EY federal AI and cyber survey

January 2026

The better the question. The better the answer. The better the world works.

Shape the future with confidence

Contents

01

Methodology

Methodology

Primary objectives

1. Measure adoption and integration of responsible artificial intelligence (AI) in cybersecurity
2. Identify use cases, challenges and oversight practices
3. Assess organizational maturity and future readiness

Market Connections and Ernst & Young LLP (EY US) collaborated to design an online survey of 200 federal government IT decision-makers and influencers who are involved in AI or cybersecurity, fielded in August 2025.

02

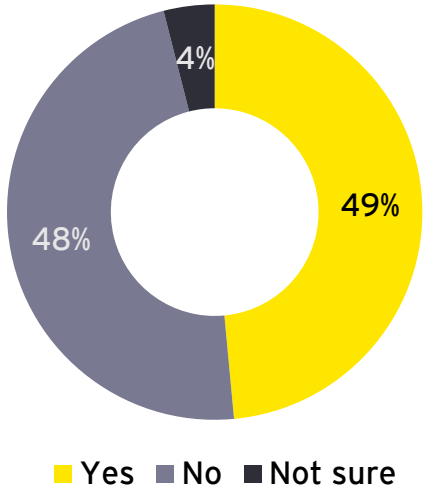
AI adoption

Status of responsible AI practices in federal cybersecurity

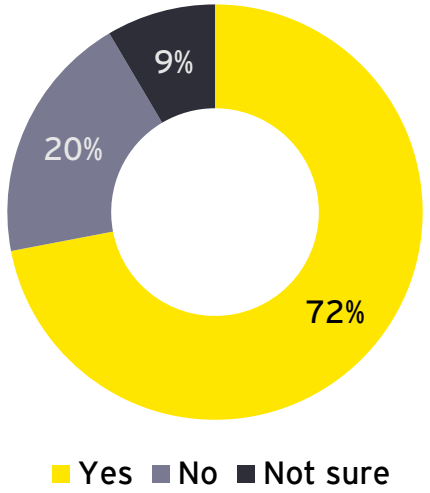
While nearly six in 10 respondents have implemented at least informal responsible AI leading practices, less than half integrate them specifically into cybersecurity operations. However, nearly three-quarters intend to expand the use of AI for cybersecurity over the next one to three years.

Responsible AI implementation

Current cyber integration



Plans to expand AI use in cybersecurity

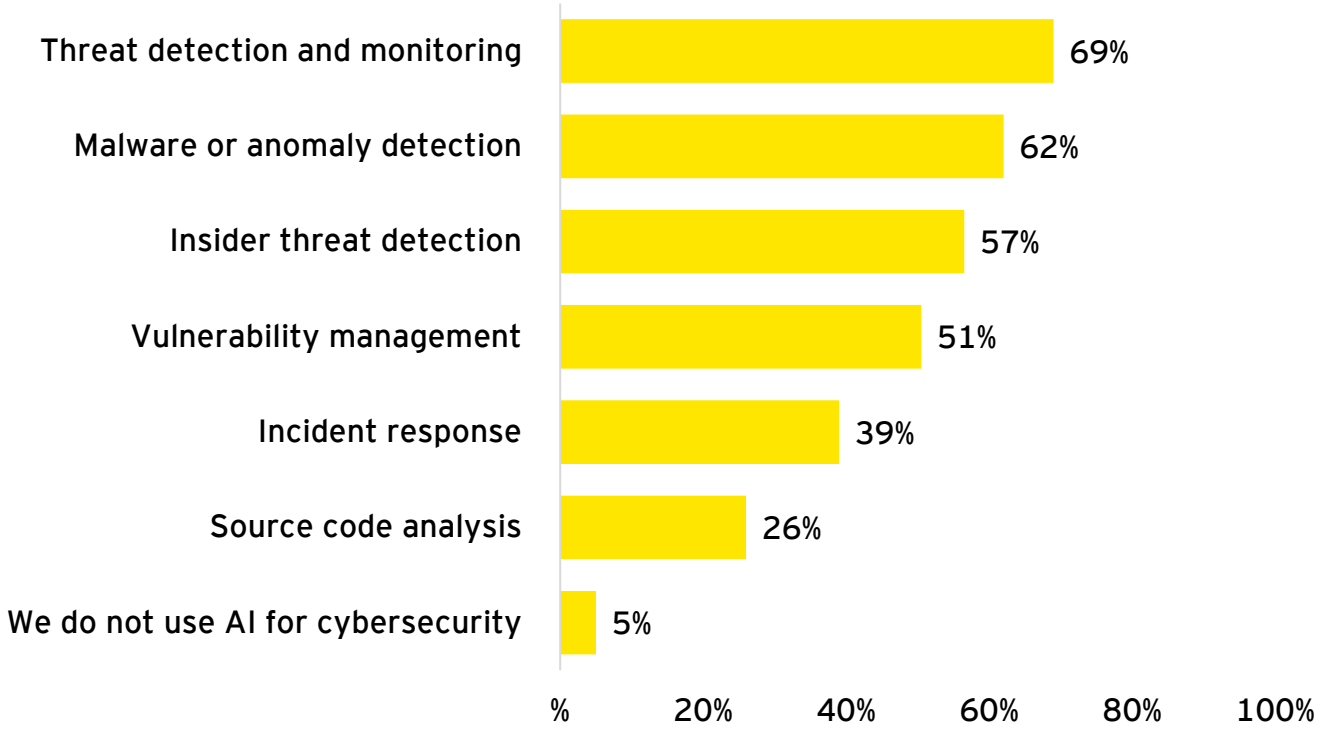


Q *Has your organization implemented responsible AI best practices?*
Does your organization integrate responsible AI practices specifically into cybersecurity operations?
Does your organization have a formal plan to expand the use of AI for cybersecurity over the next one to three years?

Note: Totals may not appear to sum due to rounding.

AI use by cybersecurity mission

Overall, AI is used most frequently for threat detection and monitoring, followed by malware or anomaly detection. Civilian respondents reported using AI more for vulnerability management.



	Defense	Civilian
Threat detection and monitoring	70%	68%
Malware or anomaly detection	66%	59%
Insider threat detection	49%	62%
Vulnerability management	40%	58%
Incident response	36%	41%
Source code analysis	25%	27%
We do not use AI for cybersecurity	6%	4%

= significant difference between segments

Q *For what cybersecurity missions is your organization currently using AI? Select all that apply.*

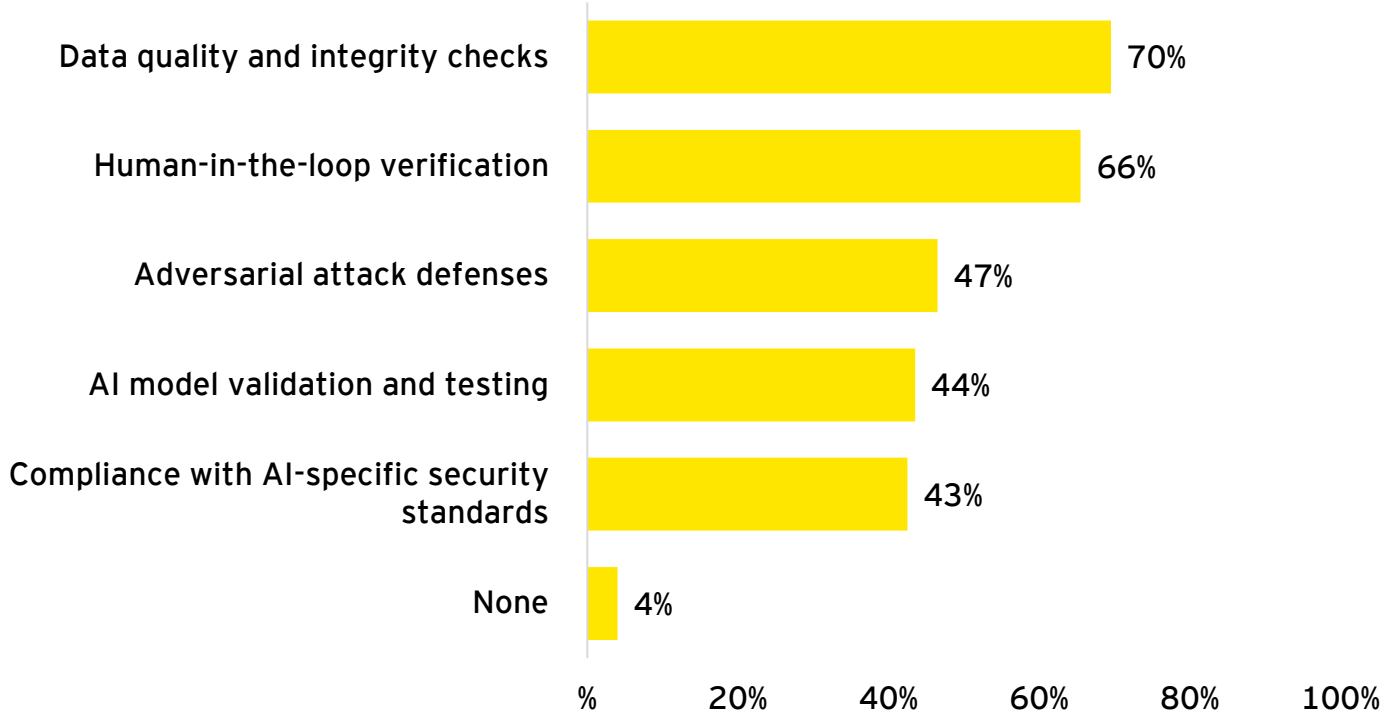
Note: Totals may not appear to sum due to rounding.

