Government Business Council

Assessing Cyber Security Readiness in the Federal Government

A Candid Poll of Federal Government Professionals

Underwritten by

Google Cloud

May 2019

Table of Contents

Overview

Purpose

The federal government has access into some of the most sensitive digital information in existence. Health records, military service information, and financial records sit in government servers and databases. The propensity for these to be monetized via ransomware and phishing makes them appealing targets.

All of this comes at a time when agencies are increasingly moving their digital operations to the cloud, introducing new security challenges. To dive deeper into the state of cyber security in the federal government and to learn more about efforts to enhance the technological tools, personnel, and skills aimed at thwarting would-be breaches, Government Business Council (GBC) partnered with Google Cloud to survey the men and women on the cyber front lines.

Methodology

Government Business Council and Google Cloud fielded a survey in March and April 2019 to a random sample of civilian and military government respondents, including individuals with cyber security expertise. A total of 659 respondents participated in the survey. Additional screening criteria about familiarity with particular aspects of cyber security narrowed the sample down for specific questions in the survey.

Executive Summary

Despite overall confidence in cyber security posture, government agencies exhibit some skepticism

In addition to the confessed inadequacy of threat modeling and other cyber security practices, federal government respondents indicate that their organization's security posture lags in certain key areas. Most notably, cyber professionals and mission-oriented respondents alike mention the lack of robust data-based insights in the cyber security apparatus as well as the need for cyber security processes to learn and incorporate past lessons.

While cyber leadership structures are forming, agencies lean into federal guidelines and polices

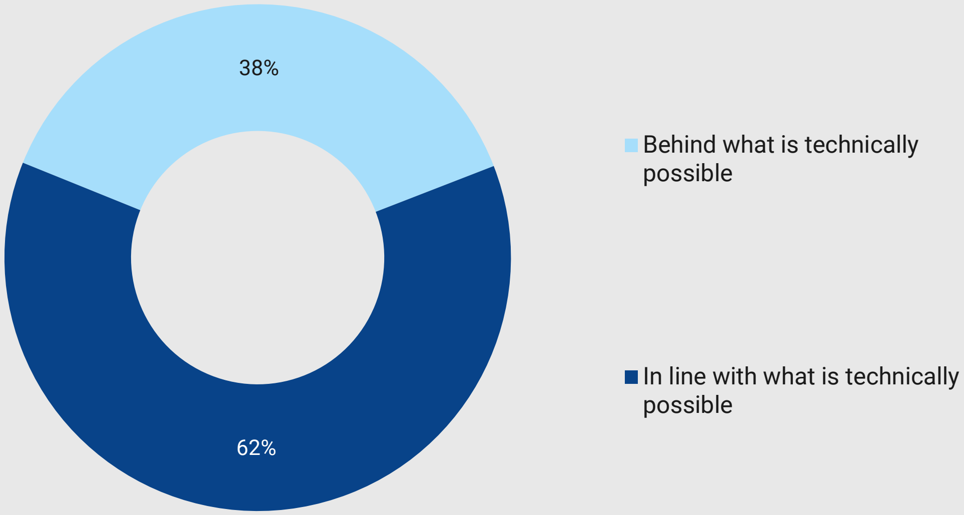
While some agencies report having a single individual tasked with cyber security, the government-wide norm is for a diffusion of cyber security responsibility based on job function or security application. For some agencies, this arrangement has resulted in less-than-clear channels for escalating cyber security concerns. Related to this is the predominance of FITARA as the foundation for federal cyber security development – as leadership is integrated and security is elevated to greater strategic prominence, cyber policies could be tailored to more effectively and directly meet agencies' needs.

Buoyed by federal initiatives, federal agencies are moving the needle on cyber projects, but gaps remain

As the President's Management Agenda, cyber-aligned executive orders, and legislation like the Modernizing Government Technology Act place cyber vulnerabilities in their sights, agencies are making measurable progress on recruitment/retention, cyber tool acquisition, and dedicating budget to thwarting cyber vulnerabilities. A key pillar for future success will be determined by agencies' ability to leverage public and private partnerships – indeed, some have already identified cloud providers and others as potential contributors.

Measuring Readiness

How would you describe your organization's cyber security achievements relative to what is technically possible given available security tools?



Percentage of respondents, n=510
Note: Percentages may not add up to 100% due to rounding

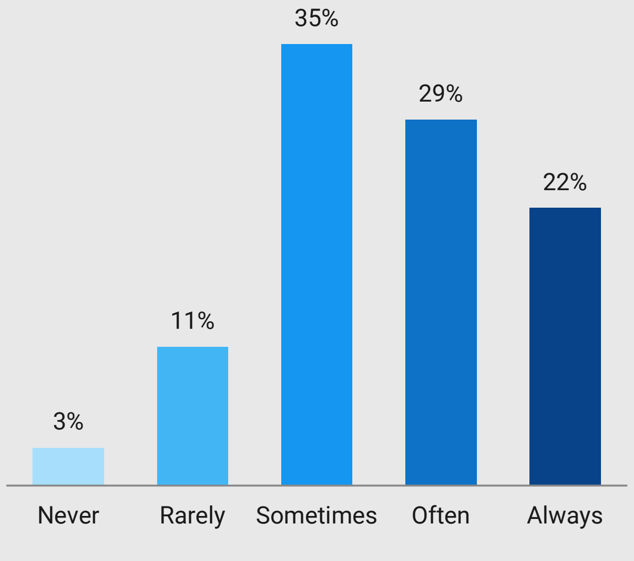
A majority (62%) of survey respondents believe their organization has been able to achieve a level of cyber security that is in line with what is technically possible. Still, 38% perceive their organization as behind what is technically possible.

62%

of respondents believe their organization's cyber security achievements are in line with what is technically possible given available security tools.

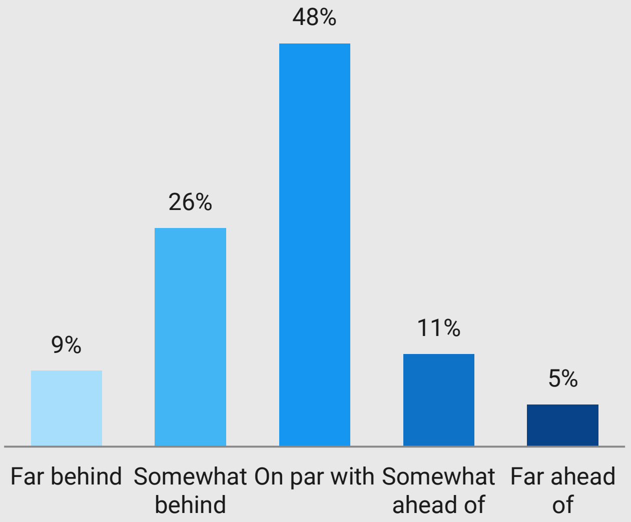
A majority indicate their organization is generally forward-thinking in cyber security

Please complete the statement: "My organization is ________ forward-thinking and innovative in its approach to cyber security."



Percentage of respondents, n=512
Note: Percentages may not add up to 100% due to rounding

Please complete the statement: "My organization's cyber security tools are ________ with the abilities of our workforce."



Percentage of respondents, n=508.
Note: Percentages may not add up to 100% due to rounding

Respondents in federal government view their organization's cyber security posture positively – a majority state that their organization is often or always forward-thinking and innovative in its approach to cyber security. Still, 14% report that their employer rarely or never exhibits such traits.

