Key Trends in Federal Cybersecurity Investment

January 2023

EY
Building a better
working world

Market Connections™
Research you can act on.
A portfolio platform of GovExec

Table of Contents

Introduction

New and more malicious cyber threats; sharp increases in supply chain attacks; and widespread compromise of privileged credentials pose persistent risks to government agencies.

There is no one-size-fits-all approach to cybersecurity. In fact, there are many technologies and tools that address individual agency priorities. This leaves leaders assessing different cyber tools and competing frameworks in the hope of finding the right approach for their agency – both in implementation and financing.

The start of this new calendar year is a critical time for leaders to assess their spending efforts and evaluate how to bring the most value to their mission.

To help with this assessment and evaluation, Ernst & Young LLP partnered with Market Connections to find out:

- Where are agency leaders focusing their time and resources?
- How can they make the most of their spending dollars?
- What are their current priorities?

This document and the information disclosed within, including the document structure and contents, are confidential and the proprietary property of Ernst & Young LLP and are protected by copyright and other proprietary rights. Any disclosure to a third party in whole or in part in any manner is expressly prohibited.

About the Study

Market Connections and EY partnered to design a survey of 200 federal employees (100 FedCiv and 100 DoD). The research was conducted in November and December of 2022.

PRIMARY OBJECTIVE: Identify where federal employees are vis-à-vis cybersecurity

Discover how prepared their agencies are and what kind of road mapping and programs they have in place

Understand what areas of cybersecurity generate the highest spends

Share the results with government leaders

Note: The report calls out differences between FedCiv and Defense respondents where they exist.

About the Study

KEY INSIGHTS

The data is a detail rich exploration of where federal agencies are in their cyber journey, with a few key insights emerging:

Spending

One in three respondents said their agency spends more than $50 million each year on cybersecurity. Within the category of cybersecurity ***data protection*** and ***privacy and security operations*** **have the biggest spends.** While not statistically significant, it is worth noting that FedCiv respondents are more likely to spend on ***data protection*** while DoD respondents are slightly more likely to spend on ***security operations. Architecture/ engineering*** and ***identity/access management*** are the lowest ranking cybersecurity spends.

Cybersecurity Programs

Nearly two thirds have both a cyber roadmap and a cyber program that focuses on operational technology (OT) in place. Of those with a cyber roadmap, most (61%) assess their cyber priorities quarterly. Perhaps more tellingly, **sizeable minorities** (somewhere between 25%-30%) **do not know whether their agencies have cyber roadmaps, a cyber program that focus on OT, a supply chain risk management program or a cyber table-top exercise in place.**

About seven in ten say they perform data protection, security operations and identify and access management in-house. Attack and penetration is the only function that a majority (58%) outsource. **Nearly all rate their End Point Detection Program as adequate or better. A quarter believe their program is "excellent."** Just 2% rate their program as poor or non-existent.

Cybersecurity Maturity

When it comes to cybersecurity maturity, only one in five rate their cyber threat intelligence program as "very" mature. Identity is the pillar for which respondents feel most prepared: 42% are "very" prepared for "identity" (another 18% are somewhat prepared). Less than a quarter feel very prepared for "network" and "data" (22% and 20% respectively) and just 9% are very ready for "devices" and "applications." **More alarmingly, three in ten are not at all prepared for devices and nearly four in 10 (38%) say they are not at all prepared on the application pillar.**

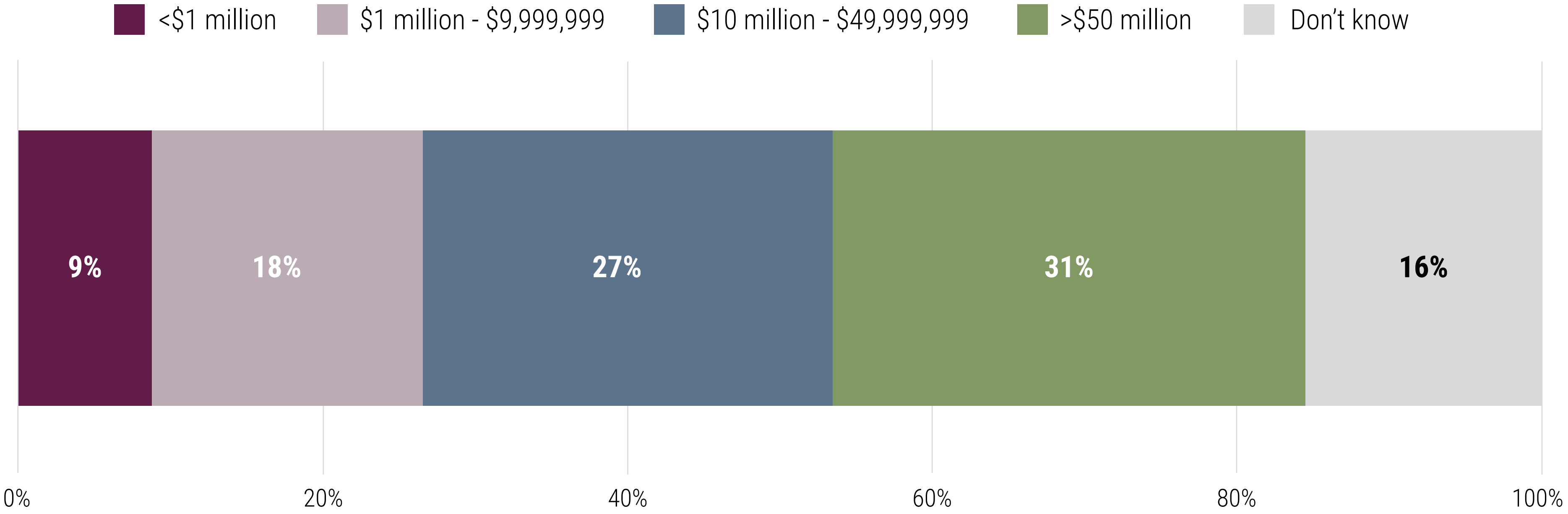
This document and the information disclosed within, including the document structure and contents, are confidential and the proprietary property of Ernst & Young LLP and are protected by copyright and other proprietary rights. Any disclosure to a third party in whole or in part in any manner is expressly prohibited.

Cyber Spending & Budget

Cyber Spending & Budget

ANNUAL SPEND ON CYBERSECURITY

One in three are spending more than $50m annually on cybersecurity; fewer than one in 10 spend less than $1m each year.