03

Risk and barriers

AI-related cyber risk mitigation measures

Data quality and integrity checks and human-in-the-loop verification are the most frequently implemented cybersecurity risk mitigation measures.



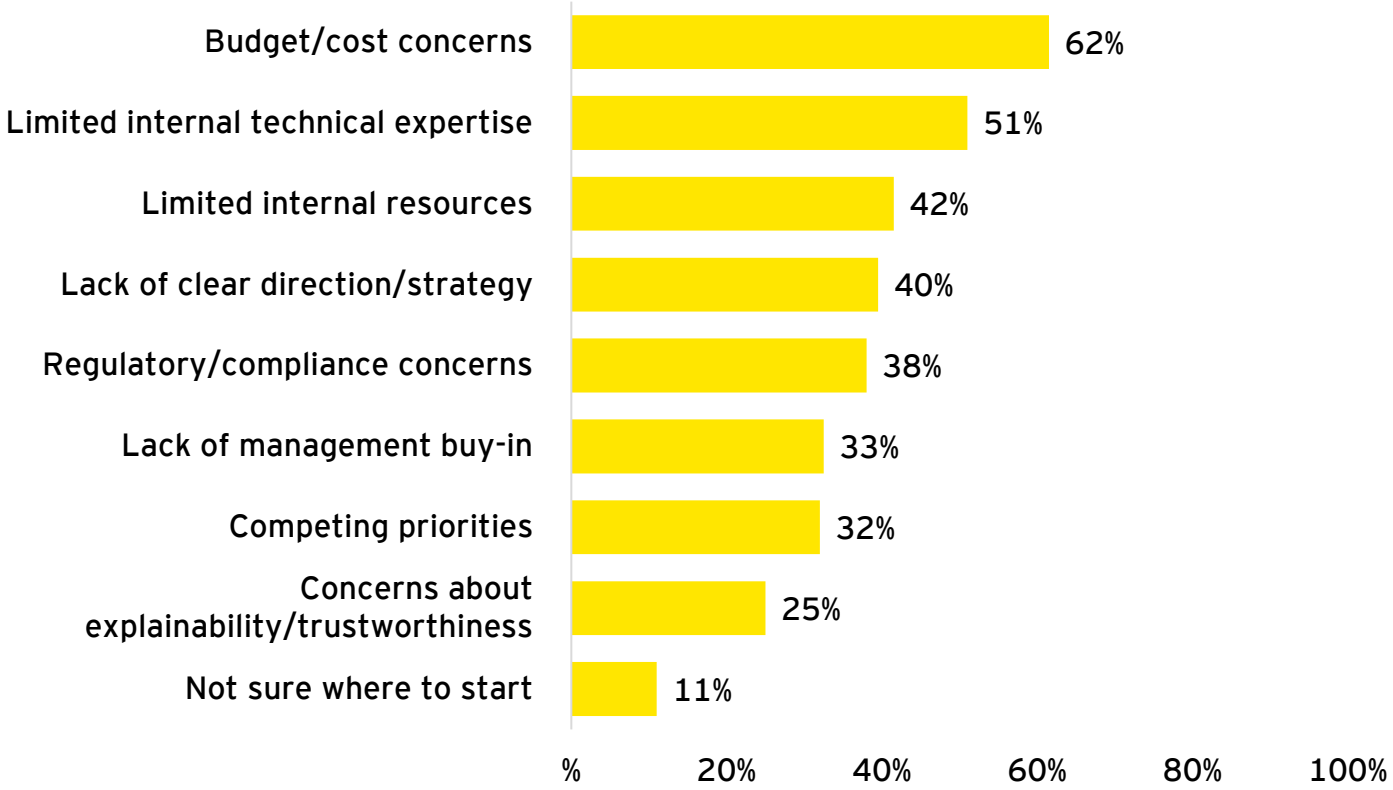
	Defense	Civilian
Data quality and integrity checks	65%	73%
Human-in-the-loop verification	71%	62%
Adversarial attack defenses	53%	43%
AI model validation and testing	36%	48%
Compliance with AI-specific security standards	36%	47%
None	4%	4%

Q *Which cybersecurity risk mitigation measures related to AI has your organization implemented? Select all that apply.*

Note: Totals may not appear to sum due to rounding.

Barriers to adopting responsible AI for cybersecurity

Budget/cost concerns are the top barrier to adopting or expanding AI for cybersecurity, followed by a lack of internal technical expertise and resources.



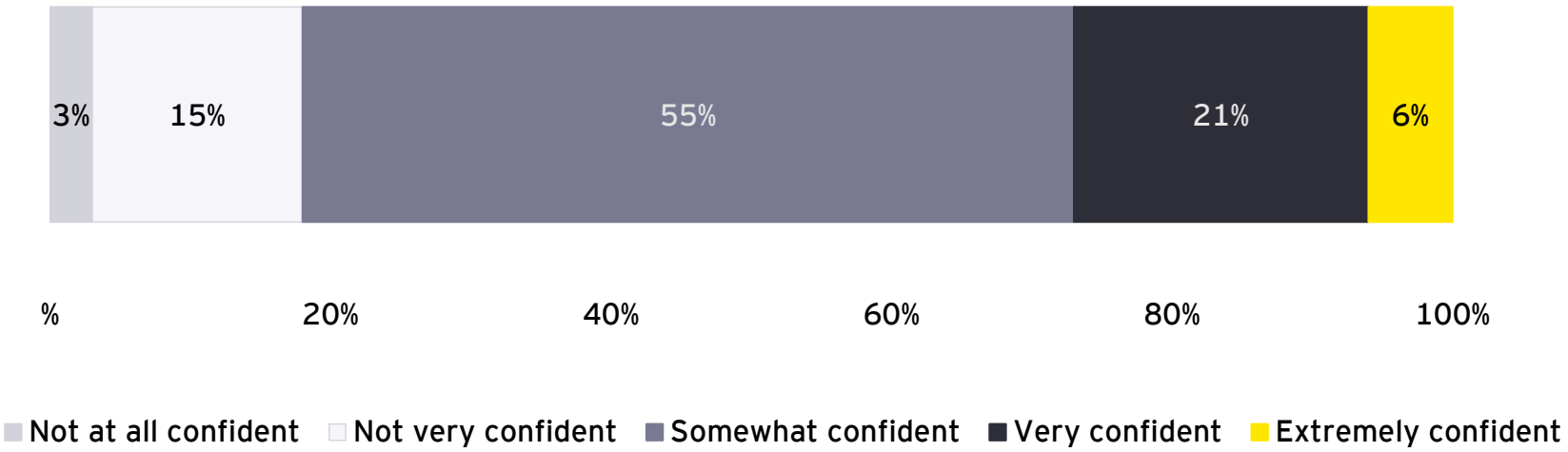
	Defense	Civilian
Budget/cost concerns	59%	63%
Limited internal technical expertise	48%	53%
Limited internal resources	38%	44%
Lack of clear direction/strategy	39%	40%
Regulatory/compliance concerns	41%	36%
Lack of management buy-in	34%	32%
Competing priorities	36%	29%
Concerns about explainability/trustworthiness	29%	23%
Not sure where to start	11%	11%

Q *What are the biggest barriers your organization faces in adopting or expanding responsible AI for cybersecurity? Select all that apply.*

Note: Totals may not appear to sum due to rounding.

Confidence in managing AI-related cyber risks

Only roughly a quarter are extremely or very confident in their organization's ability to manage AI-related cybersecurity risks.



Extremely/very confident		
Total	Civilian	Defense
27%	29%	24%

Q *How confident is your organization in its ability to manage AI-related cybersecurity risks?*

Note: Totals may not appear to sum due to rounding.