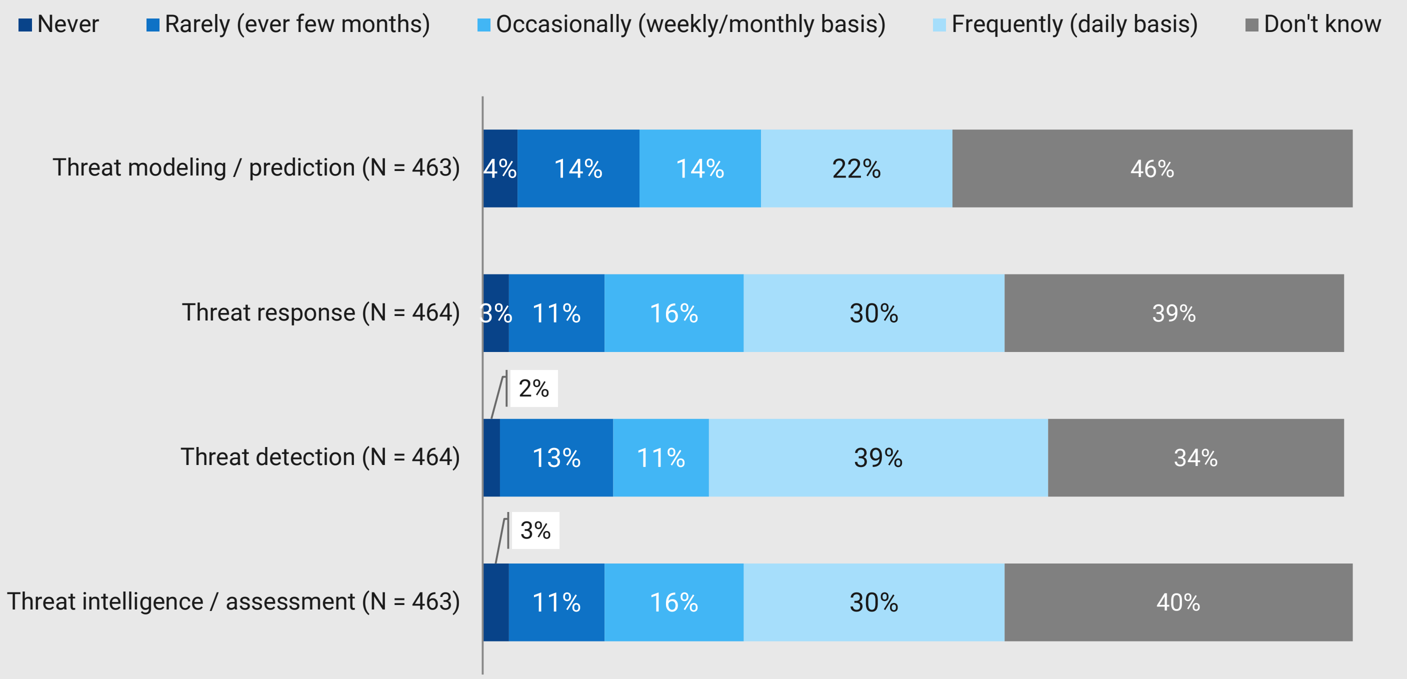
31% of government employees report misalignment between their organization's cyber security tools and the abilities of their workforce. 37% of respondents indicate that the two are very or extremely aligned.

14%

of those polled report that their organization is never or rarely forward-thinking and innovative in its approach to cyber security.

Threat detection is the most prevalent cyber security technique; thread modeling and prediction are still rare

In your best estimation, how frequently does your organization practice the following cyber security techniques?



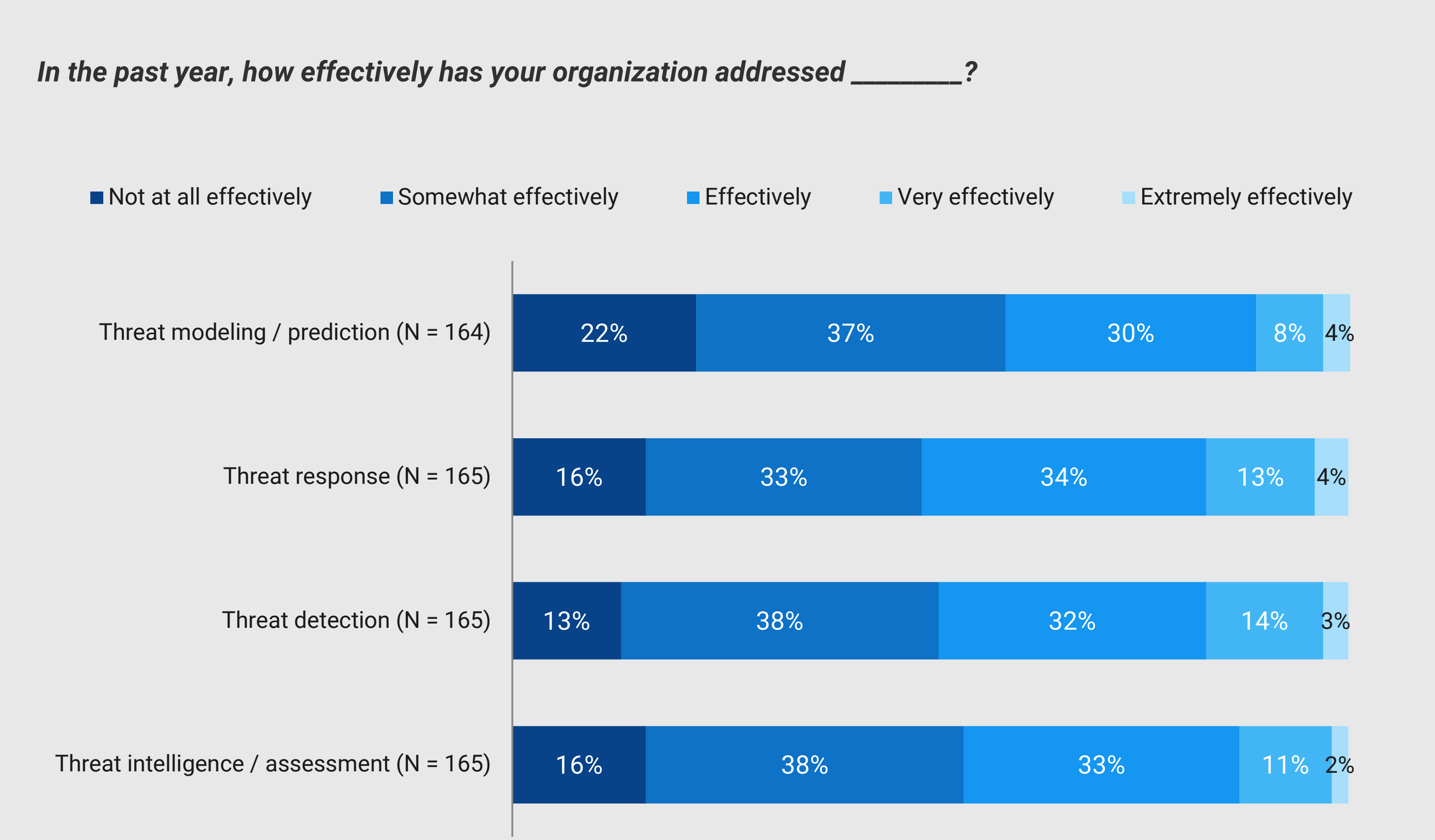
Percentage of respondents, n varies by item.
Note: Percentages may not add up to 100% due to rounding

Half of all respondents report that their organization utilizes threat detection practices at least weekly or monthly, and 46% of those surveyed report the same for threat response and threat intelligence / assessment. Threat modeling / prediction appears to lag most– just 36% of respondents employ this technique on a monthly basis or more frequently.

50%

of respondents report that their organization engages in threat detection occasionally or frequently – the large majority do so on a daily basis.

Government respondents report modest effectiveness within threat framework, identify gaps in key practices



Percentage of respondents, n varies by item.
Note: Percentages may not add up to 100% due to rounding

Survey respondents identify key gaps in cyber security practices: just 12% believe threat modeling / prediction has been addressed very or extremely effectively by their organization, with similar shares for threat response (17%), threat detection (17%), and threat intelligence / assessment (13%).