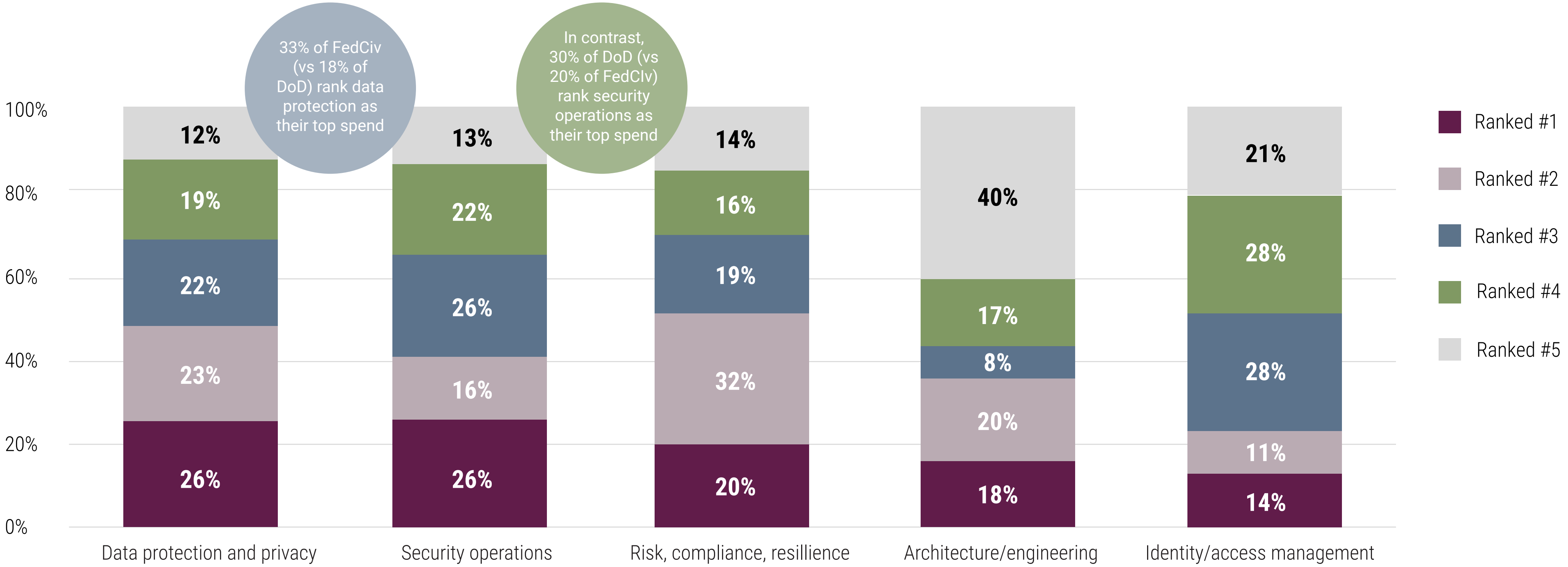


Q1. What is your total annual spend on cybersecurity? Total (n=200)

Cyber Spending & Budget

RANK ORDER OF CYBERSECURITY BUDGET

Data protection and privacy and security operations get the biggest spends. FedCiv respondents are more likely to spend on **data protection** while DoD employees are slightly more likely to spend on **security operations**. *Architecture/engineering* and *identity/access management* are the lowest ranking cybersecurity spends.



33% of FedCiv (vs 18% of DoD) rank data protection as their top spend

In contrast, 30% of DoD (vs 20% of FedCIv) rank security operations as their top spend

Q2. Please rank order your cybersecurity budget by the following areas where 1 means you spend the most in that area and 5 means you spend the least money in that area. Total (n=200)

Cyber Spending & Budget

IN-HOUSE VS. OUTSOURCED

About seven in ten say they perform data protection, security operations and identify and access management in-house. Attack and penetration is the only function that a majority (58%) outsource.

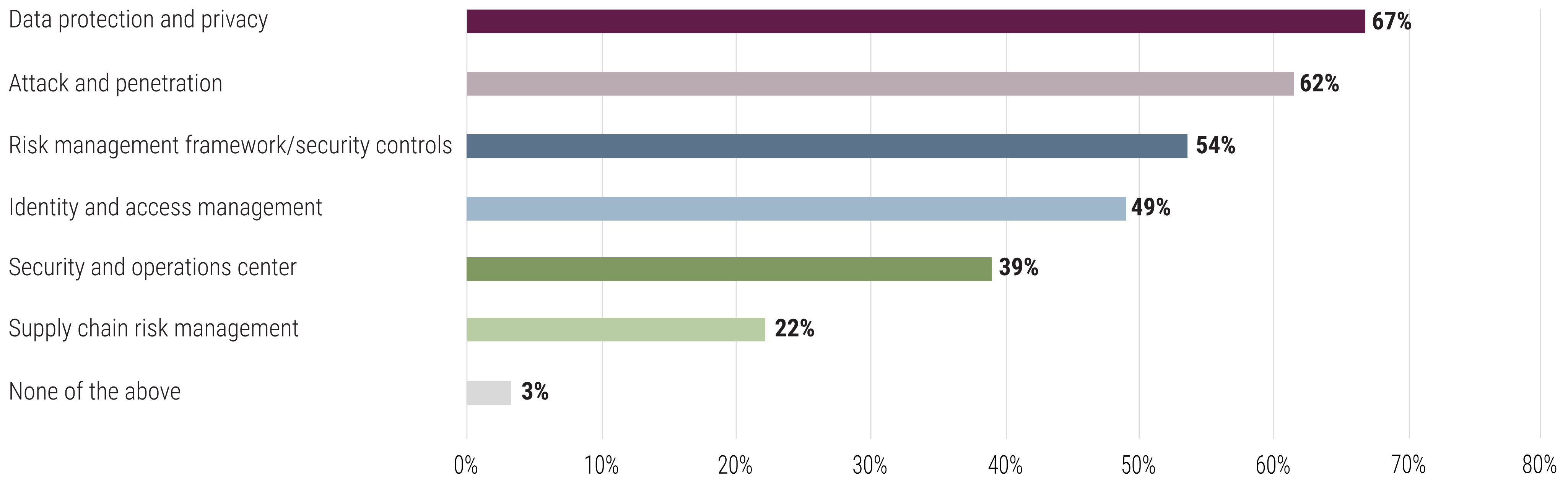
	In-House			Outsourced		
	Total	FedCiv	DoD	Total	FedCiv	DoD
Identity/access management	73%	69%	77%	27%	31%	23%
Security and operations center	71%	70%	72%	29%	30%	28%
Data protection and privacy	69%	66%	72%	31%	34%	28%
Risk management framework/security controls	67%	60%	73%	34%	40%	27%
Supply chain risk management	58%	56%	59%	43%	44%	41%
Cyber Tabletop Exercises	57%	60%	54%	43%	40%	46%
Cyber Threat Intel	54%	53%	55%	46%	47%	45%
Attack and penetration	43%	40%	45%	58%	60%	55%

Q3. Please indicate which of the following security functions you perform in-house vs. outsourcing (using a contractor support). If you both in-house and outsource, please indicate the way you use more often. Total (n=200), FEDCIV (n=100), DOD (n=100)

Cyber Spending & Budget

CYBERSECURITY SERVICES MERITING A PREMIUM PRICE

Strong majorities say data protection/privacy, attack and penetration and identity and access management are services for which it is worth paying a premium. For these public sector employees, supply chain risk management is the least deserving of a premium price.