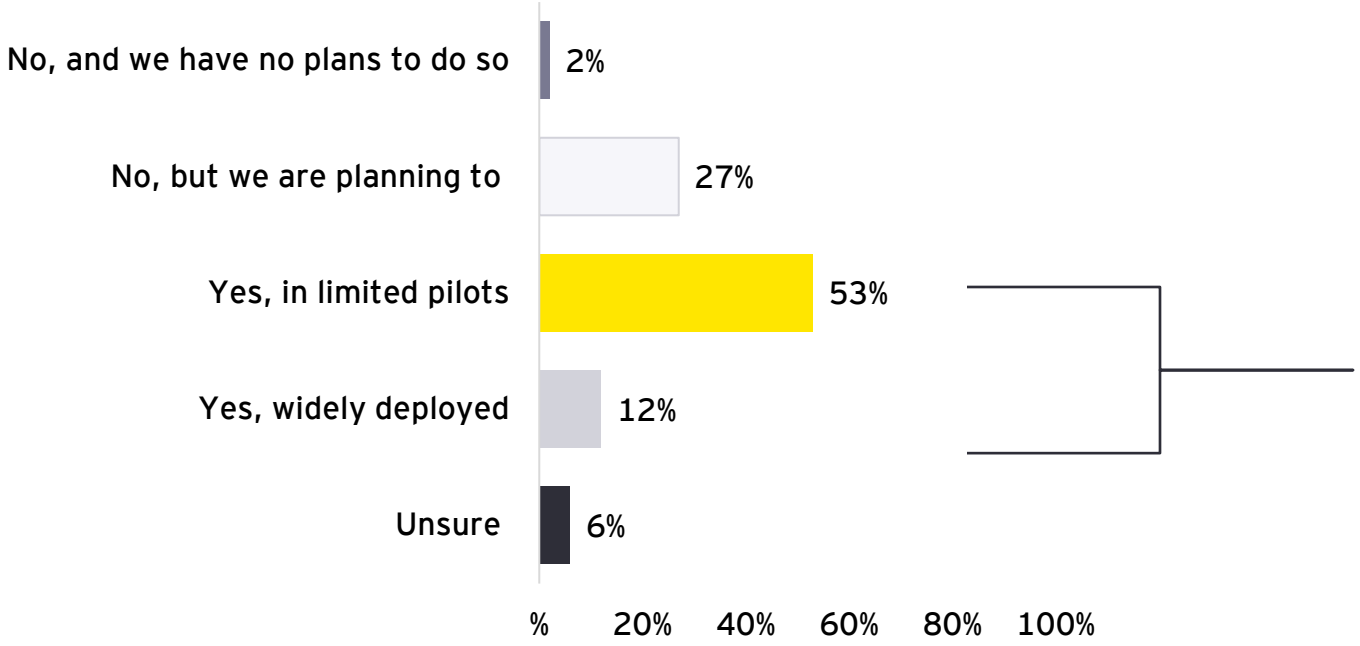
04

Deployment and oversight

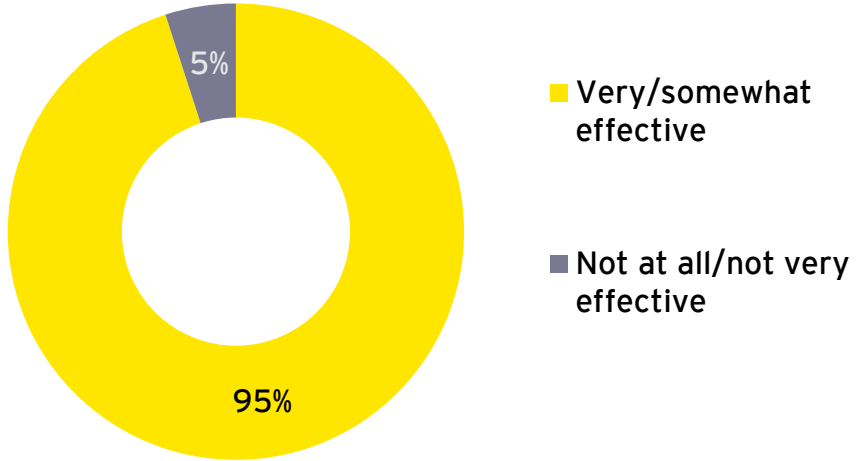
Use and impact of AI in cybersecurity operations

Nearly two-thirds are using AI or machine learning (ML) tools to support cybersecurity operations, and those who do perceive them to be effective. However, these tools are not yet widely deployed, with most being in limited pilots.

AI/ML usage for cybersecurity



Perceived effectiveness of AI



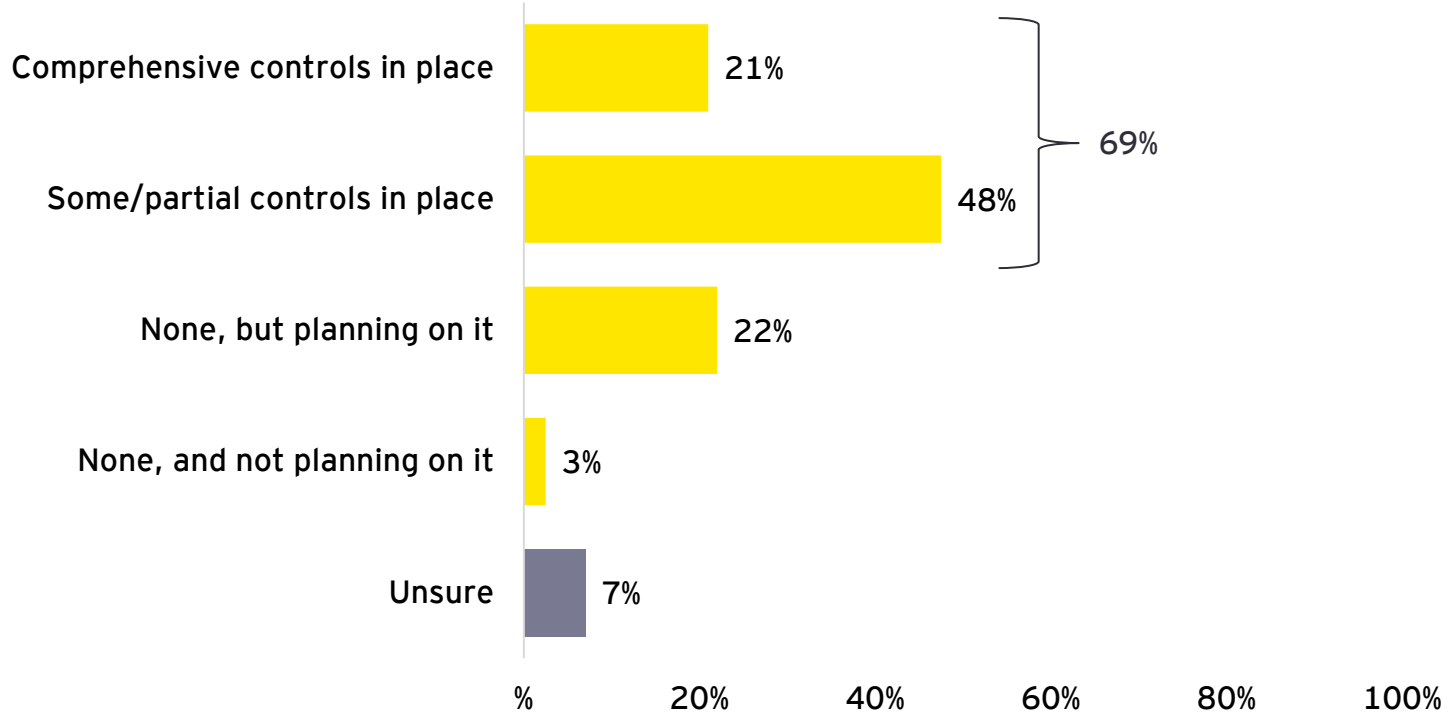
Note: based to those who are using, N=130

Q *Is your organization currently using AI or machine learning tools to support cybersecurity operations (e.g., threat detection, anomaly detection or predictive analytics)? How effective has AI been in strengthening your organization's cybersecurity posture?*

Note: Totals may not appear to sum due to rounding.

Policies and controls to mitigate AI risks

Nearly seven in 10 have at least some/partial controls in place to mitigate AI risks, and nearly another quarter are planning on it.

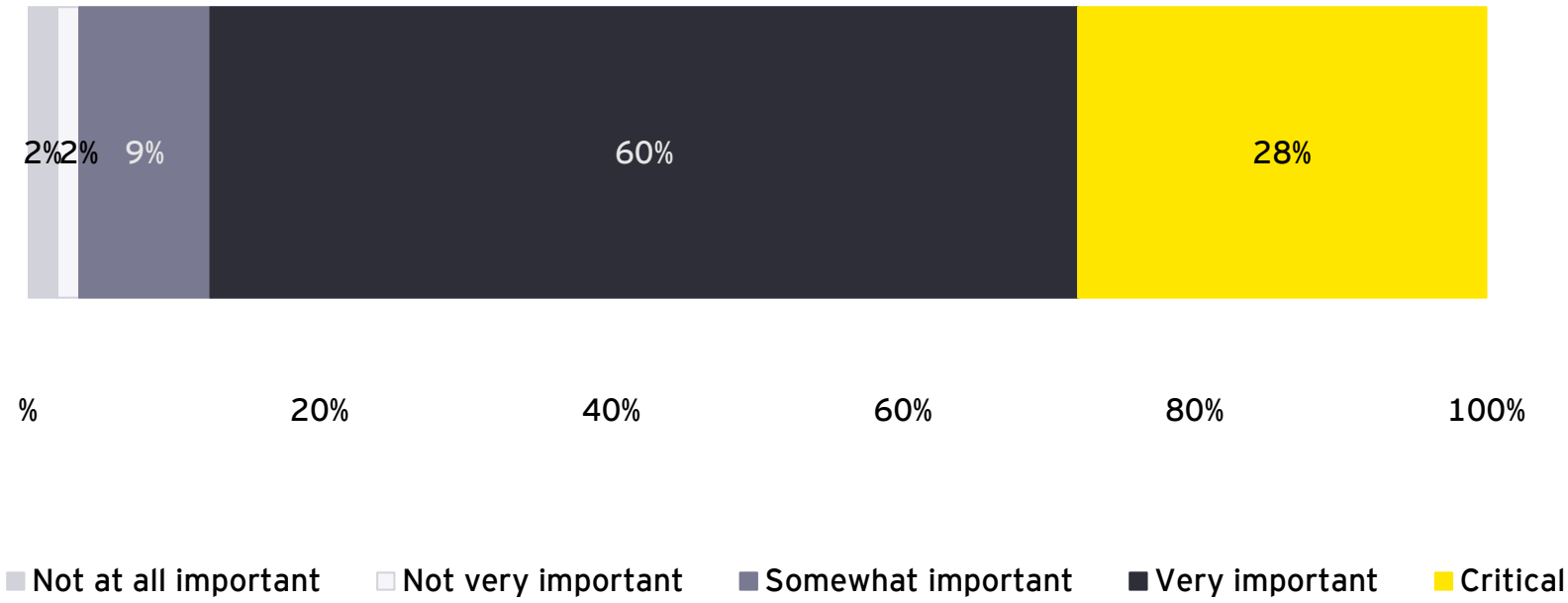


Q *To what extent, if at all, has your organization implemented specific policies or technical controls to mitigate AI risks, such as hallucinations, bias or misuse?*

Note: Totals may not appear to sum due to rounding.

Importance of data privacy in AI adoption strategy

Nearly nine in 10 feel it is critical or very important to consider data privacy and confidentiality — nearly all find it at least somewhat important. Civilian respondents are even more likely to say it is critical or very important.