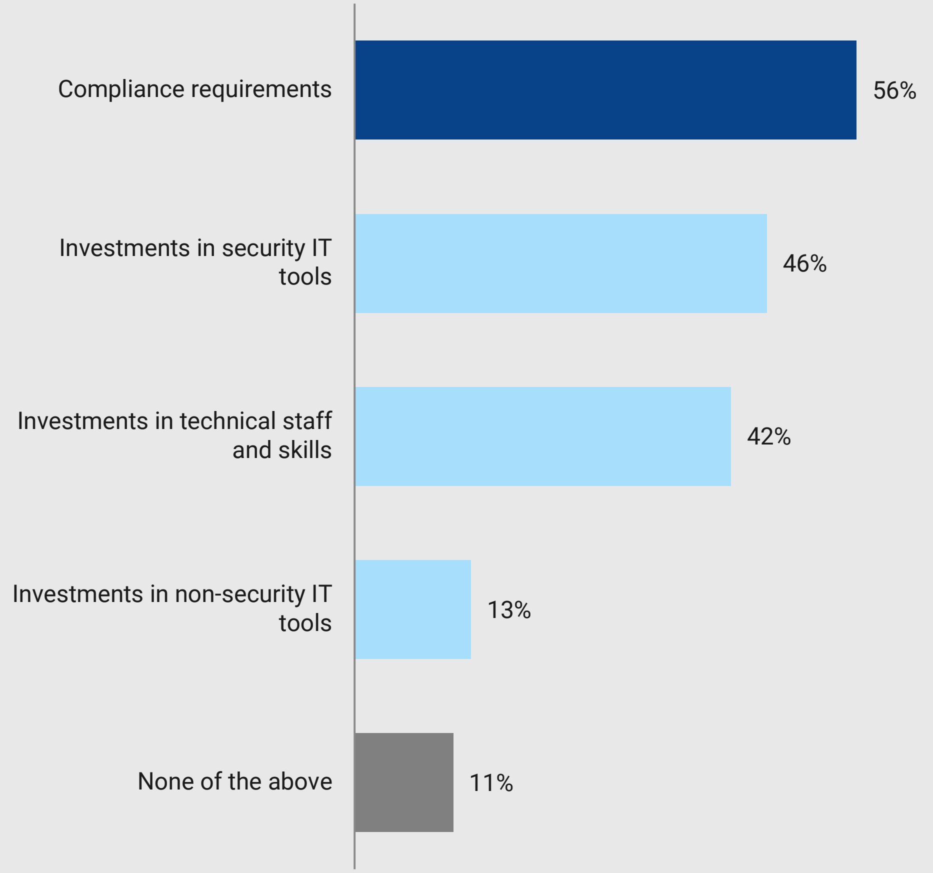
Large shares report that their organization's implementation of these practices has been somewhat or not at all effective. 60% of those polled have this view of threat modeling / prediction, and 49% to 54% have the same view of other threat mitigation tools.

59%

of respondents believe their organization has not been effective in addressing threat modeling / prediction, or that this has only been somewhat effective at their agency.

Compliance maintains a deciding influence over cyber strategy

Which factors were most important in shaping your organization's cyber security strategy in the last year? Please select all that apply.



Percentage of respondents, n=376
Respondents were asked to select all that apply

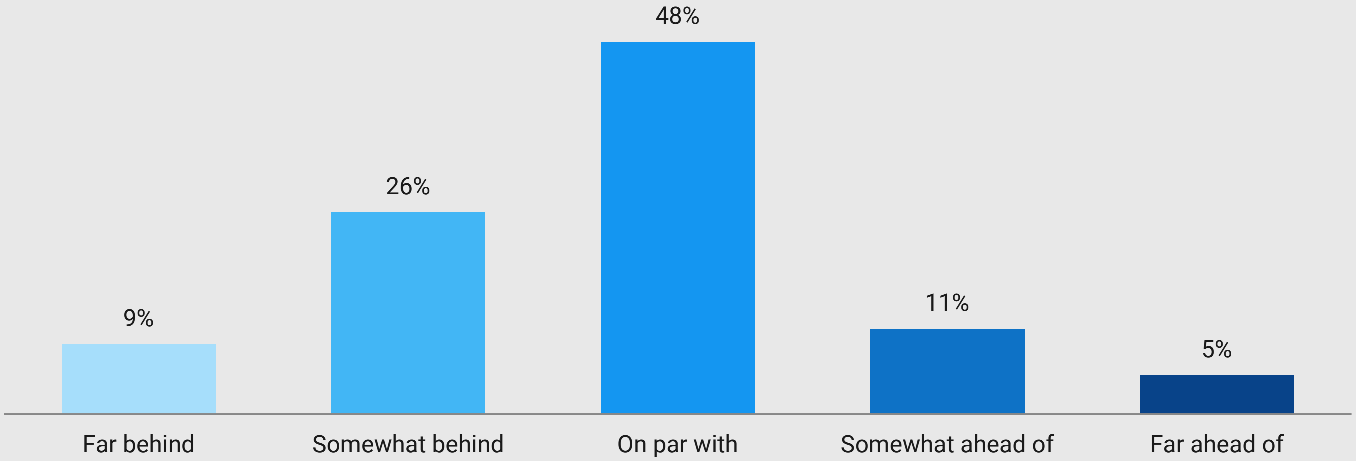
According to respondents, compliance requirements are still the biggest factor driving civilian and military federal government organizations' security strategies – 56% selected this option.

Smaller yet significant shares selected investments in security IT tools and investments in technical staff and skills, showing that regulatory pressure is not the only factor pushing cyber security efforts forward.

56%
of federal government respondents report that compliance requirements were important in shaping their organization's cyber security strategy.

The use of data in cyber security is seen as trailing the use of data in other IT functions

Please complete the following sentence: "My organization's use of data-based insights in its cyber security framework is ________ our other IT functions."



Percentage of respondents, n=341
Note: Percentages may not add up to 100% due to rounding

Though a plurality of surveyees indicate that their organization's ability to derive cyber security insights from data is on par with their ability to do so in other IT functions, 35% report that cyber security actually lags behind other IT functions.

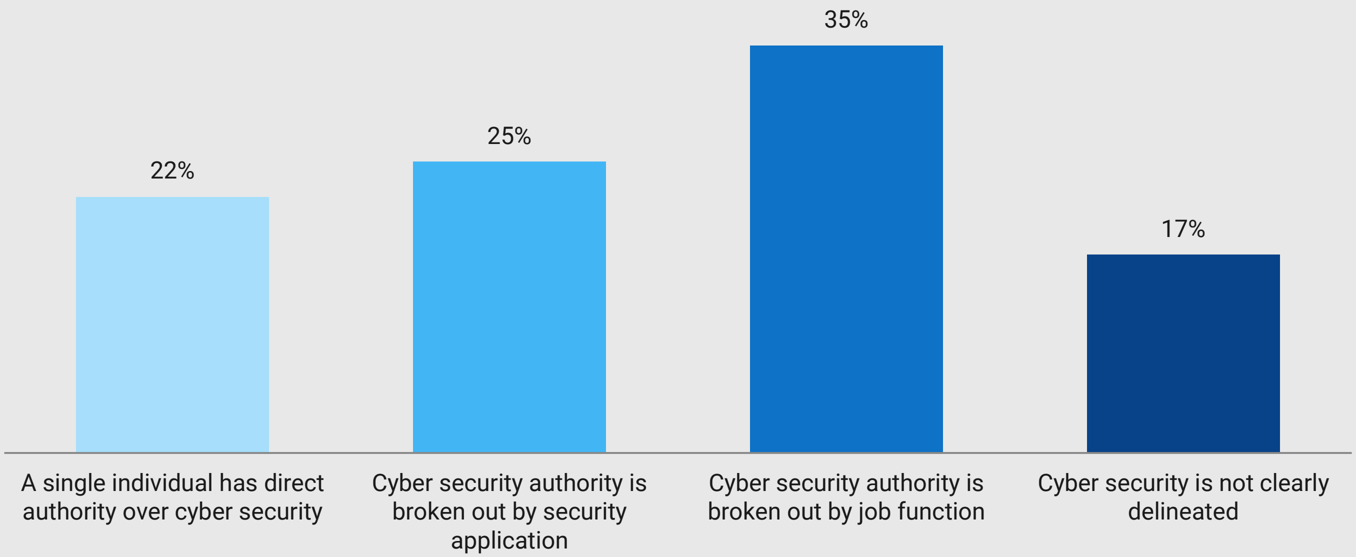
This distribution produces a net gap of 19%, showing that the share of respondents with *lag* in their data-based cyber security functions is substantially larger than the share for whom cyber security *leads* other functions.

35%

of government respondents report that their organization's use of data-based insights in cyber security trails other IT functions.

Amidst growth in CIO and CISO roles, cyber security authority is typically distributed by job function / application

Which of the following best describes your organization's cyber security apparatus?



Percentage of respondents, n=103; N = 194 respondents who selected *Don't know* not displayed here.
Note: Percentages may not add up to 100% due to rounding

Less than one-quarter (22%) of government respondents report that a single individual has direct authority over cyber security – shared or distributed authority is much more common.