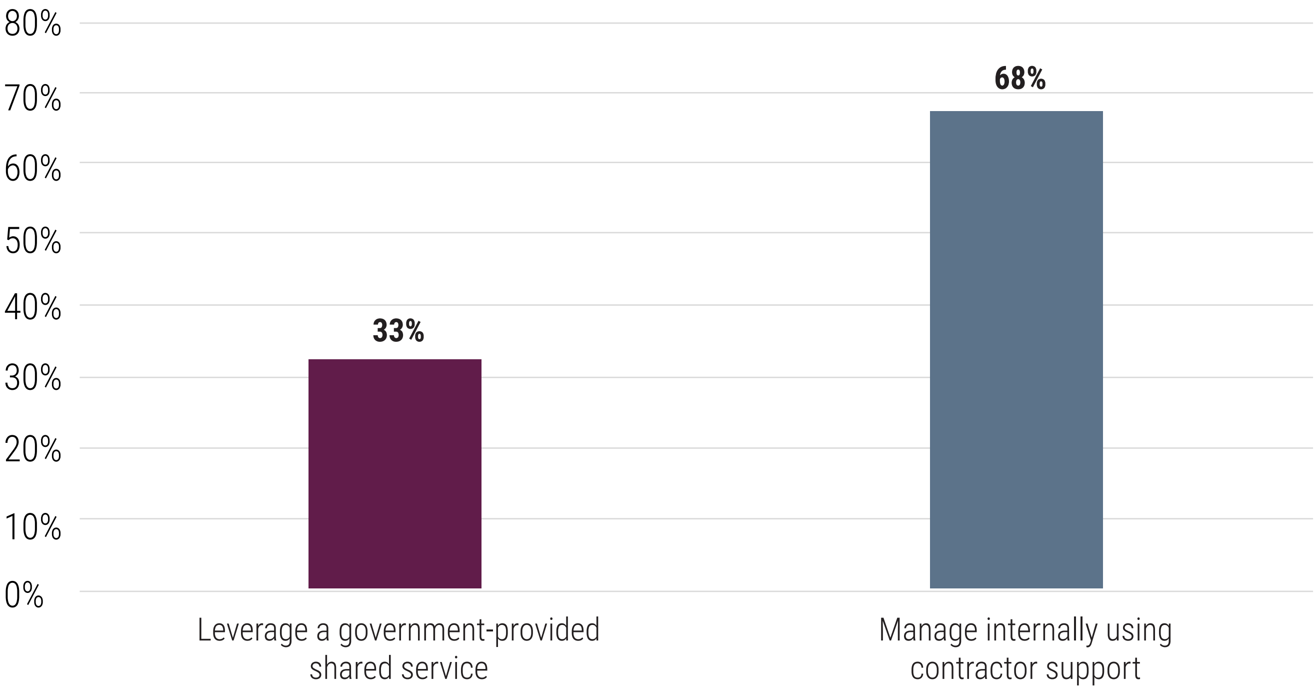


Q4. Which of the following cybersecurity services do you consider worth paying a premium for? Select all that apply. Total (n=200)

Cyber Spending & Budget

SECURITY OPERATION CENTER SERVICES

Most manage their security operation centers internally, using contractor support.


80%
70%
60%
50%
40%
30%
20%
10%
0%
33%
68%
Leverage a government-provided shared service
Manage internally using contractor support

Q13. In terms of Security Operations Center services, which of the following better describes what you do? Total (n=200)

This document and the information disclosed within, including the document structure and contents, are confidential and the proprietary property of Ernst & Young LLP and are protected by copyright and other proprietary rights. Any disclosure to a third party in whole or in part in any manner is expressly prohibited.

Cyber Spending & Budget

PREPARATION AND FUNDING OF FUTURE CYBER OPERATIONS

"An annual budget for IT infrastructure and cybersecurity."

"Provides an all-Inclusive risk-based vulnerability management solution."

Top responses shown	Total	FedCiv	DoD
External budget approval	17%	17%	16%
Cybersecurity (meeting needs, improving, discussing needs, etc.)	16%	16%	16%
Vulnerability prioritization assessment/risk assessment	15%	12%	17%
Addressing and fixing threats/Vulnerabilities	15%	15%	14%
Training/Updating agencies/Testing/Continual planning	15%	10%	20%
Internal budget concerns	13%	11%	15%
Practice Zero trust/Follow federal guidelines	13%	10%	16%
Threat intelligence/Keep an eye out for future threats	12%	10%	14%

○ = significant difference between segments

"Review services that will meet our security requirements."

"Conduct virtual workshops, briefings and sessions."