Critical/very important		
Total	Civilian	Defense
88%	92%	81%

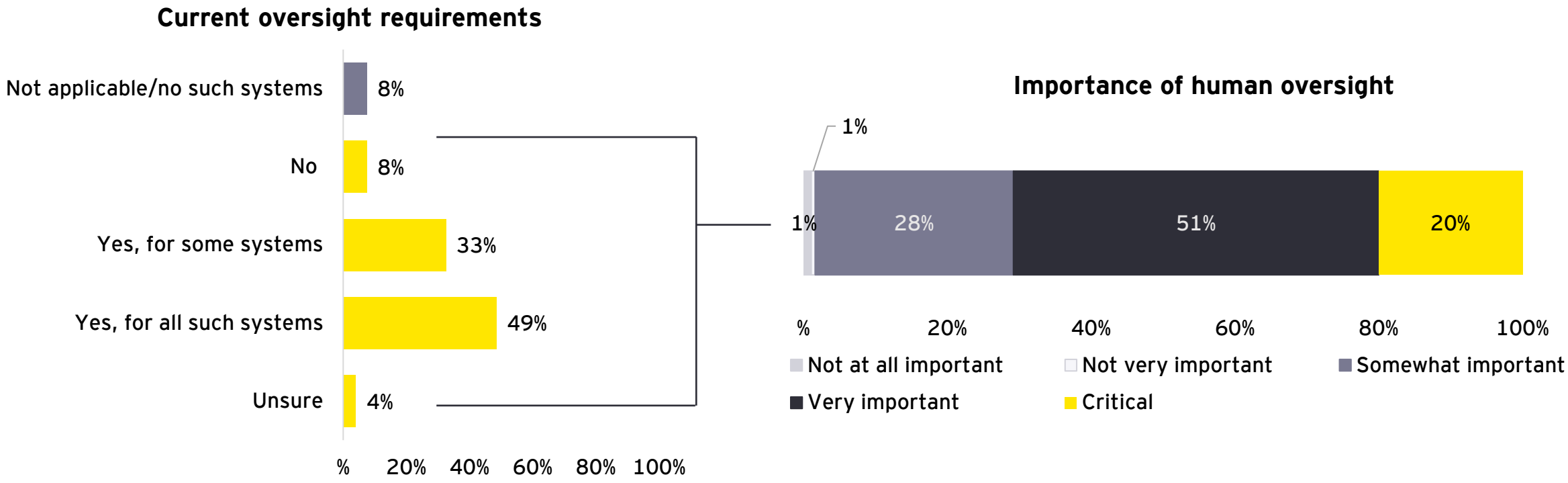
= significant difference between segments

Q *How important are data privacy and confidentiality concerns when considering your organization's AI adoption strategy?*

Note: Totals may not appear to sum due to rounding.

Human oversight of AI in cybersecurity

More than eight in 10 require human oversight for at least some AI systems that impact decisions related to cybersecurity. Only one in five, however, view human oversight as critical.



Q *Does your organization currently require human oversight for AI systems that impact decisions related to cybersecurity?*
How important is it to your organization that there is human oversight for AI systems that impact decisions related to cybersecurity?

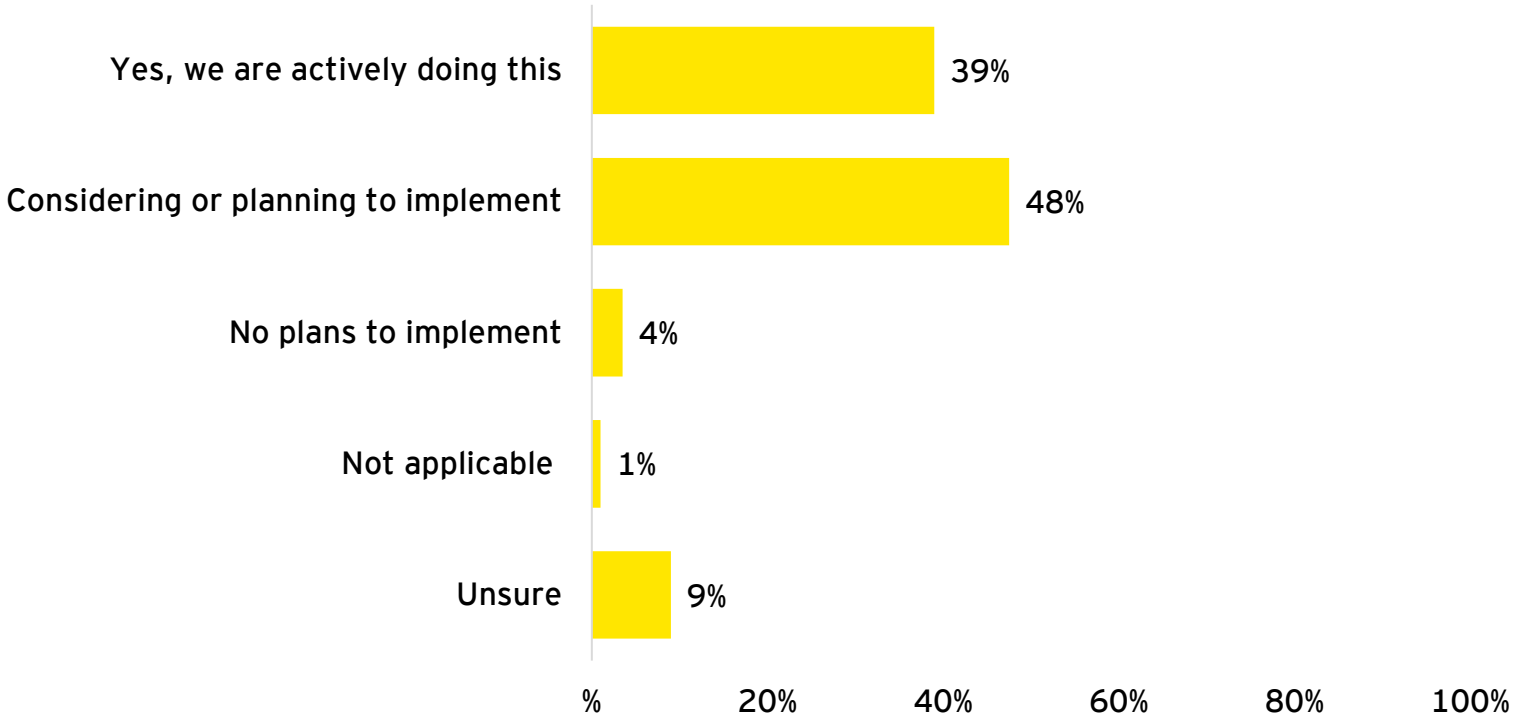
Note: Totals may not appear to sum due to rounding.

05

Maturity and strategy

AI stress testing for security vulnerabilities

Nearly half are considering or planning to implement stress tests on AI systems, while four in 10 already are.

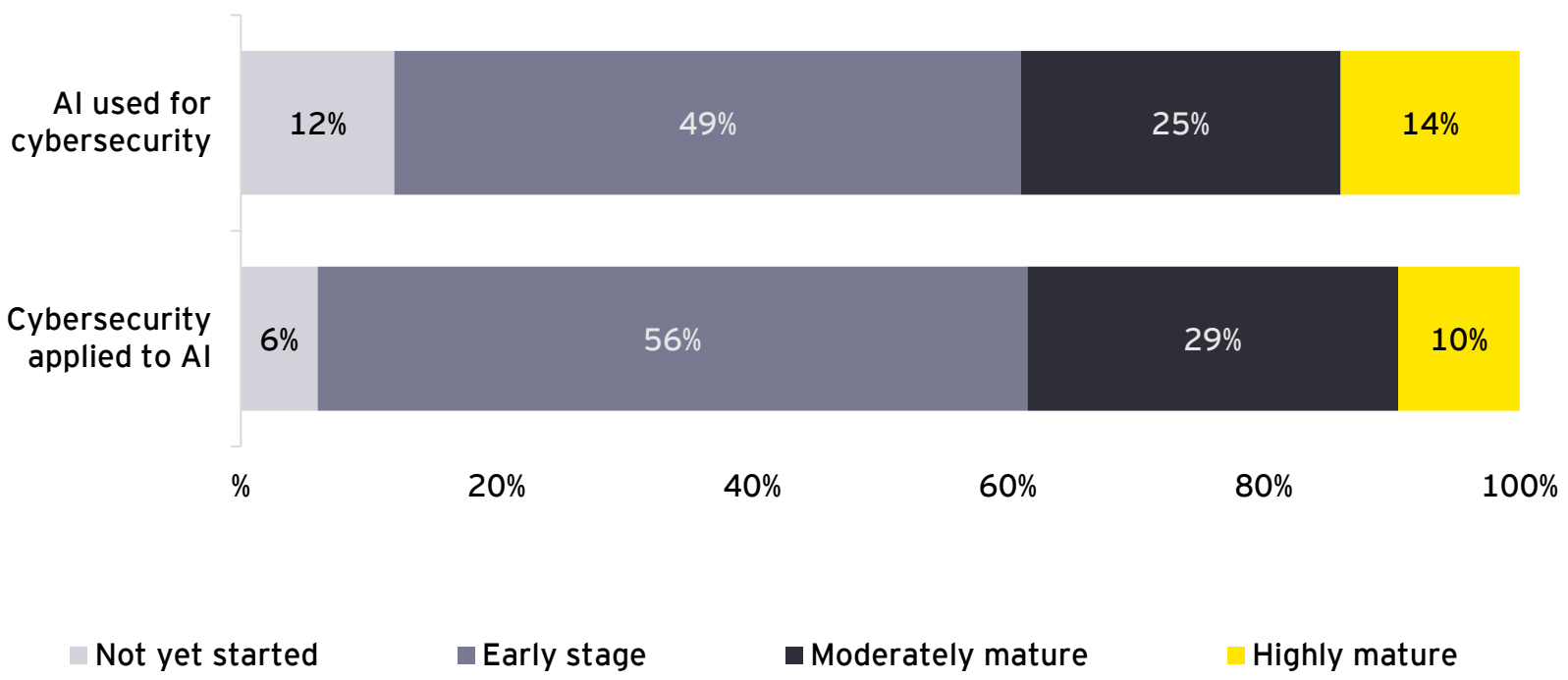


Q *Is your organization using or considering conducting stress tests on AI systems against potential security vulnerabilities?*

Note: Totals may not appear to sum due to rounding.