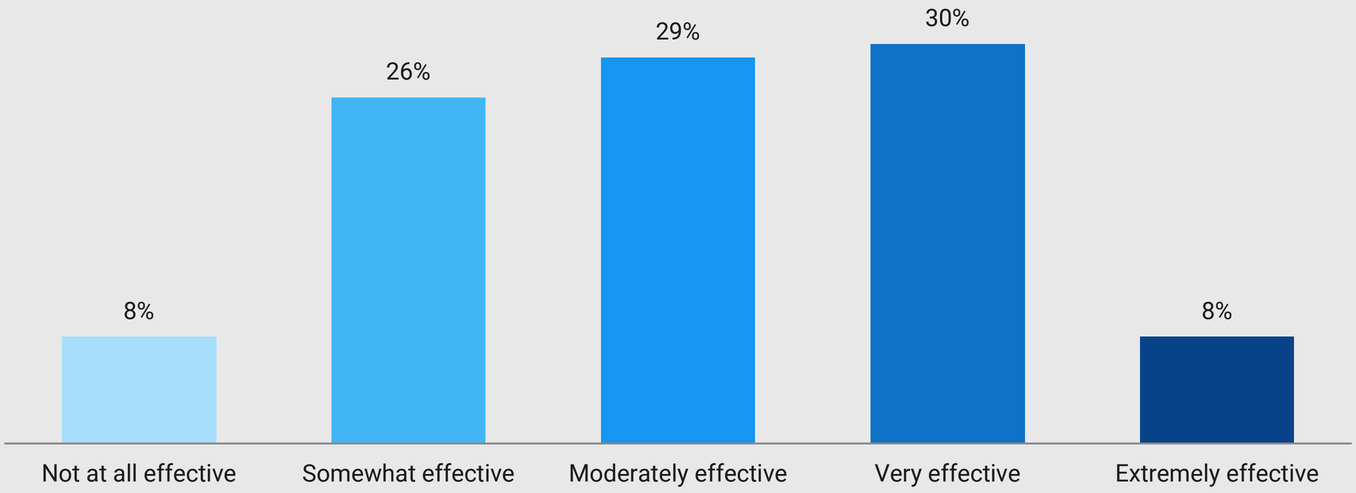
Among the various distributed authority arrangements, it is more common for authority to be broken out by function than by security application. Relatively few (17%) government organizations lack clearly defined authority roles.

60%

of respondents with insight into their organization's cyber security staffing indicate that cyber security authority is distributed.

Government respondents see their organization’s ability to leverage past security incidents as mostly adequate

How effective is your organization at leveraging lessons learned from past cyber security incidents?



Percentage of respondents, n=321
Note: Percentages may not add up to 100% due to rounding

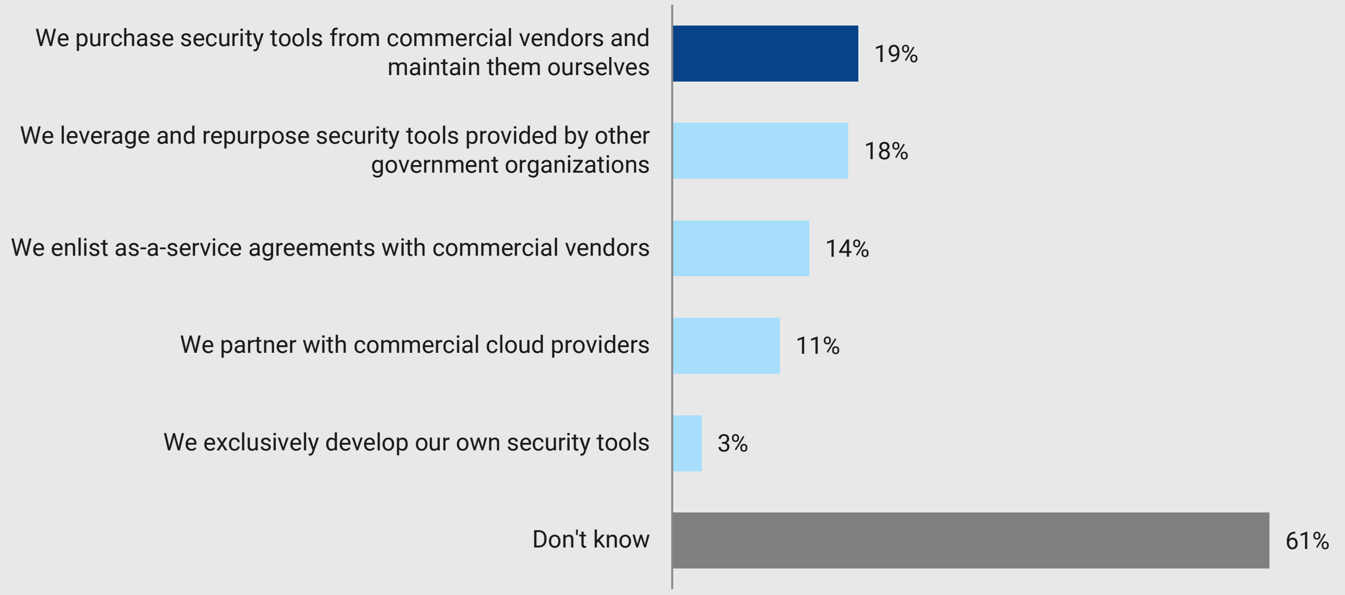
It appears that confidence varies by agency throughout government. While 38% of those polled believe their organization is very or extremely effective at leveraging lessons learned from past cyber security incidents, 34% perceive their employers as not at all effective or just somewhat effective.

38%

stated that their organization’s ability to leverage lessons from past cyber security is very or extremely effective.

Guiding Principles

How does your organization fulfill its cyber security needs? Please select all that apply.



Percentage of respondents, n=376
Respondents were asked to select all that apply

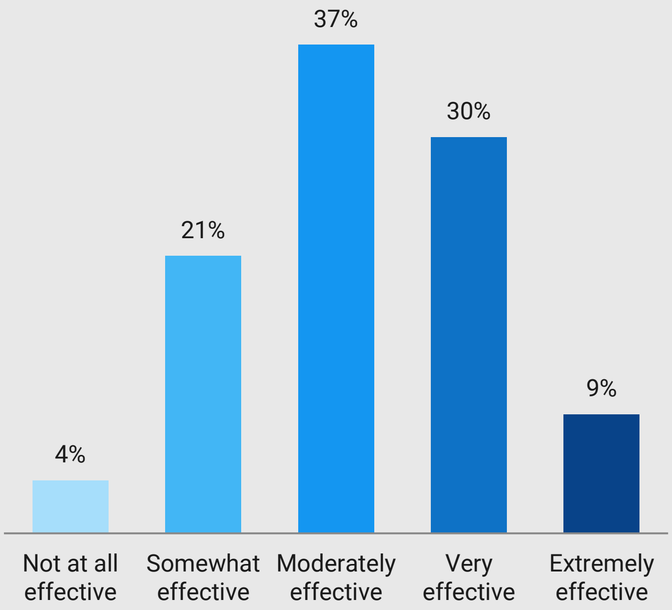
According to survey respondents, government organizations are about as likely to purchase security tools from commercial vendors and maintain them as they are to leverage and repurpose security tools provided by other government organizations. The results show that federal agencies are slightly less likely to enlist as-a-service agreements with commercial vendors to fulfill their cyber security needs, while fewer still partner with commercial cloud providers.

19%

of government respondents purchase security tools from commercial vendors.

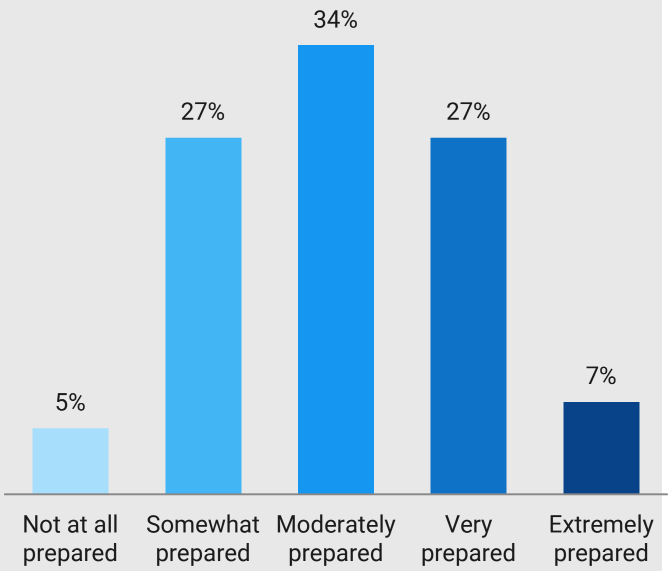
Relative confidence in existing cyber security compliance buttressed by confidence in future compliance

How effective is your organization at complying with current cyber security requirements?



Percentage of respondents, n=321
Note: Percentages may not add up to 100% due to rounding

How prepared is your organization when it comes to meeting cyber security compliance over the next 1-3 years?



Percentage of respondents, n=311.
Note: Percentages may not add up to 100% due to rounding

Employees of civilian and military agencies in the federal government are mostly optimistic about their organization's compliance with current cyber security requirements – 76% believe their organization was at least moderately effective in this capacity at the time of the survey.