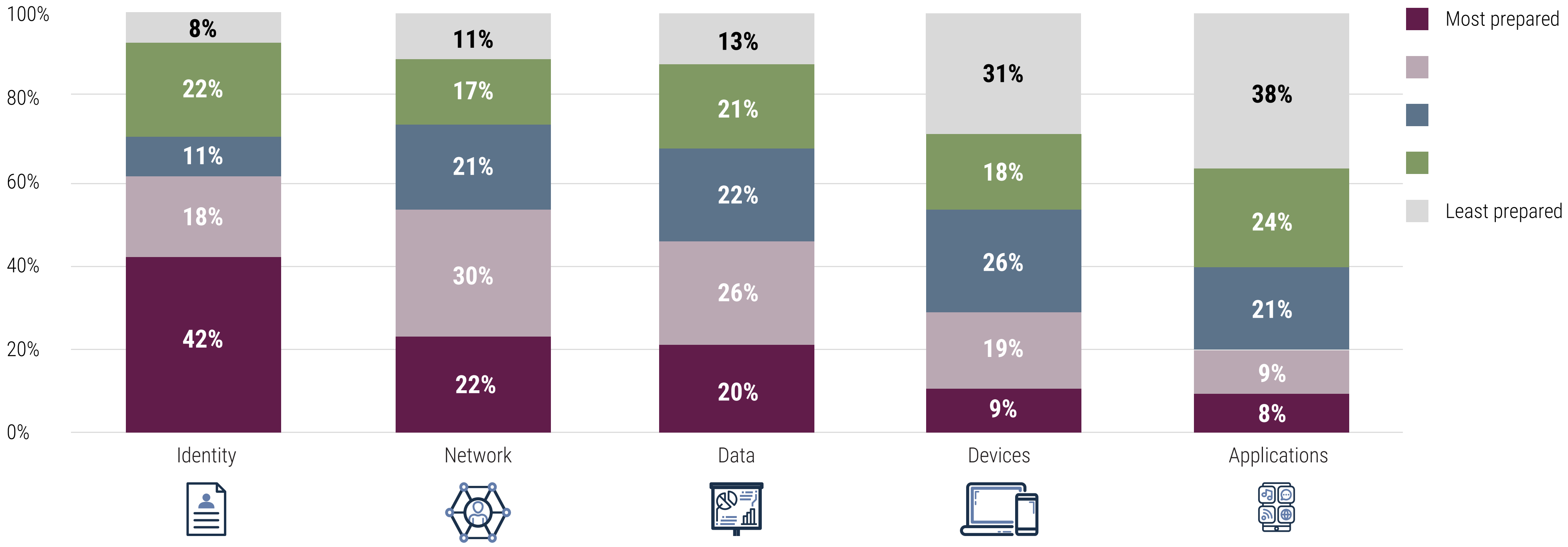
Q16. How does your CISO prepare for future cyber operations and how are future operations funded? Total (n=200), FEDCIV (n=100), DOD (n=100)

Cyber Programs and Maturity

Cyber Programs and Maturity

PREPAREDNESS FOR CISA'S FIVE PILLARS OF ZERO TRUST

Respondents report lack of preparedness for four of the five pillars of trust. 42% are "very" prepared for "identity" (another 18% are somewhat prepared). Less than a quarter feel very prepared for "network" and "data" (22% and 20% respectively). Just 9% are very ready for "devices" and "applications." More alarming, three in ten are not at all prepared for devices and nearly four in ten (38%) say they are not at all prepared on the application pillar.

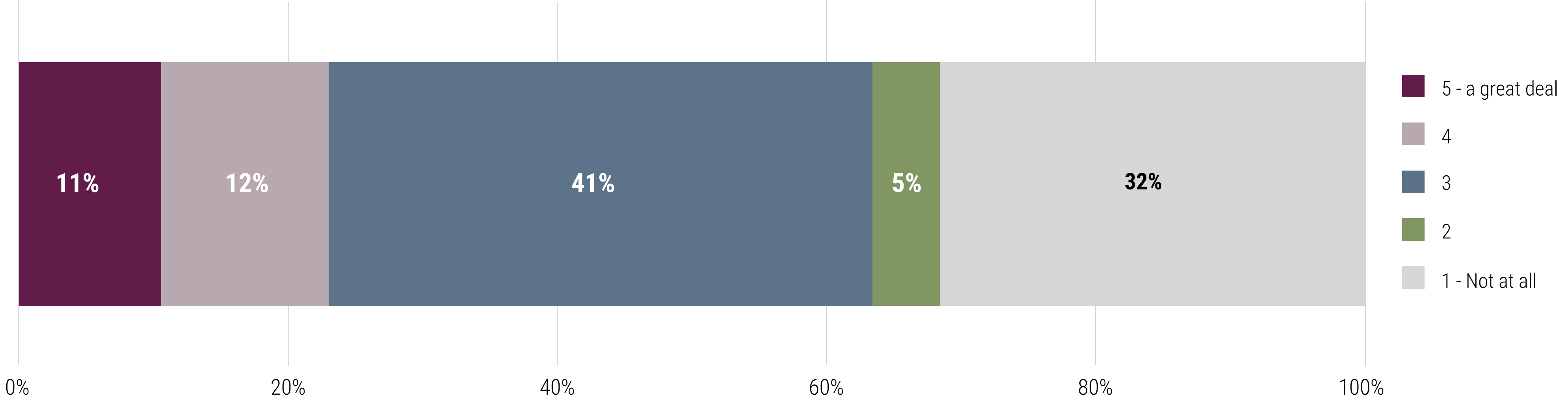


Q5. Please rank order the five pillars of Zero Trust in terms of your agency's preparedness where 1 means most prepared and 5 means least prepared. Total (n=200),

Cyber Programs and Maturity

USE OF CISA'S QUALITY SERVICES MANAGEMENT OFFICE OFFERINGS

CISA's Cyber QSMO is the single shared service office for managing cybersecurity solutions for the U.S. Government **Most respondents do not use the QSMO offerings very much, with a third saying they do not use the offerings at all.**



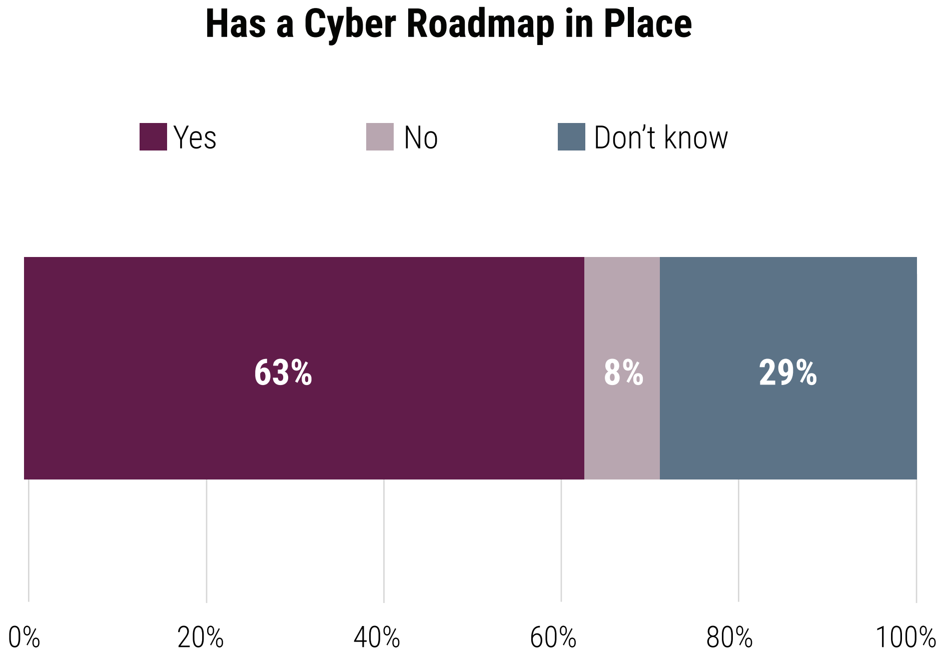
Q6. How much have you used the shared cybersecurity offerings of the Federal Cyber QSMO (Quality Services Management Office)? Please use a five point scale where 1 means you haven't used it at all and 5 means you use it a great deal. Total (n=200),