Secure AI adoption maturity

Both AI used for cybersecurity and cybersecurity applied to AI are largely seen as being in the early stage of maturity.



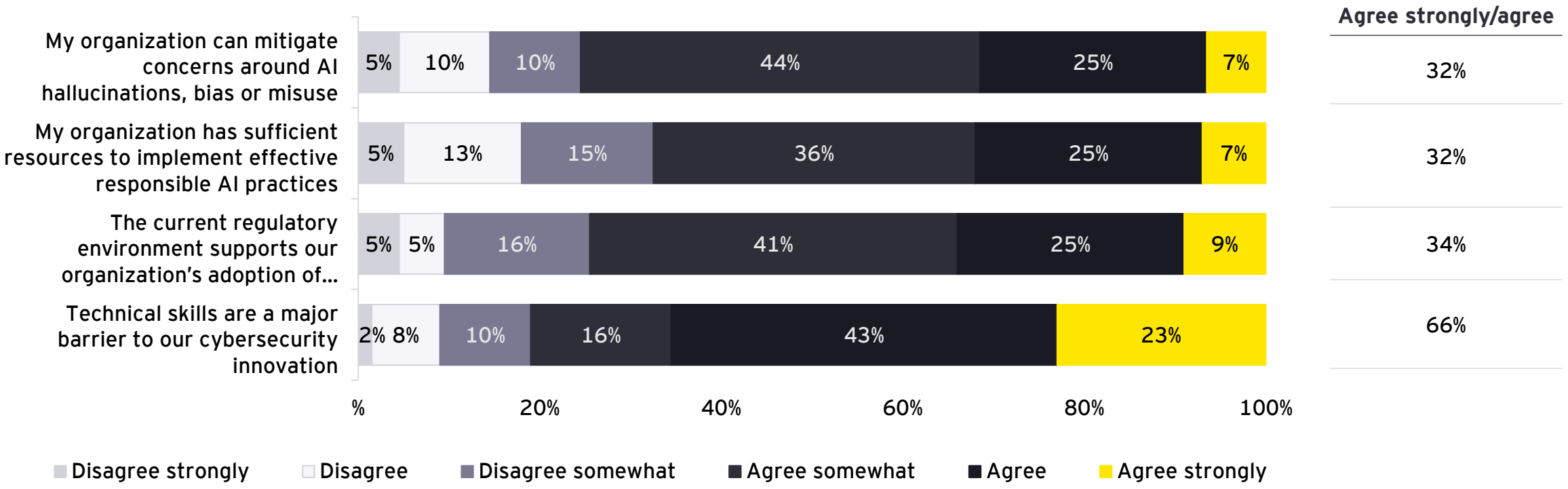
	Highly/moderately mature
AI used for cybersecurity	39%
Cybersecurity applied to AI	39%

Q *How would you describe your organization's overall maturity when it comes to secure AI adoption?*

Note: Totals may not appear to sum due to rounding.

Agreement with statements on AI readiness and risk management

Two-thirds agree that technical skills are a major barrier to cybersecurity innovation.



Agree strongly/agree
32%
32%
34%
66%

Q *Please indicate how much you agree or disagree with the following statements:*

Note: Totals may not appear to sum due to rounding.

06

Key takeaways

Key takeaways

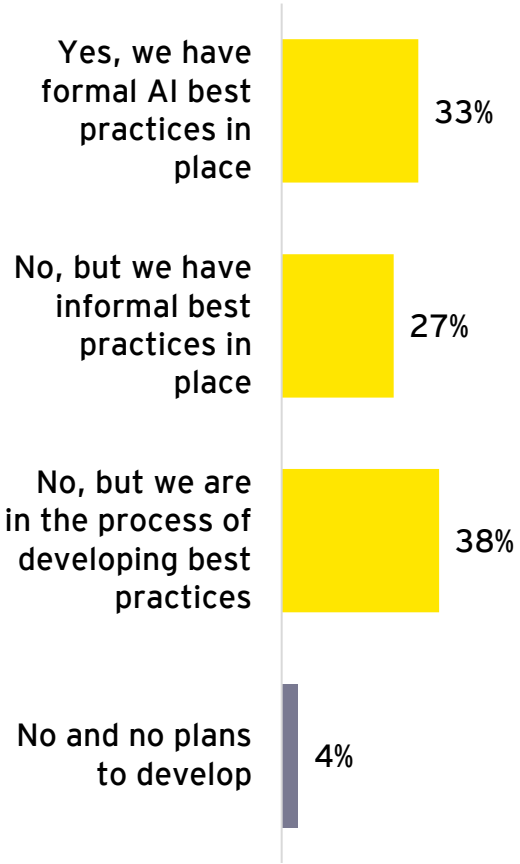
Key takeaway

Responsible AI implementation is nearly universally either in process or being planned, with most planning to expand its usage.

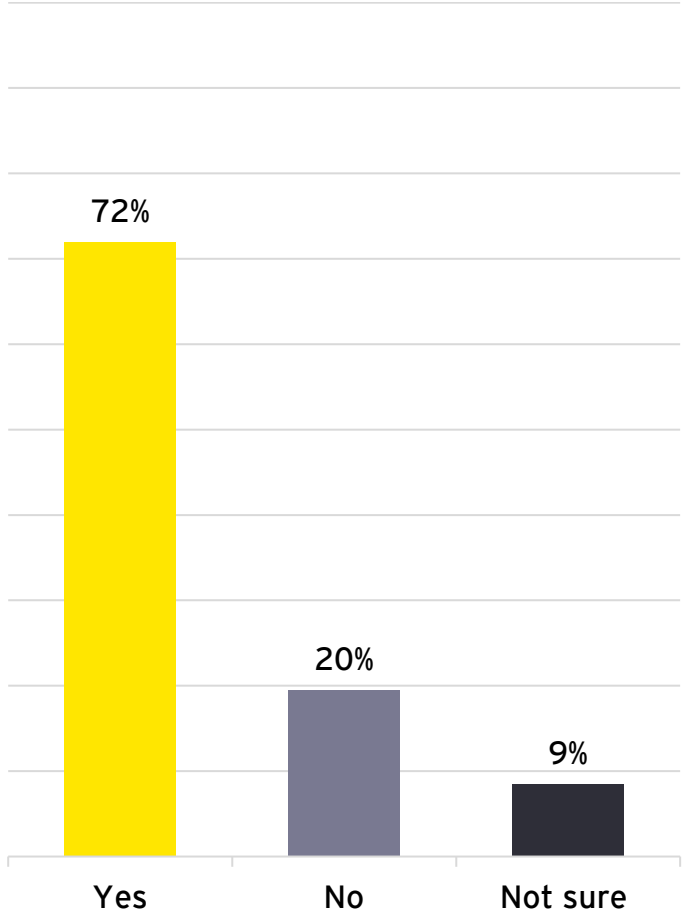
INSIGHT

- Nearly six in 10 have either formal or informal AI leading practices in place, while nearly four in 10 are in the process of developing them.
- Nearly three-quarters have a formal plan to expand the use of AI for cybersecurity over the next one to three years.

Responsible AI implementation



Future expansion



Note: Totals may not appear to sum due to rounding.