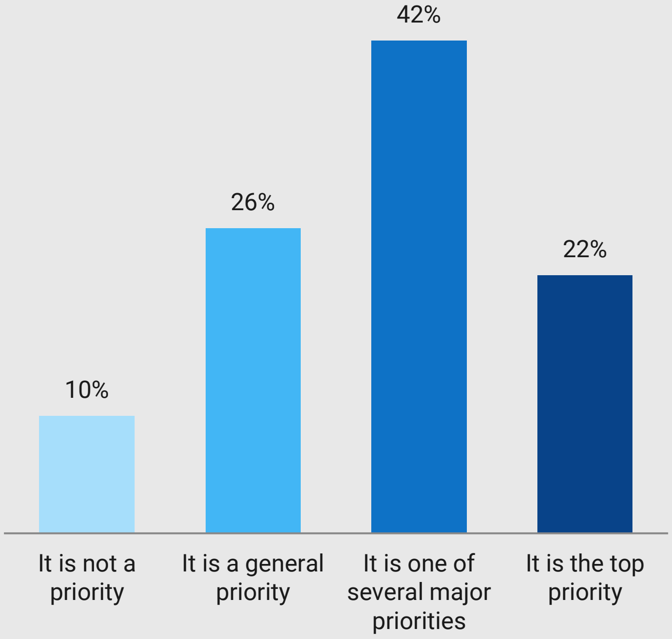
These individuals were also relatively bullish on their ability to meet cyber security compliance requirements over the next 1-3 years, with 34% of survey respondents indicating that their organization is very or extremely prepared to meet such standards.

32%

of respondents reported that their organization is not at all or just somewhat prepared to meet cyber security compliance over the next 1-3 years.

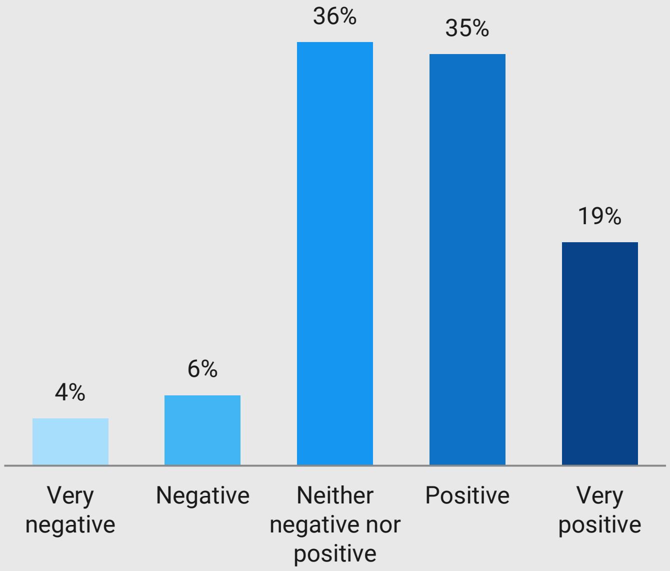
For the majority of government, FITARA is a priority and is seen as having a positive impact on cyber security

To what extent is FITARA compliance a priority in your organization's broader cyber security goals?



Percentage of respondents, n=96; N = 214 respondents who selected *Don't know* not displayed here.
Note: Percentages may not add up to 100% due to rounding

How would you describe the impact that FITARA has had on your organization's ability to defend itself from cyber security threats and vulnerabilities?



Percentage of respondents, n=78; N = 232 respondents who selected *Don't know* not displayed here.
Note: Percentages may not add up to 100% due to rounding

90% of federal government respondents report that FITARA compliance is at least a general priority in their organization's broader cyber security goals, while sizeable portions indicate that it is one of several major priorities (42%) or the top priority (22%).

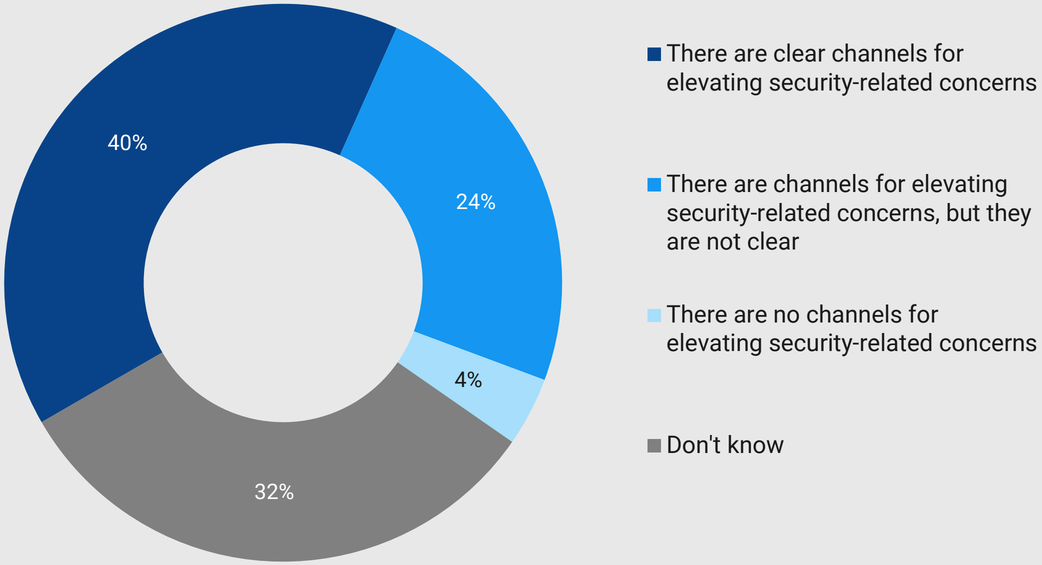
Respondents also have a favorable view of the legislation: 54% report that FITARA has had a positive or very positive impact on their organization's ability to defend itself from cyber security threats and vulnerabilities, while just 10% report a negative or very negative impact.

90%

of those surveyed indicate that FITARA compliance is at least a general priority in their organization's broader cyber security goals.

Survey respondents indicate an opportunity for elevating security-related concerns in cyber security operations

Which best describes your attitude towards your organization's cyber security operations?



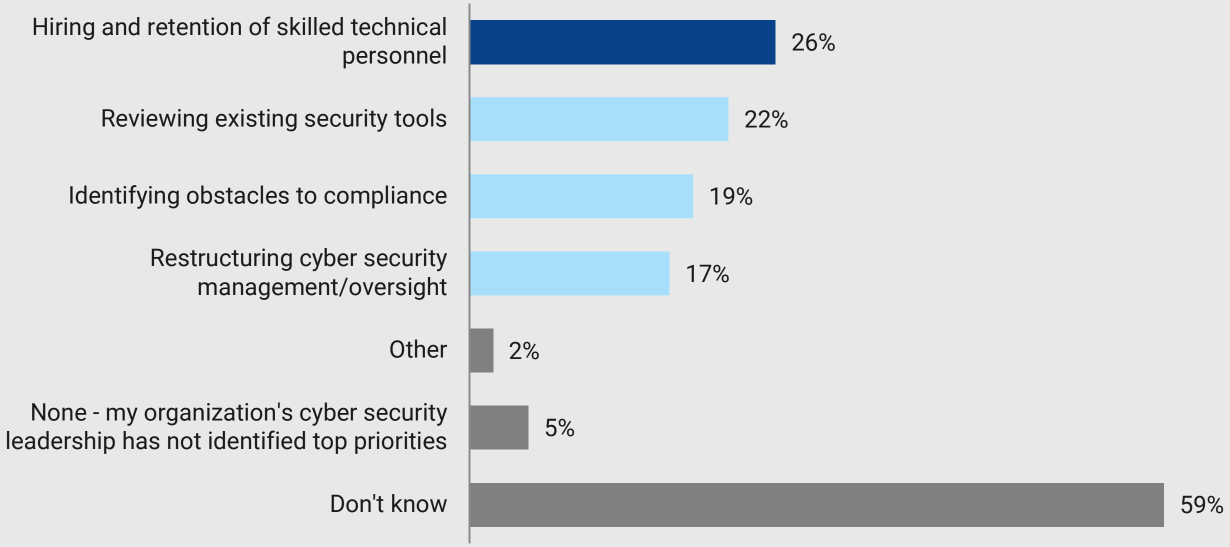
Percentage of respondents, n=293
Note: Percentages may not add up to 100% due to rounding

Although 40% of survey respondents report that their organizations have clear channels for elevating security-related concerns, 24% report that the channels at their organization are unclear. More worryingly, 4% of those polled report that there are no such channels at their organization.