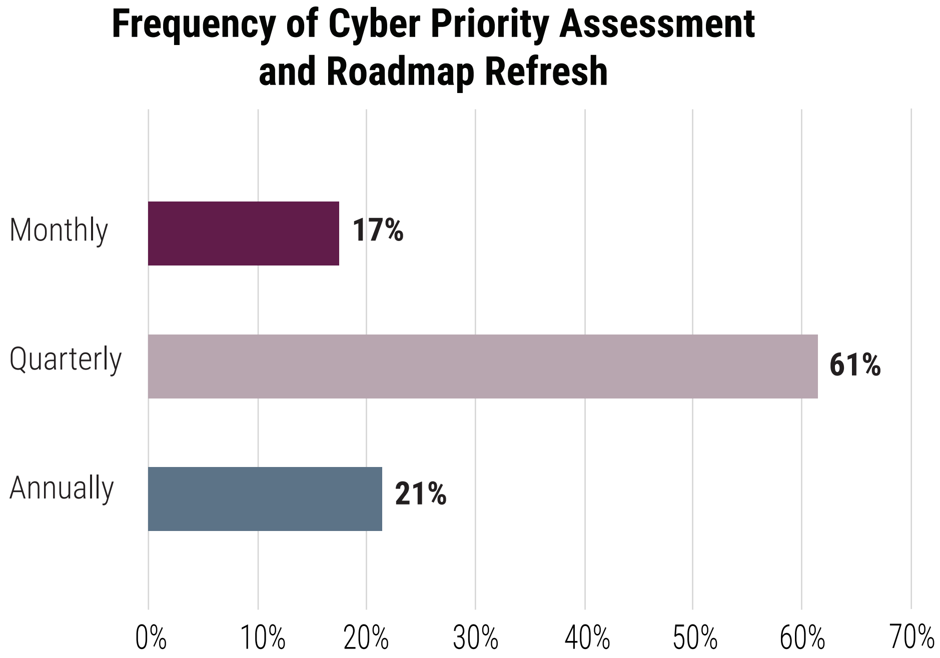
This document and the information disclosed within, including the document structure and contents, are confidential and the proprietary property of Ernst & Young LLP and are protected by copyright and other proprietary rights. Any disclosure to a third party in whole or in part in any manner is expressly prohibited.

Cyber Programs and Maturity

CYBER ROADMAPS

Nearly two thirds have both a cyber roadmap in place. Of those with a cyber roadmap, most (61%) assess their cyber priorities quarterly.



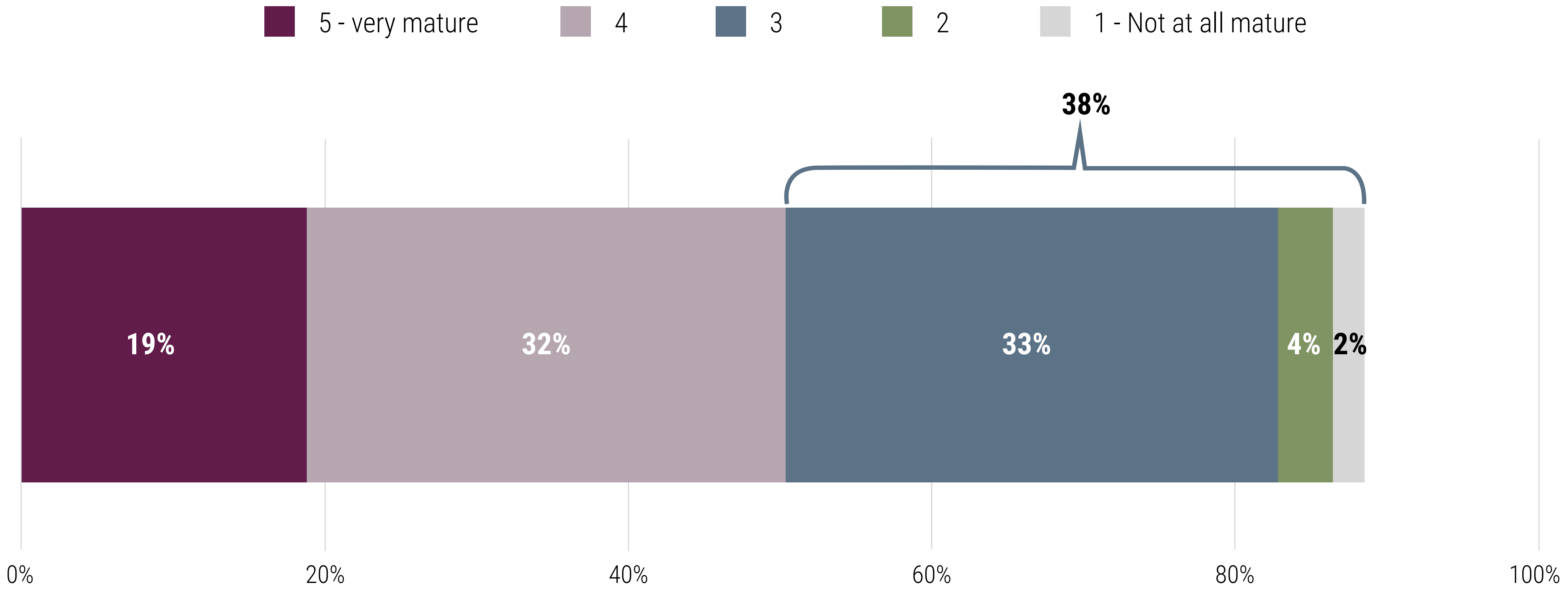


Q7. Does your agency have a cyber roadmap in place? Total (n=200).
Q8. How often do you assess your cyber priorities and refresh your roadmap? Total (n=126)

Cyber Programs and Maturity

CYBER THREAT INTEL PROGRAM MATURITY

One in five rate their cyber threat intel program as “very” mature; another third say their program is “somewhat mature.” Still, nearly four in 10 rate their program as a three or below.