Key takeaways

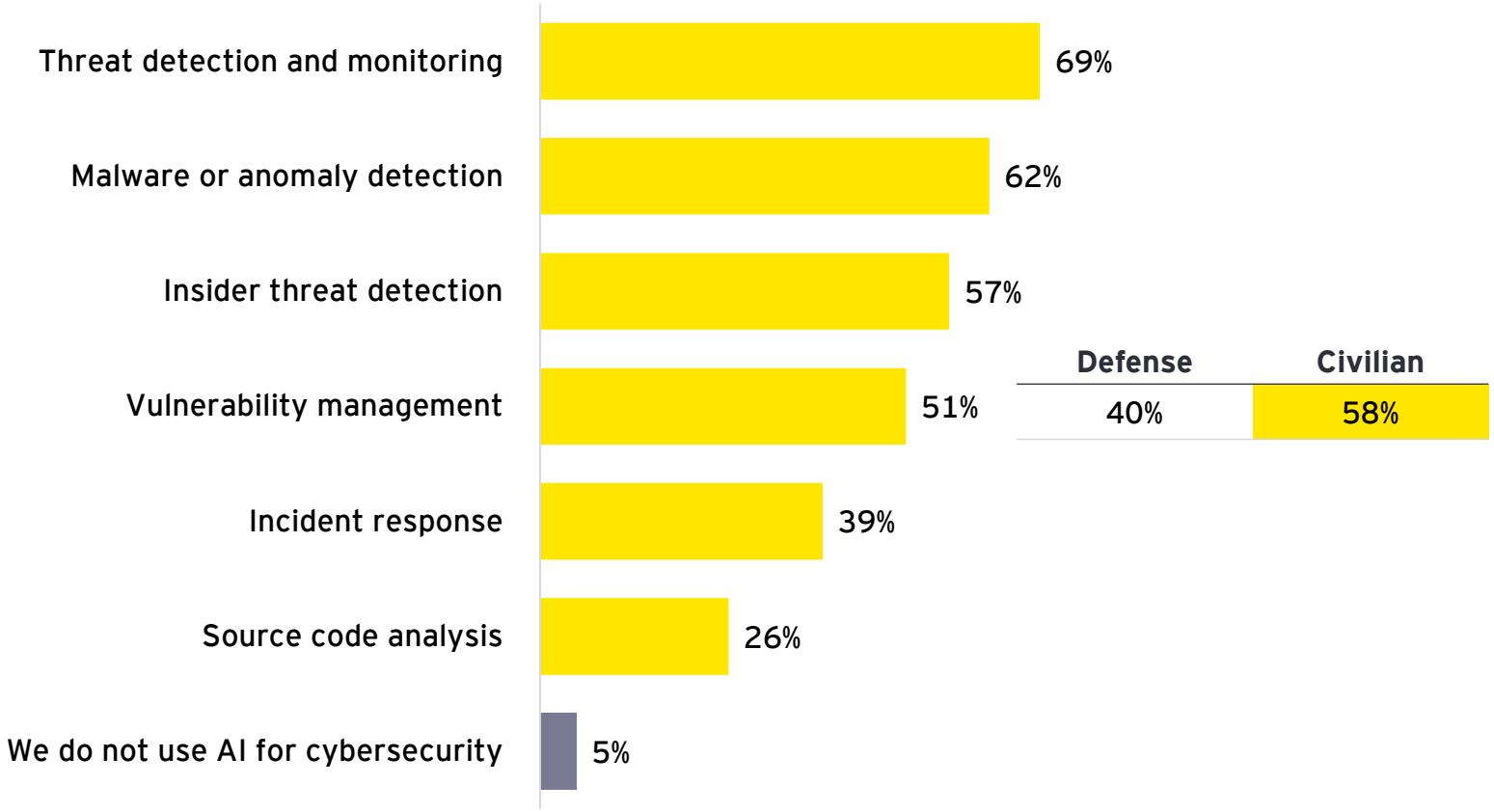
Key takeaway

AI is being used for cybersecurity in a variety of different ways, mostly for monitoring.

INSIGHT

- Most use AI for threat detection and monitoring, followed by malware or anomaly detection and insider threat detection.
- Civilian respondents were more likely to cite using AI for vulnerability management than those in defense.

Cybersecurity mission AI use cases



Note: Totals may not appear to sum due to rounding.

Key takeaways

Key takeaway

Budget, internal expertise and resourcing are seen as the biggest barriers to adopting responsible AI for cybersecurity.

INSIGHT

- More than six in 10 cite budget/cost concerns as a barrier.
- Half cite a lack of internal technical expertise, while more than four in 10 cite a lack of internal resources.
- Further, four in 10 also cite a lack of clear direction/strategy.

Barriers to adopting responsible AI for cybersecurity

Note: Totals may not appear to sum due to rounding.

Key takeaways

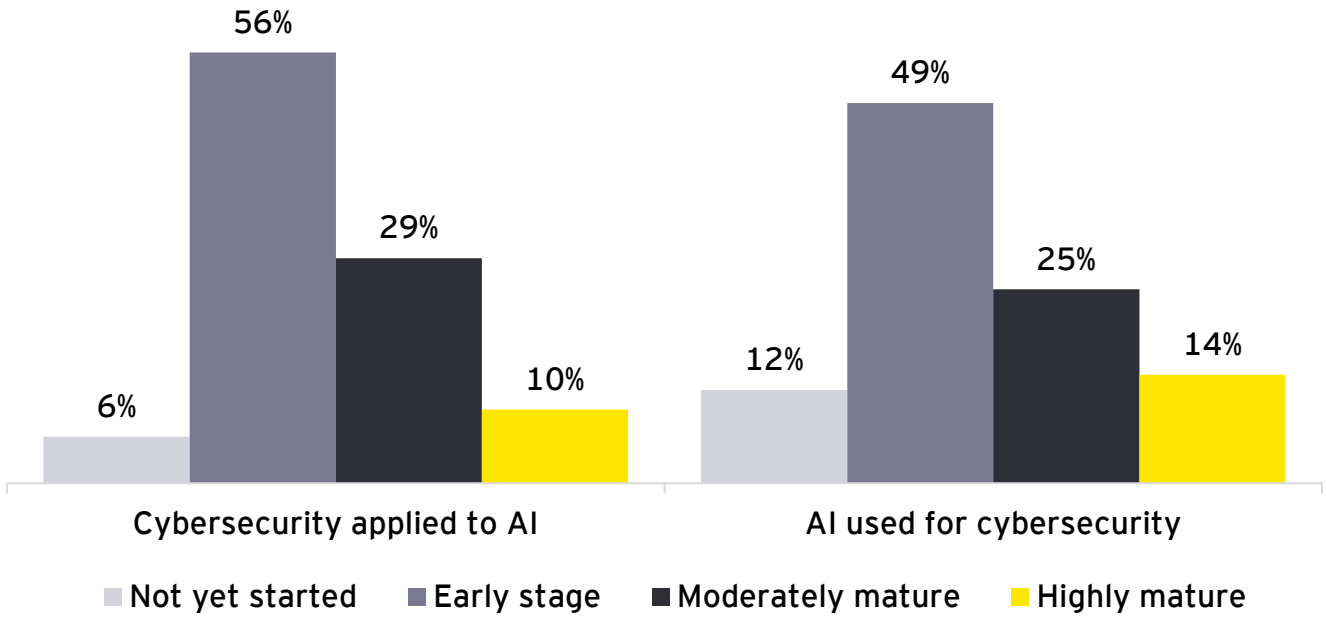
Key takeaway

Both cybersecurity applied to AI and AI used for cybersecurity are largely seen as being in the early stage of maturity.

INSIGHT

- At least six in 10 say the adoption maturity of cybersecurity applied to AI and AI used for cybersecurity has either not yet started or is in the early stage.

Secure AI adoption maturity



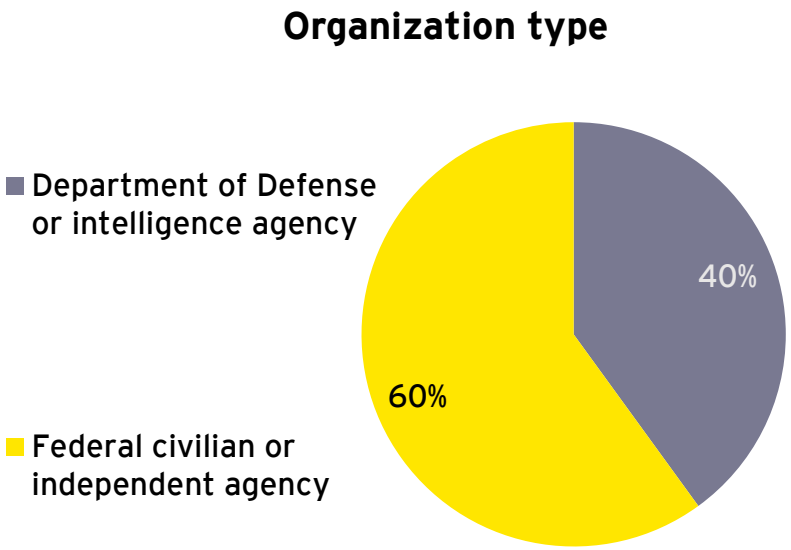
Note: Totals may not appear to sum due to rounding.