28%
of government respondents report that their organization either does not have channels for elevating security-related concerns, or that the channels exist but are not clear.

Moving Forward

Which of the following has your cyber security leadership identified as top priorities for your organization? Please select all that apply.



Percentage of respondents, n=297
Respondents were asked to select all that apply

The federal government has numerous cyber security challenges, but hiring and retention of skilled technical personnel and reviewing existing security tools are at the top of the list.

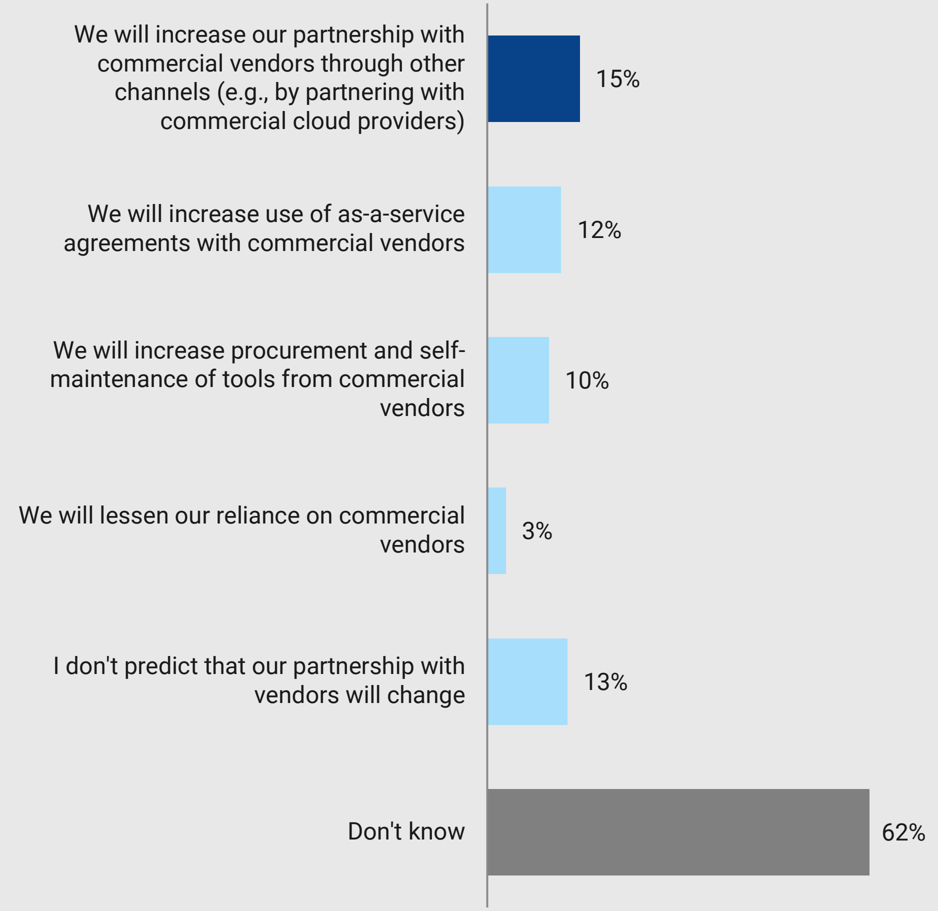
Identifying obstacles to compliance and restructuring cyber security management/oversight also feature prominently, indicating that the various options present a united obstacle for federal decision makers.

26%

of respondents report that hiring and retention of skilled technical personnel has been identified as a top organizational priority.

Cloud-based and other commercial partnerships are most likely for future of vendor-government relationships

In your opinion, how will your organization's partnership with commercial vendors change over the next 1-3 years? Please select all that apply.



Percentage of respondents, n=352
Respondents were asked to select all that apply

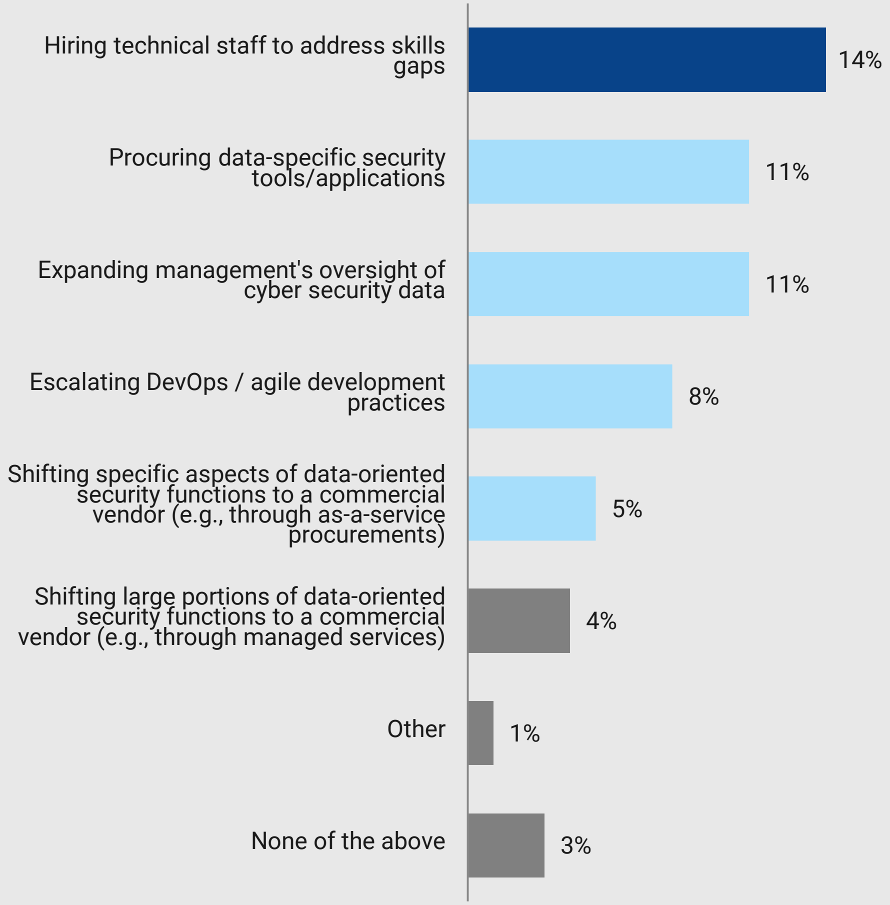
According to survey respondents, federal government organizations are most likely to increase their partnership with commercial vendors through commercial cloud and other channels than through as-a-service agreements and individual procurement/self-maintenance.

15%

of respondents believe their organization will increase their partnership with commercial vendors through cloud-based or other commercial providers over the next 1-3 years.

Federal respondents identify technical staff hiring as most common tactic for improving data security operations

How does your organization plan to improve its data security operations in the next 6-12 months? Please select all that apply.



Percentage of respondents, n=332; Share of respondents who selected *Don't know (70%)* is not displayed here.
Respondents were asked to select all that apply

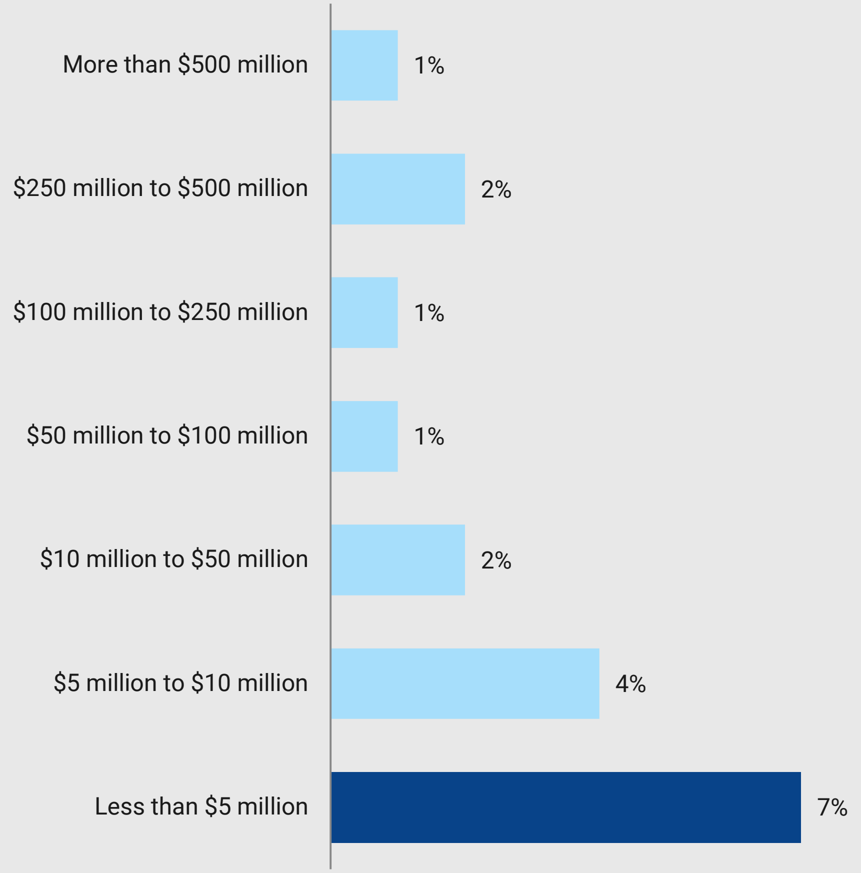
Technical staff hiring, procurement of data-specific security tools/applications, and expanding cyber security data oversight by agency management are most likely to feature into federal organizations' data security plans over the next 6-12 months.