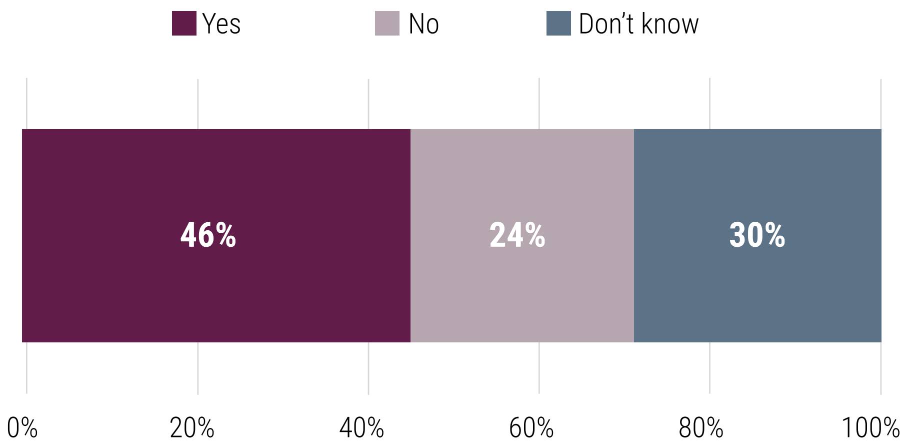
Q11. How mature is your Cyber Threat Intel Program? Please use a five point scale where 1 means not at all mature and 5 means very mature. Total (n=200)

Cyber Programs and Maturity

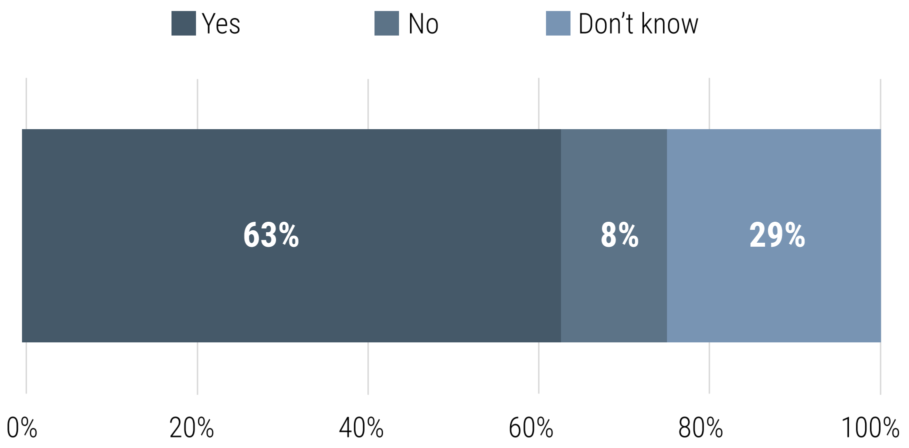
SUPPLY CHAIN RISK MANAGEMENT

Fewer than half have a supply chain risk management program, but two thirds have a cyber program that focuses on OT. Perhaps more tellingly, sizeable minorities (somewhere between 25%-30%) do not know whether their agencies have these functionalities (cyber roadmaps, a cyber program that focus on IT, a supply chain risk management program or a cyber table-top exercise).

Has a Supply Chain Risk Management Program



Has a Cyber Program Focused on Operational Technology

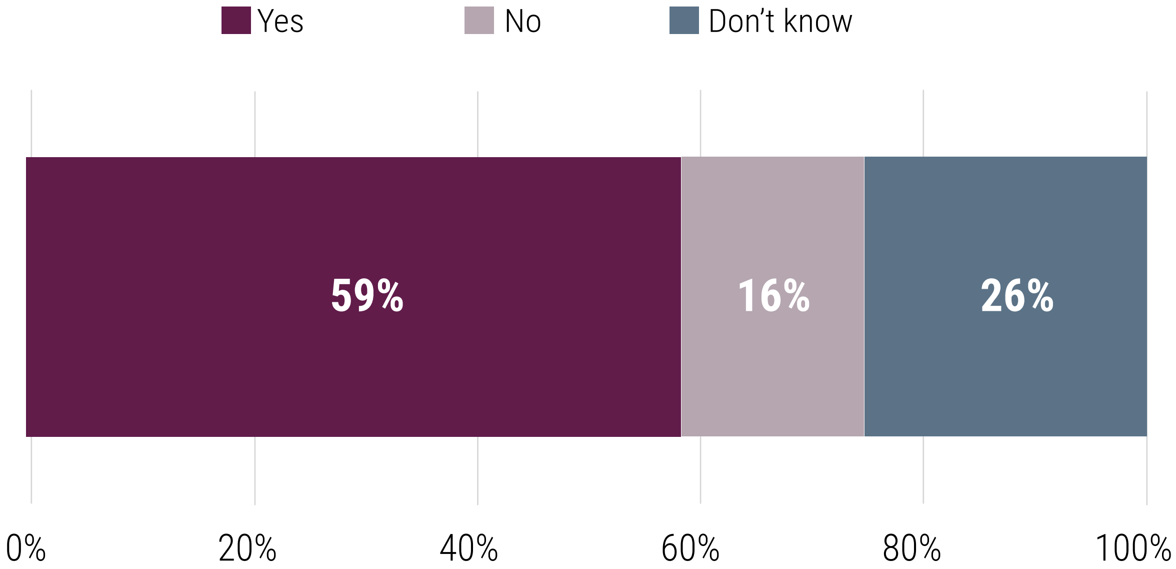


Q9. Does your agency currently have a Supply Chain Risk Management program in place? Total (n=200)
Q10. Does your agency have a cyber program focused on Operational Technology (OT)? Total (n=200),

Cyber Programs and Maturity

CYBER TABLE-TOP EXERCISE

A majority have conducted a cyber table-top exercise in the past year, but more than a quarter do not know whether they have or not.

