuals such as myself that interface with NIST, IEEE, etc.
	Recruit more trained civilians
More Collaboration	Align to the National Cybersecurity Workforce Framework
	Collaborate
	Embed cybersecurity personnel throughout the agency instead of having a silo of information and specialists.
	Engage non-IT leadership
	It won't work individually. Design must be global along with global implementation.
	They need to work closely with the program/mission Executives
More Funding	Connect security to budget
	Convince non-security leadership to care more about and invest more into security
	Direct funding for reactive needs
	Ensure adequate funding and training
	Ensure funding is continue to support all technology security efforts
	Ensure that the techs are well funded and good leadership is provided.
	Fund it
	Provide budget increases to meet security mandates
	Provide funds for training.
	Restore funding levels
Quantitatively Measure Security Risks, Determine Acceptable Level	Better quantify business risk (cost/mission) than focusing on cyber risk
	Demonstrating risk and to what degree the mission is able to tolerate or accept it. And how risk mitigation can be folded into development and in the end save timer and money for the agency.
	Directly relate potential attacks to mission failure.
	Relate risk profile in terms of adverse affect on the mission.
	Remain vigilant even if the immediate threat is not visibly apparent
Show Consequences Of Failure	Demonstrate what the consequences are should security fail.
	Illustrate consequences for failure to secure.
	Show what happens when security fails
	What happens if a network attack is successful
Strengthen Policies And Penalties	Make it part of Business Requirements or pay a fine
	Put teeth in their policy, hold accountable those who weaken the security posture.
	Start hitting the award fees of projects that will not comply with Agency directives on security. There is still sense of "you can't tell me what to do" attitude is too many places/projects.
Other	Address concern with all networked devices, not just IT
	Bpm process
	Data driven status aligned to mission
	Designate the network as a weapons system/platform
	Destroy stovepipes
	Do not have a comment
	Focus on the Top 20 Critical Controls to close gaps in security compliance, rather then singular focus on NIST 800-53 compliance.
	Get more independent assessments
	Incorporate cyber security as one component of a broader enterprise-wide risk analysis that could impact delivering mission services and actively mitigate the risks.

CATEGORY	RESPONSES
	Life cycle integration
	Limit interaction with personal data as much as possible.
	Map the business architecture to the security architecture
	No opinion
	Red Team all agencies and govt-wide internal monitoring
	Reduce the number of cleared personnel in the TS/SCI program
	Start using Risk Management to Mission/Functions and Stop using compliance reports that do NOT relate to real security
	Stop certifying applications, instead, require certification of business processes. This would require both internal controls, business people, and security personnel to collaborate and work together to ensure that the automation and semi-automation of business processes are fully covered. We have seen errors in business processes that have nothing to do with any formal system. We have also seen an increase in "client-led" development - meaning non-professionals trying to automate business processes. If you make them certify the business processes, then these all get caught and appropriately assessed. In addition, the true risk holder - the business unit - gets tagged with the risk and having to mitigate it rather than a central security group getting tagged for their largess.
	Stop focusing on spying on its citizens. Stop borrowing money from countries that hate us. Hire competent people. Have competent people make security decisions, and create the policies.
	Traceability to business requirements and service delivery standards - esp to Citizens
	Unsure

n=87

Project Evaluation Form

Hanover Research is committed to providing a work product that meets or exceeds client expectations. In keeping with that goal, we would like to hear your opinions regarding our reports. Feedback is critically important and serves as the strongest mechanism by which we tailor our research to your organization. When you have had a chance to evaluate this report, please take a moment to fill out the following questionnaire.

http://www.hanoverresearch.com/evaluation/index.php

Caveat

The publisher and authors have used their best efforts in preparing this brief. The publisher and authors make no representations or warranties with respect to the accuracy or completeness of the contents of this brief and specifically disclaim any implied warranties of fitness for a particular purpose. There are no warranties which extend beyond the descriptions contained in this paragraph. No warranty may be created or extended by representatives of Hanover Research or its marketing materials. The accuracy and completeness of the information provided herein and the opinions stated herein are not guaranteed or warranted to produce any particular results, and the advice and strategies contained herein may not be suitable for every client. Neither the publisher nor the authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages. Moreover, Hanover Research is not engaged in rendering legal, accounting, or other professional services. Clients requiring such services are advised to consult an appropriate professional.

1750 H Street NW, 2nd Floor
Washington, DC 20006

P 202.756.2971 F 866.808.6585
www.hanoverresearch.com