14%

of respondents cite hiring technical staff to address skills gaps as one of the tools their organization will use to improve their data security operations in the next 6-12 months.

Cyber security budgets vary across federal government agencies

To the best of your knowledge, how much does your organization currently invest in security tools and processes on a yearly basis?



Percentage of respondents, n=323; N = 266 respondents who selected *Don't know* is not displayed here.
Note: Percentages may not add up to 100% due to rounding

5%

of those polled report that their organization currently invests at least $100 million in security tools and processes on a yearly basis.

Final Considerations

Looking forward, cyber security professionals and federal government leaders should…

Preserve and expand their capacity for threat modeling

While the future of cyber security will require frequent and effective threat detection and response, it will also be heavily reliant on modeling. Adequately predicting and acting to prevent threats before infiltration will be key to safeguarding PII and other citizen data as services become increasingly digitized and a greater share of customer interactions take place in the cyber domain. A scalable threat modeling apparatus should feature prominently in ongoing cyber security preparation.

Identify key skills needs and apply holistic analysis to recruitment and retention

Compensation, benefits, agency reputation, and organizational culture all factor into potential employees' decisions about whether to accept an offer. But agency tools, IT investment, and communication of a coherent cyber security strategy can also shape cyber professionals' thought processes during candidacy. One of the most important steps to ensuring an adequate security workforce is to treat this as a mission issue, not just a human capital issue.

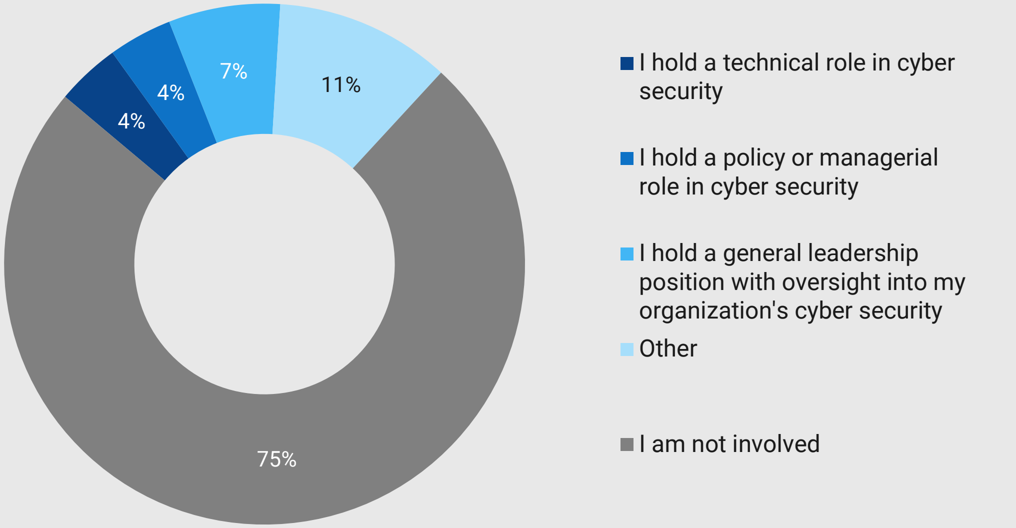
Assess opportunities for key partnerships

Many federal agencies continue to face the biggest threats – sophisticated hackers and adversarial nations – in a one-off, case-by-case capacity. Even as bodies like NIST and DHS work to integrate federal security efforts, opportunities for greater integration abound. Indeed, these extend to both public and private sector opportunities, as evidenced by the experts surveyed for this study.

Respondent Profile

One-quarter (25%) of all federal employees hold a tech-facing role in their organization

Which of the following best describes your role in your organization's cyber security?



Percentage of respondents, n=624
Note: Percentages may not add up to 100% due to rounding

Respondents represent a wide range of federal agencies and military branches

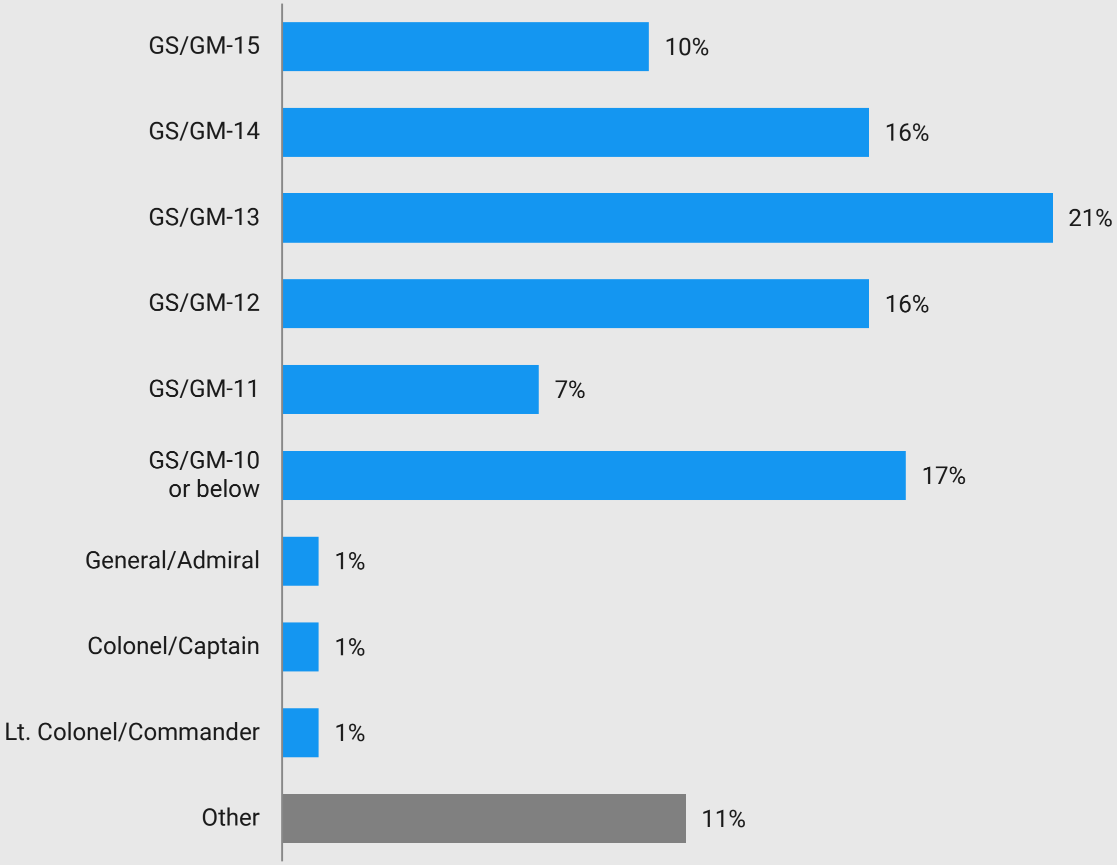
For which department/agency do you work?

- Veterans Affairs
- Agriculture
- Air Force
- Homeland Security
- Interior
- Army
- Navy
- Other independent agency
- Treasury
- Housing and Urban Development
- Social Security Administration
- Transportation
- Justice
- Environmental Protection Agency
- General Services Administration
- Office of the Secretary of Defense
- State
- National Aeronautics and Space Administration
- Commerce
- Energy
- Marine Corps
- Congress/Legislative Branch
- Education
- Office of Personnel Management
- Agency for International Development
- Labor
- Government Accountability Office
- Multiple departments/agencies
- Small Business Administration
- Combatant Commands
- Joint Chiefs of Staff
- Intelligence Community/ODNI
- National Science Foundation
- Nuclear Regulatory Commission

Departments and agencies are listed in order of frequency.