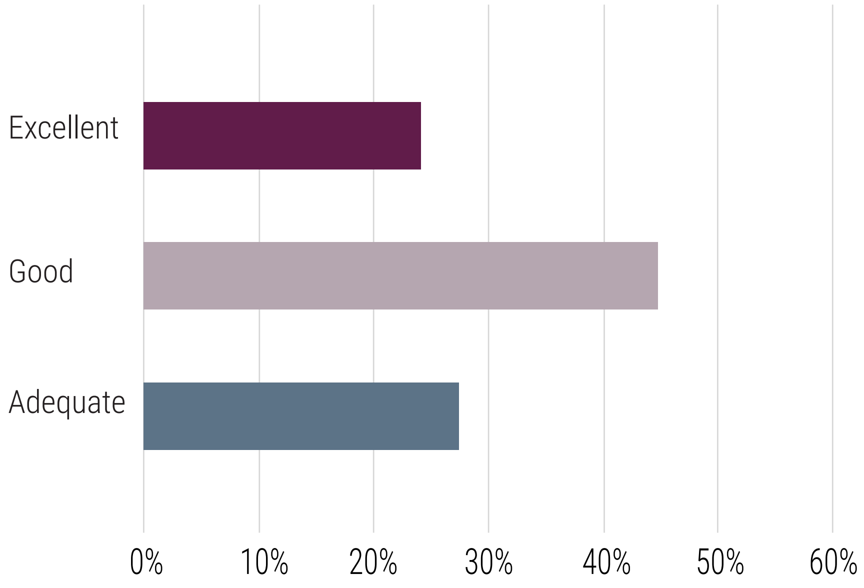


Q15. Have you conducted a cyber "table top" exercise in the last year? Total (n=200).

Cyber Programs and Maturity

END POINT DETECTION PROGRAM

Nearly all rate their End Point Detection Program as adequate or better. A quarter believe their program is “excellent.” Just 2% (not pictured below) rate their program as poor/non-existent.

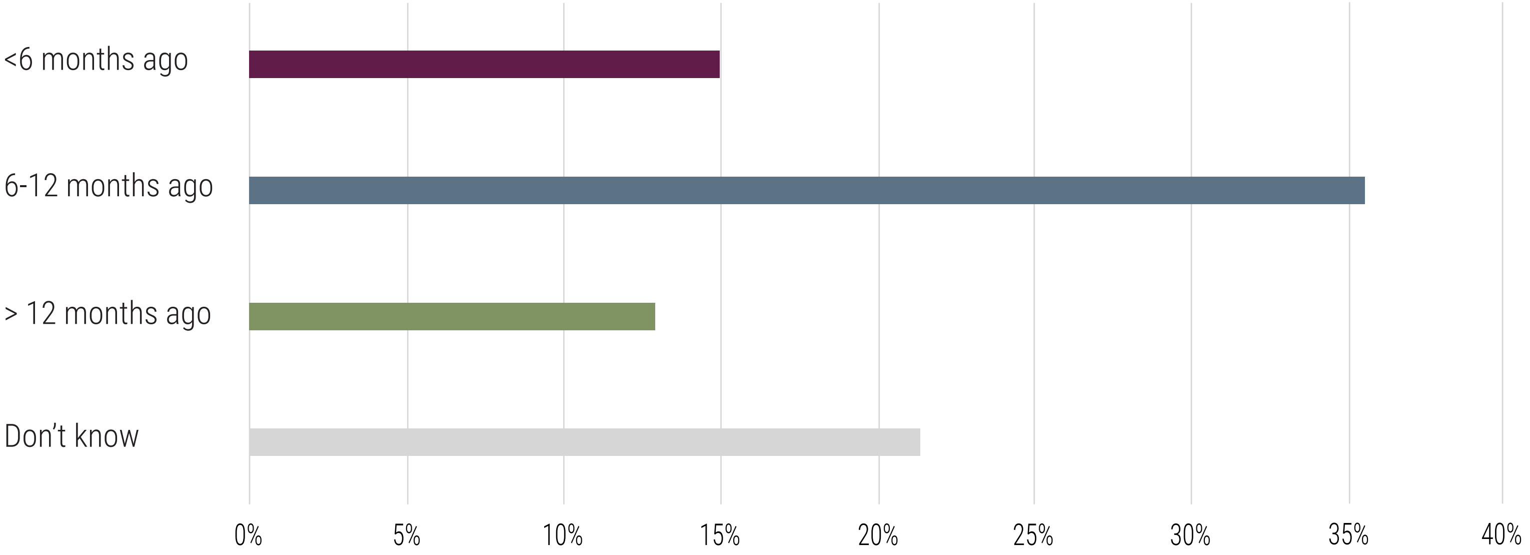


Q12. How would you rate your End Point Detection program? Total (n=200),

Cyber Programs and Maturity

DISASTER RECOVERY/CONTINUITY OF OPERATIONS PLAN

Two thirds have updated their disaster plans within the past year (three in ten have updated in the past six months).



Q14. When was the last time you updated your disaster recovery/continuity of operations plan? Total (n=200)

Industry POV

Industry POV

IS YOUR AGENCY PREPARED TO DETECT AND RESPOND TO A CYBER EVENT?

Conduct a cyber tabletop training exercise each year, and include multiple stakeholders from the start

Large multiagency tabletop exercises have shown how preparation for a cyber response helps organizations enhance their cybersecurity posture. Including multiple groups, such as legal, public affairs and business units, into tabletop exercises is critical for success.

Prioritize and implement a cyber supply chain risk management (SCRM) program – early detection of supplier risks will enable risk-informed decisions

With continued federal government requirements for stronger SCRM, agencies must prioritize SCRM and establish programs to mitigate risk as supply chains are increasingly targeted by adversaries.

Cyber threat intelligence (CTI) programs are essential – actionable intelligence tailored to your agency needs

CTI enables effective decision-making to mitigate information security risks. CTI is not just an indicator of compromised feeds or detection signatures. It is a holistic program designed to inform information security risk mitigation and provides the foundation for threat hunting, controls design for defense in depth and other risk mitigation strategies.

Be prepared across all five pillars of zero trust – establish a security framework that covers all aspects of zero trust

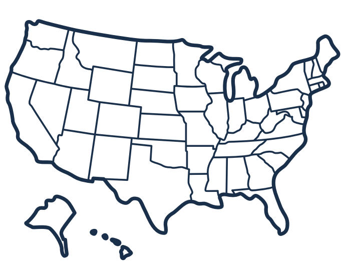
Zero trust frameworks and use cases vary by organization and function. EY teams are helping multiple agencies focus on business and cyber use cases with zero trust solutions across the five pillars to include mapping to the DHS CISA Zero Trust Maturity Model.

Respondent Characteristics

Respondent Characteristics

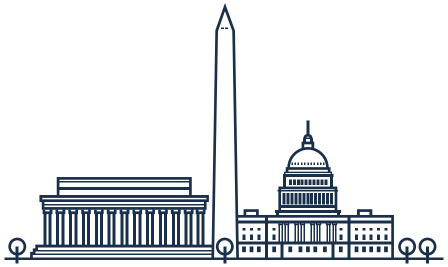
WORK LOCATION

In Which State Do You Work?