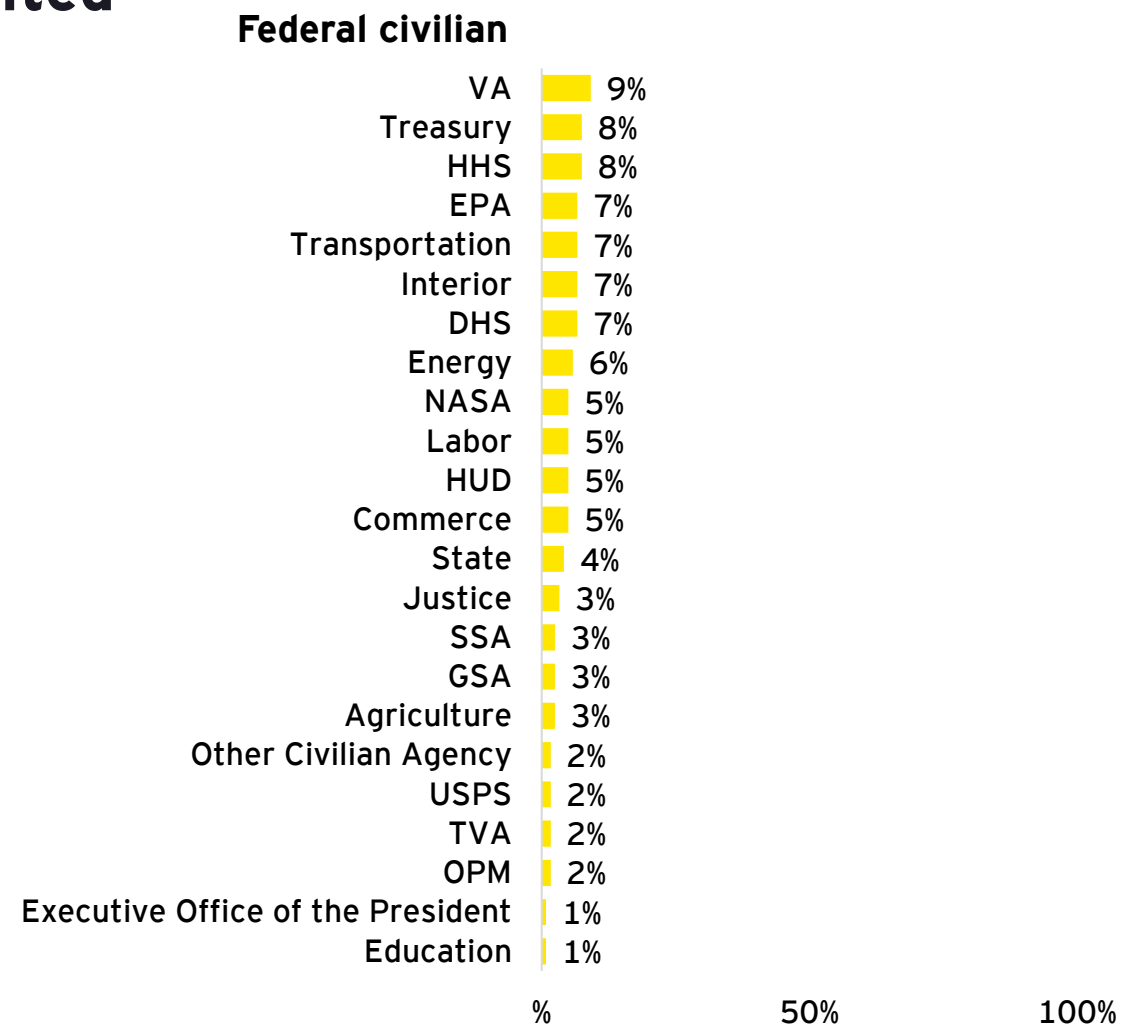
07

Appendix

Organization type and agencies represented

Takeaway

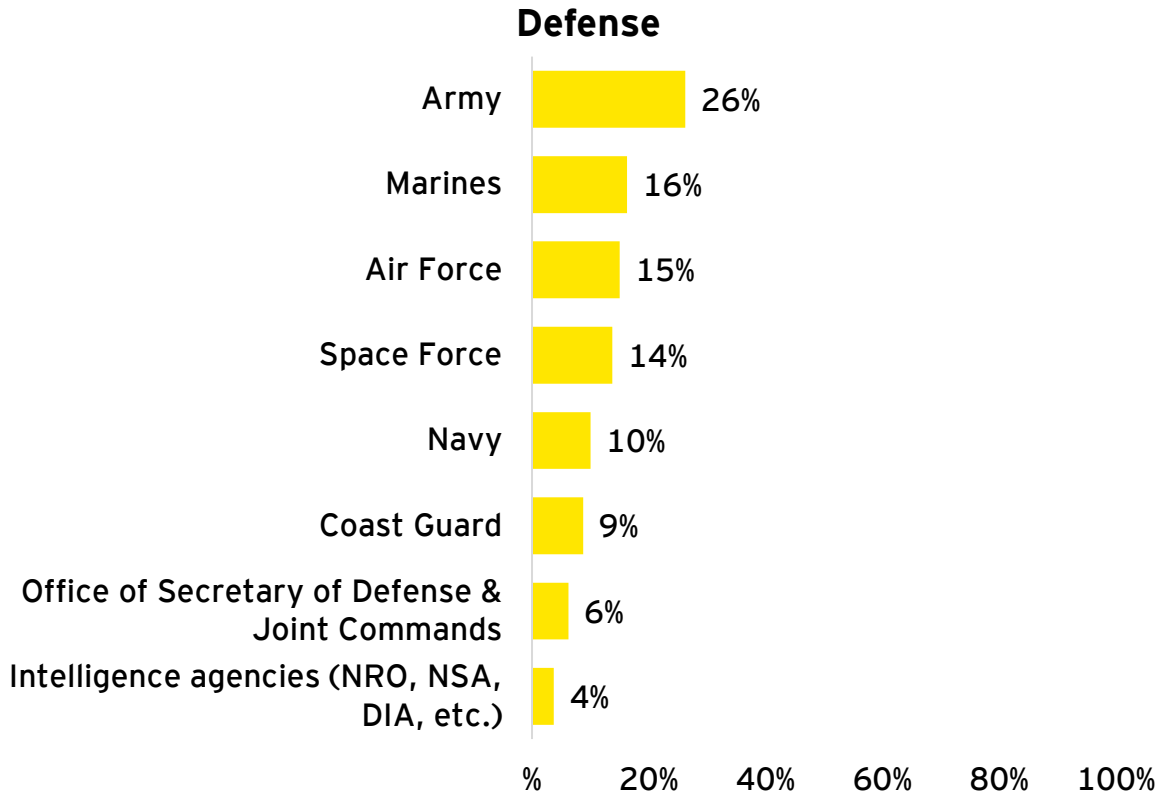


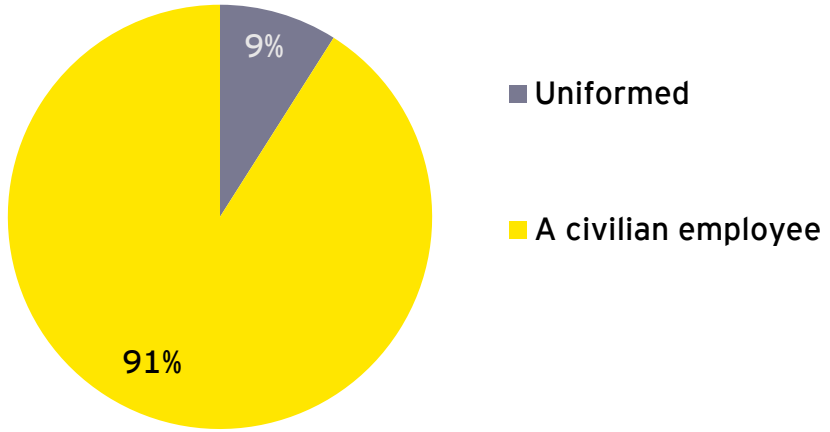


Q *What type of organization do you work for?*
[IF FEDCIV] In which government department or agency do you work?

Note: Totals may not appear to sum due to rounding.