Half of those surveyed are ranked GS-13 or above, or have the equivalent military rank

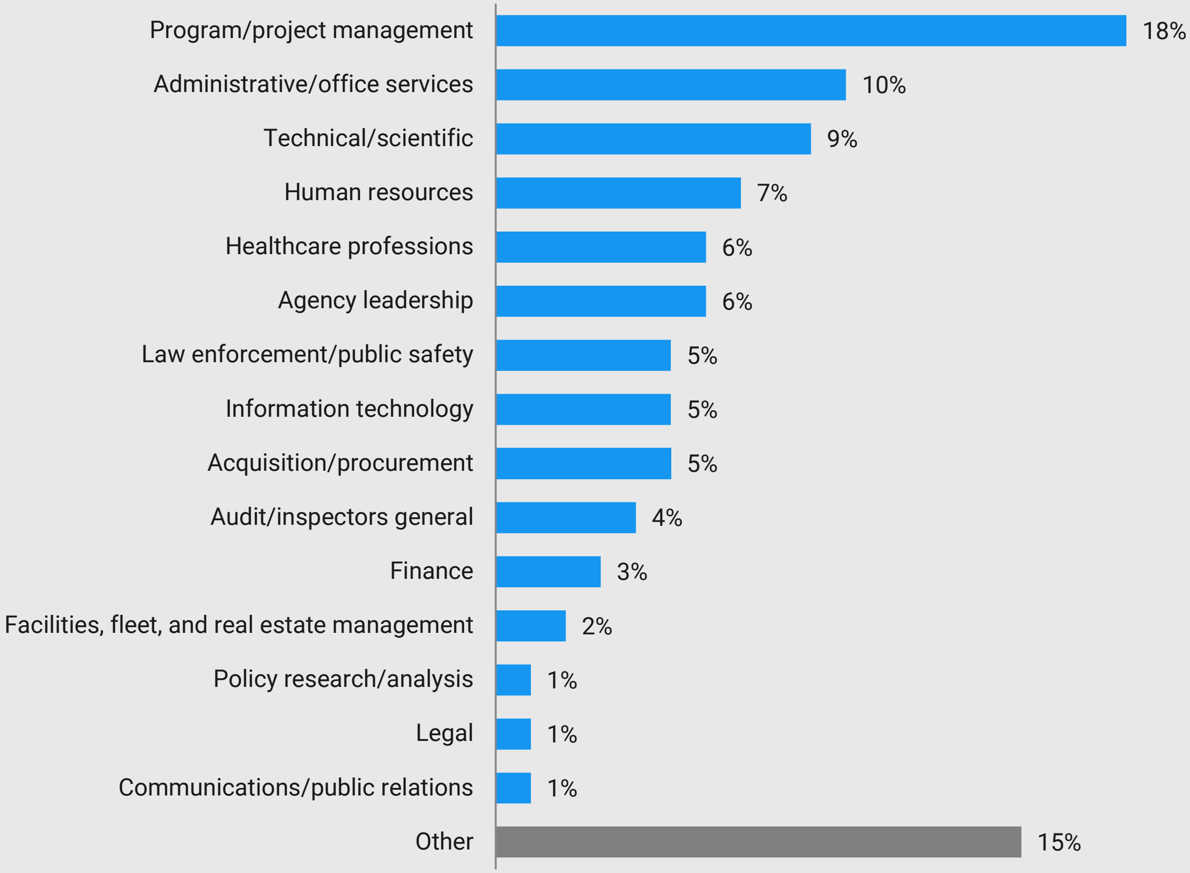
Please indicate your job grade/rank.



Percentage of respondents, n=293
Note: Percentages may not add up to 100% due to rounding

Respondents represent a variety of job functions, including management and technical roles

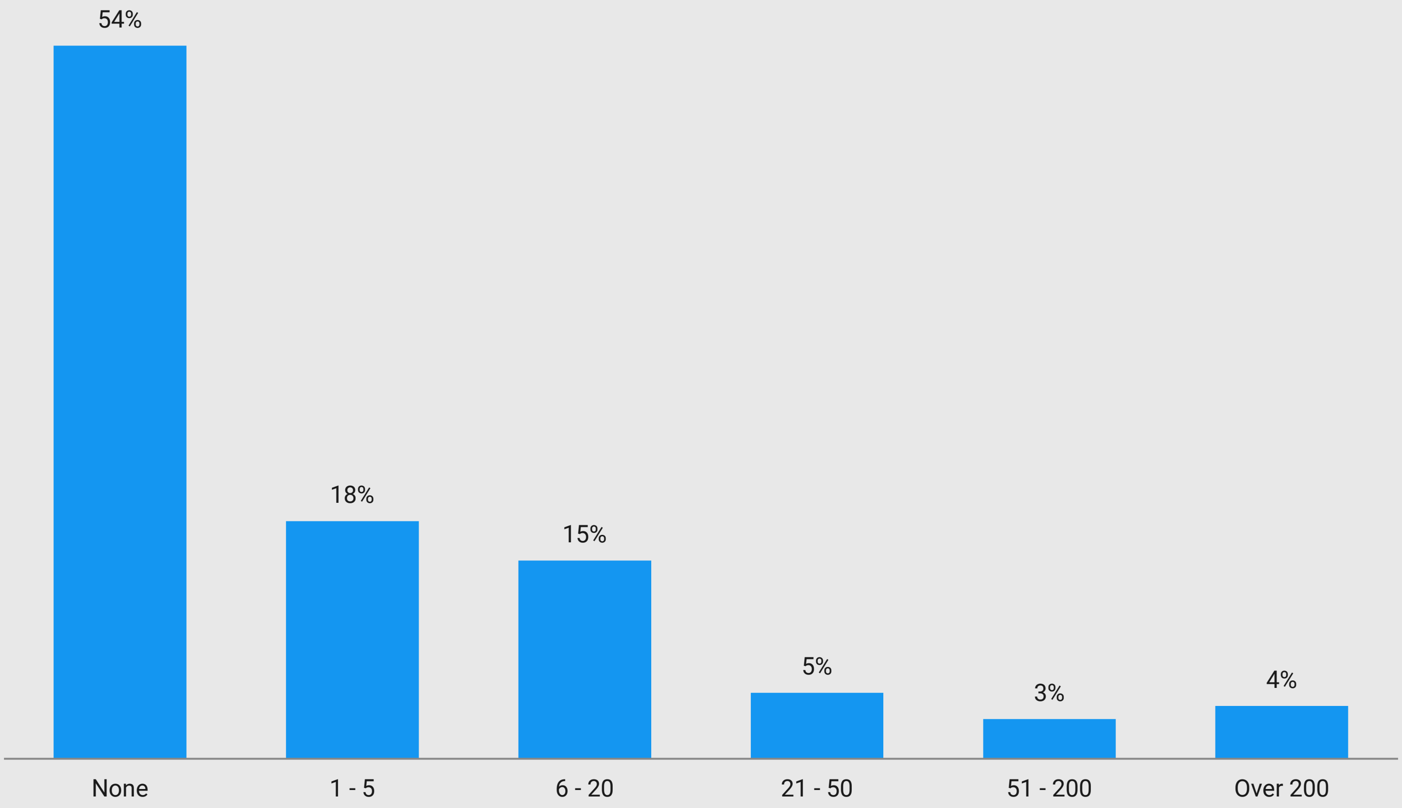
Which of the following best describes your job function?



Percentage of respondents, n=289
Respondents were asked to select all that apply

Nearly one-half (46%) of federal government respondents are managers

How many people do you oversee in total, either directly or through your direct reports?



Percentage of respondents, n=289
Respondents were asked to select all that apply

About

Government Business Council

As Government Executive Media Group's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of *Government Executive*'s 40 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis.

Report Author: Igor Geyn

Contact

Daniel Thomas
Manager, Government Business Council
Government Executive Media Group
Tel: 202.266.7905
Email: dthomas@govexec.com

govexec.com/insights
@GovExecInsights

Google Cloud

Google Cloud is widely recognized as a global leader in delivering a secure, open, intelligent and transformative enterprise cloud platform. Our technology is built on Google's private network and is the product of nearly 20 years of innovation in security, network architecture, collaboration, artificial intelligence and open source software. We offer a simply engineered set of tools and unparalleled technology across Google Cloud Platform and G Suite that help bring people, insights and ideas together. Customers across more than 150 countries trust Google Cloud to modernize their computing environment for today's digital world.