Region	Total	FedCiv	DoD
South	56%	58%	54%
Northeast	18%	21%	15%
West	16%	12%	20%
Midwest	10%	9%	11%

Do You Live or Work in the DC Metro Area?



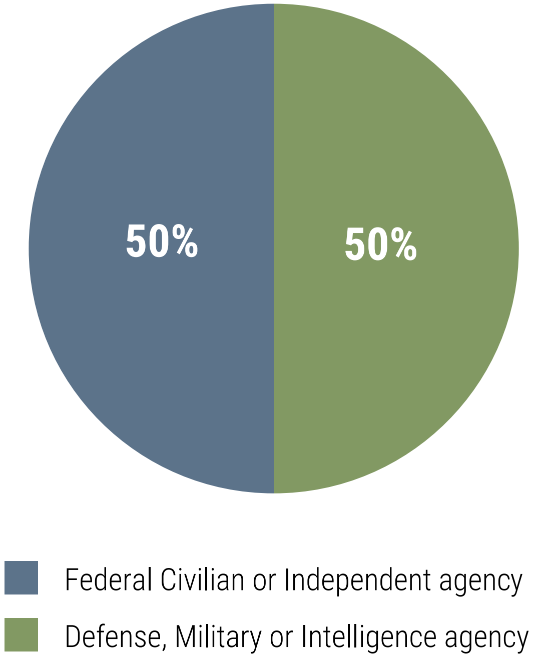
	Total	FedCiv	DoD
Yes	44%	48%	40%
No	56%	52%	60%

C1. In which state do you work? Total (n=200), FEDCIV (n=100), DOD (n=100)
C2. Do you live or work in the Washington DC metro area? Total (n=200), FEDCIV (n=100), DOD (n=100)

Respondent Characteristics

ORGANIZATION TYPE & ROLE

Organization Type



Role/Function in Organization

	Total	FedCiv	DoD
Administration/operations	21%	24%	18%
Program/project management	21%	16%	25%
IT manager	18%	16%	20%
IT specialist	17%	16%	18%
IT decision maker	10%	8%	12%
Security management	8%	11%	4%
Executive management/command	4%	4%	3%
Chief Technology Officer (CTO)	1%	1%	--
Chief Information Officer (CIO)	--	--	--
Chief Information Security Officer (CISO)	--	--	--
Chief Risk Officer (CRO)	--	--	--
Other	2%	4%	--

S1. What type of organization do you work for? Total (n=200)
S5. Which of the following best describes your job role/function in your organization? Total (n=200), FEDCIV (n=100), DOD (n=100)

Respondent Characteristics

Involvement in Selecting Firms Implementing IT and Digital Services

	Total	FedCiv	DoD
Have direct experience working with providers to implement solutions	60%	65%	54%
Have direct involvement in recommending or selecting solutions and providers	58%	51%	65%
Develop contract requirements, or recommending/selecting solutions and providers	44%	40%	47%
Make the final decision/approve solutions/providers	19%	22%	15%
None of the above	7%	10%	4%

○ = significant difference between segments

Involvement in Management and Selection of Hired Firms Implementing IT and Digital Services

	Total	FedCiv	DoD
Routine interaction with providers to accomplish work	72%	74%	69%
Management or providers delivering consulting and/or IT solutions	59%	55%	62%
Executive-level oversight of programs or projects	25%	21%	28%
None of the above	2%	2%	1%

S6. In which of the following ways are you involved in your organization's selection of firms that implement IT and digital services? Total (n=200), FEDCIV (n=100), DOD (n=100)
S7. In which of the following ways are you or have you been involved in your organization's management and selection of firms that implement IT and digital services once the firm has been hired by your agency? Total (n=200), FEDCIV (n=100), DOD (n=100)

Respondent Characteristics

GOVERNMENT DEPARTMENT OR AGENCY: CIVILIANS

	FedCiv
Veterans Affairs	16%
Treasury	10%
Energy	7%
Postal Service	7%
Commerce	6%
OPM	6%
Transportation	6%
Homeland Security	5%
Agriculture	4%
GSA	4%
HHS	4%

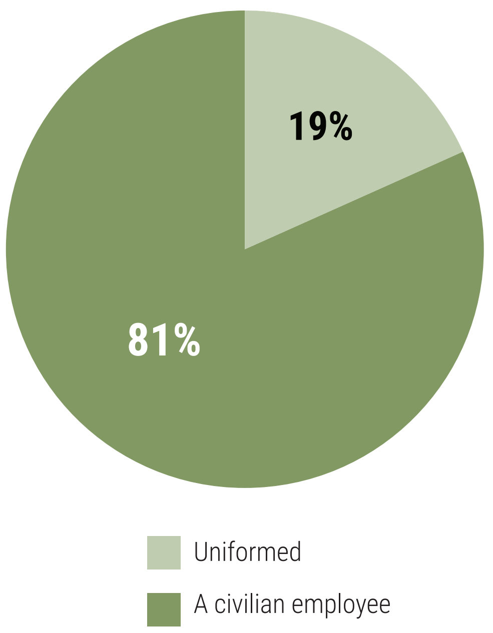
	FedCiv
Labor	4%
TVA	4%
Executive Office of the President	3%
NASA	3%
SSA	3%
HUD	2%
Justice	2%
Education	1%
EPA	1%
Interior	1%
State	--
Other	1%

S2. In which Government Department or Agency do you work? FEDCIV (n=100)

Respondent Characteristics

GOVERNMENT DEPARTMENT OR AGENCY: DEFENSE

Government Department or Agency	DoD
Army	28%
Air Force	24%
Marines	21%
Navy	15%
Intelligence Agencies (NRO, NSA, DIA, etc.)	5%
Coast Guard	4%
Office of the Secretary of Defense & Joint Commands	1%
Space Force	1%
Other	1%



S3. In which Government Department or Agency do your work? DOD (n=100)
S4. Are you…? DOD (n=100)

About

EY

EY government and public sector consulting services provides support to transform programs and optimize operations to achieve mission outcomes. We solve complex challenges for federal, state, and local governments and education institutions. Through the enablement of technology and the use of data, we help government agencies with transformation and modernization initiatives to better serve the public.

To learn more, visit www.ey.com/govmod

Market Connections™
Research you can act on.
A portfolio platform of GovExec

Market Connections, a portfolio platform of GovExec, delivers actionable intelligence and insights that enable improved business performance and positioning for leading businesses, trade associations, and the public sector. The custom market research firm is a sought-after authority on preferences, perceptions, and trends among the public sector and the contractors who serve them, offering deep domain expertise in information technology and telecommunications, healthcare, and education.

To learn more, visit www.marketconnectionsinc.com