Defense agency and employee type



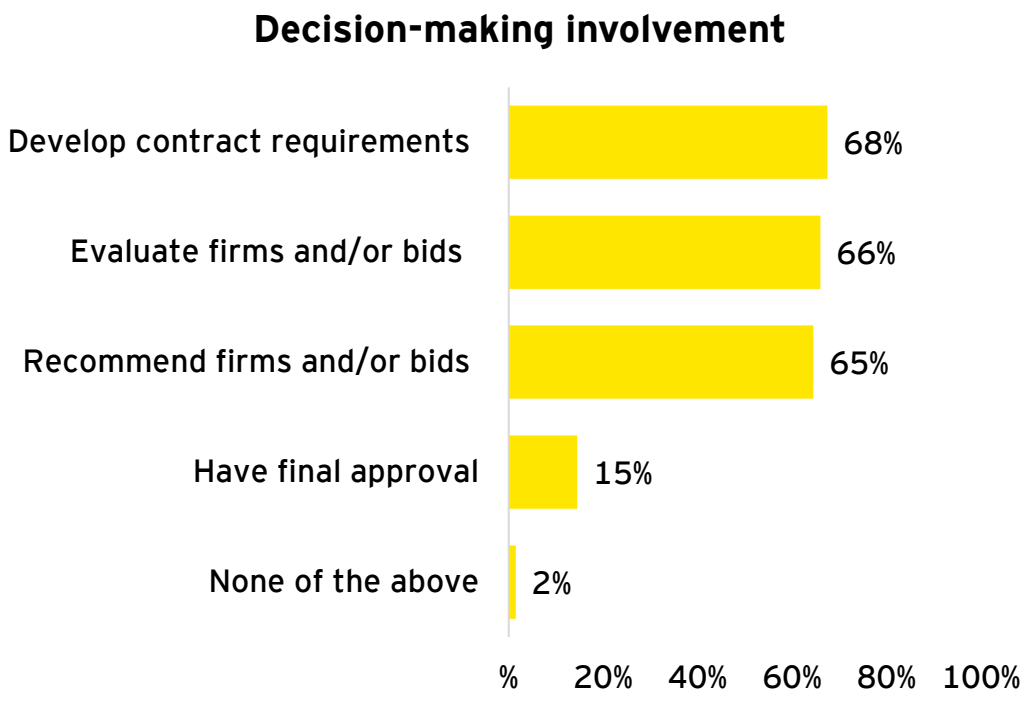


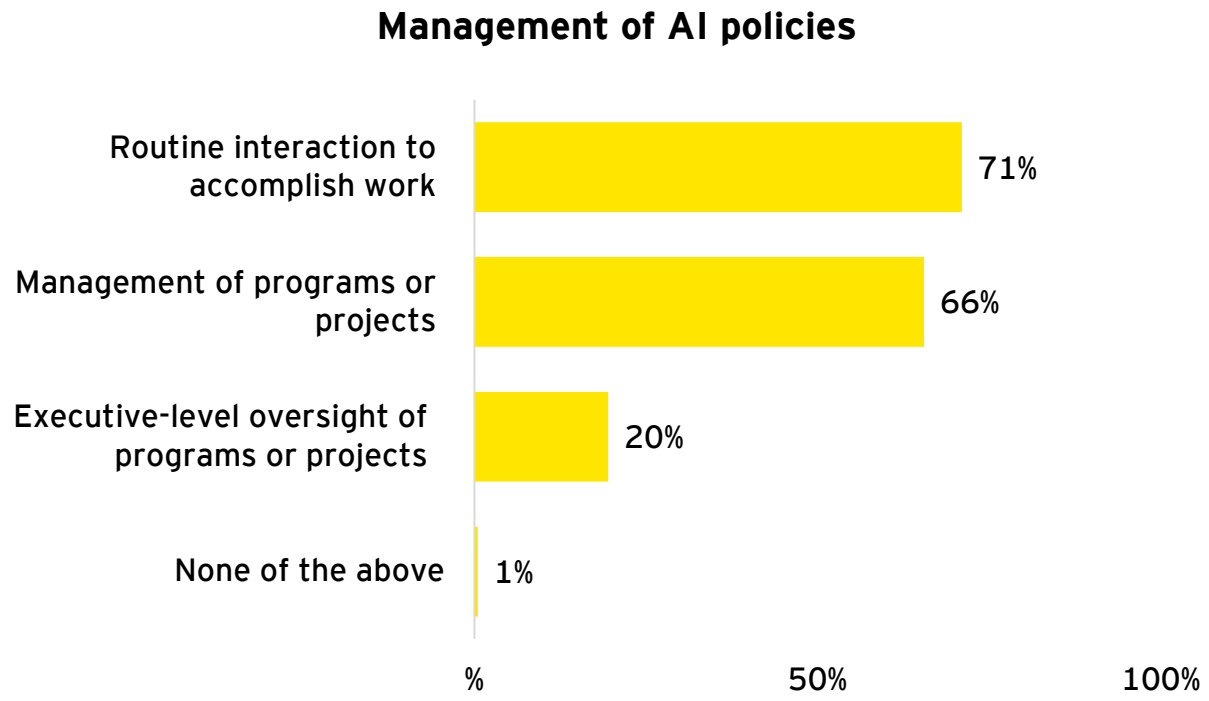
Q *[IF DEFENSE] In which government department or agency do you work?*
[IF DEFENSE] Are you:

Note: Totals may not appear to sum due to rounding.

Decision-making involvement

Respondents were screened for their involvement in the decision-making or management of AI.



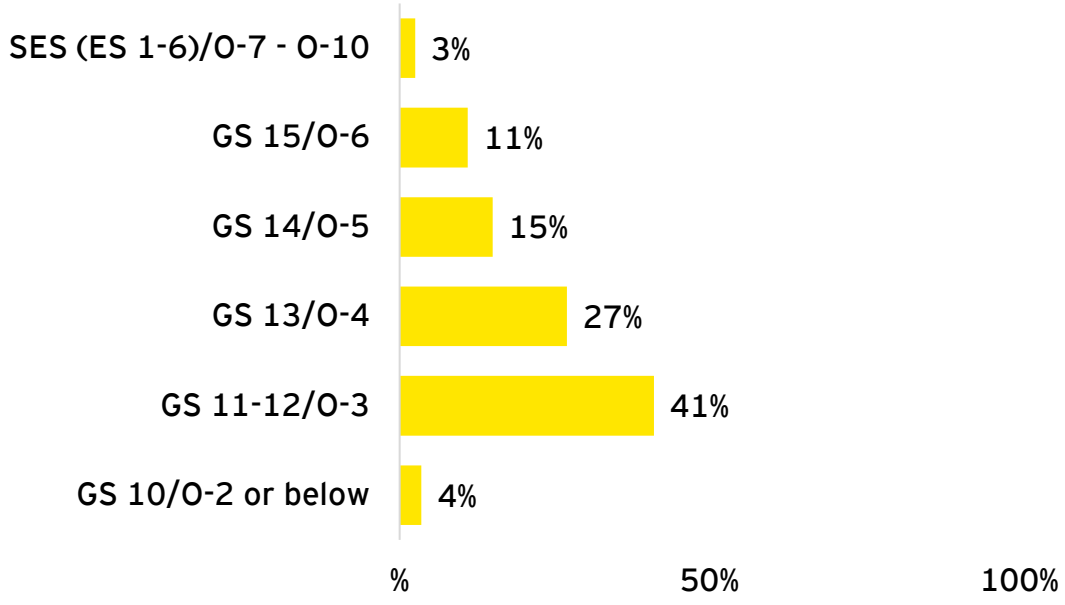


Q *In which of the following ways are you involved in your organization's selection of firms that provide technology products and services to the federal government? Select all that apply.*
In which of the following ways are you involved in your organization's management of these firms once they have been hired or selected? Select all that apply.

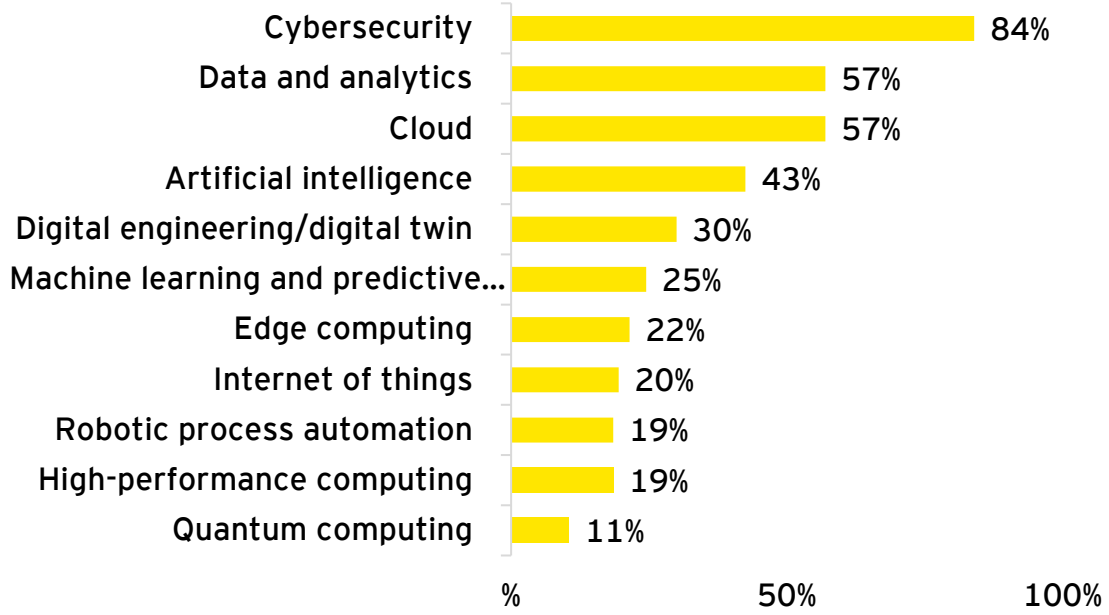
Note: Totals may not appear to sum due to rounding.

Pay grade and technology involvement

Pay grade/level



Areas of technology involvement

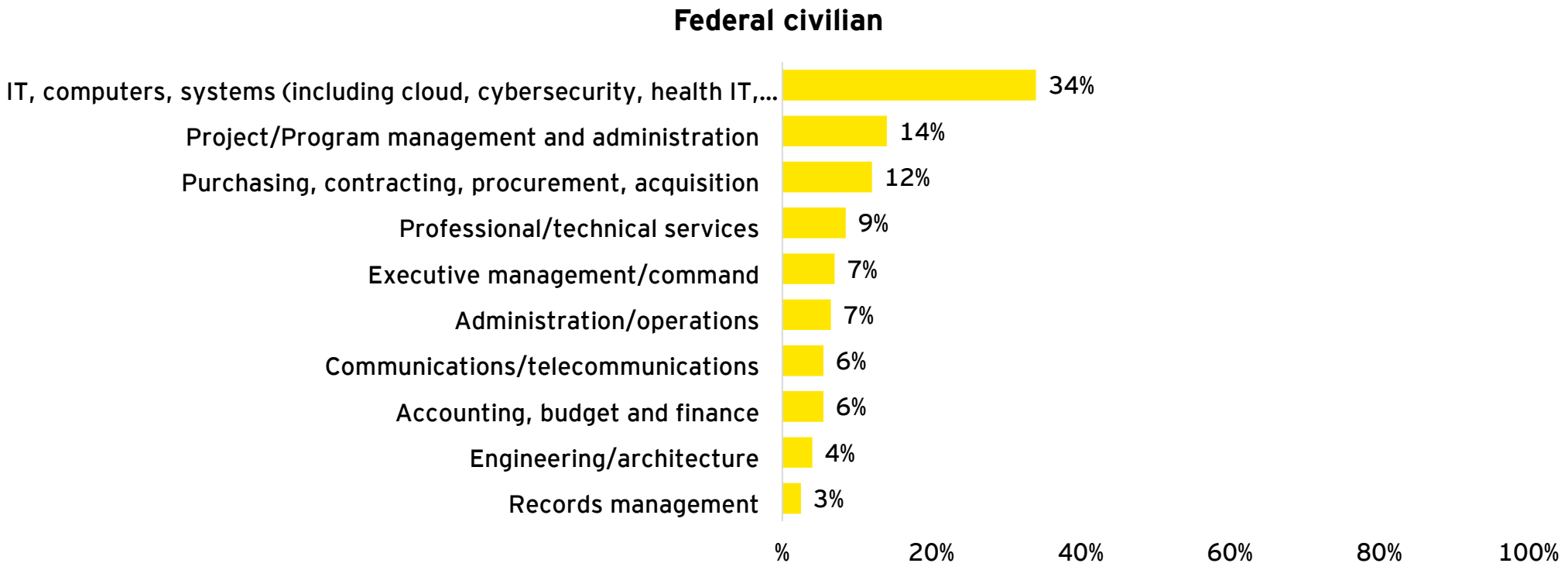


Q *Please indicate your equivalent federal civilian or military pay grade/level.*
Which, if any, of the following areas are you involved in within your organization? Select all that apply.

Note: Totals may not appear to sum due to rounding.

Job role

Takeaway



Q *Which of the following best describes your job role/function in your organization?*

Note: Totals may not appear to sum due to rounding.

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

US SCORE no. 29491-261US

2512-10304-CS
ED None

ey.com