The dual imperative: AI and cybersecurity

January 2026

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

EY
Shape the future
with confidence

INTRODUCTION

Artificial intelligence (AI) is rapidly becoming the defining force in federal cybersecurity. In agencies across government, leaders are racing to harness its potential — more than 70% plan to expand AI use in the next one to three years. Yet as algorithms grow more powerful, so do the adversaries who exploit them. Threat actors are now using generative AI (GenAI) to craft convincing phishing campaigns and deepfakes, weaponizing automation to accelerate ransomware-as-a-service, and manipulating machine learning models through data poisoning and adversarial attacks. At the same time, federal systems face mounting risks from compromised machine identities and third-party AI components woven through the software supply chain.

The convergence of AI and cybersecurity is no longer theoretical; it is the new battleground for protecting national data, critical infrastructure, and public trust. But while the potential of AI is vast, the readiness gap is widening. Nearly two-thirds of agencies already use AI or machine learning (ML) tools in some cybersecurity capacity, yet many remain in pilot phases. Only one in four federal leaders is confident in their organization's ability to manage AI-related cyber risks, and half cite a lack of internal technical expertise as a top barrier to progress.

This white paper explores how agencies can navigate this new frontier — using AI to defend their missions while securing the intelligent systems that now underpin them.

METHODOLOGY

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

CYBER FOR AI: SECURING INTELLIGENT SYSTEMS

As agencies deploy AI to strengthen their defenses, those same systems are becoming new targets for attack. Protecting them demands a new level of sophistication and vigilance.

AI systems differ fundamentally from traditional software. Their decision-making processes depend on complex, dynamic data inputs, making them susceptible to new forms of compromise. Adversarial actors can subtly manipulate model inputs to produce false outputs, poison data sets to erode accuracy, or probe models to extract proprietary algorithms and decision logic. At scale, these attacks can undermine entire cybersecurity frameworks, creating blind spots precisely where agencies rely most on automation.

As the risks become clearer, federal leaders are beginning to take a more proactive stance.

STRESS TESTING

Nearly four in 10 (39%) of respondent agencies already conduct stress tests on their AI models and another 48% are considering or planning to implement.

RISK MITIGATION

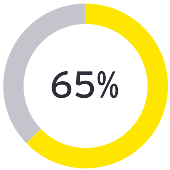
Over two-thirds (69%) report having at least partial risk mitigation controls in place; another quarter are developing them.

DATA PRIVACY

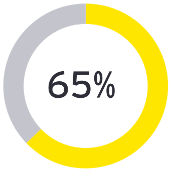
Nine in 10 say that protecting data privacy and confidentiality is critical to their AI adoption strategy, reflecting the recognition that the integrity of AI systems depends on the integrity of their data.

Yet progress remains uneven. Fewer than half of agencies have embedded Responsible AI principles directly into cybersecurity operations, and six in 10 say they are still in early stages of maturity for both AI used for cybersecurity and cybersecurity applied to AI. This challenge is not just technical – it's human. Protecting intelligent systems requires expertise that spans AI engineering, model governance, and cyber defense. Without trained professionals capable of testing, validating and monitoring AI, agencies risk embedding vulnerabilities into the very tools designed to keep them secure.

AI for cyber: Defense multiplier



use AI/ML to support cybersecurity operations



of deployments remain in limited or proof-of concept stages

Top uses cases:

1 Threat detection/monitoring

2 Malware/anomaly detection

3 Insider threat identification

4 Vulnerability management

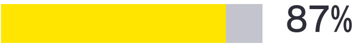
AI FOR CYBER: ENHANCING CYBER DEFENSE WITH INTELLIGENCE

If cybersecurity processes to protect AI systems is one side of the coin, using AI to enhance cyber defense is the other. Sixty-five percent of respondents already use AI or ML tools to support cybersecurity operations. The top use cases include threat detection and monitoring, malware and anomaly detection, insider threat identification, and vulnerability management.

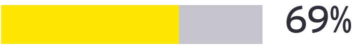
AI is rapidly reshaping this landscape by augmenting speed, scale and precision. Automated systems can detect anomalies across vast data sets, correlate attack indicators in real time, and prioritize the most urgent threats. Predictive analytics can identify vulnerabilities before adversaries exploit them. AI-driven automation reduces analyst fatigue and accelerates incident response, helping agencies do more with fewer people. There is immense promise for AI as a force multiplier in the cybersecurity threat environment.

But here too, the expertise gap is limiting progress. Although AI tools are widely piloted, 65% of deployments remain in limited or proof-of-concept stages. Agencies frequently lack personnel who can interpret AI results, fine-tune models, or connect algorithmic outputs to mission goals — a significant concern when 83% of respondents report that their agency requires human oversight of AI-driven cyber decisions. Two-thirds of federal leaders agree that skill shortages are a major barrier to cybersecurity innovation. And even as AI promises to lower costs, 62% of respondents cite budget or cost concerns as their top barrier.

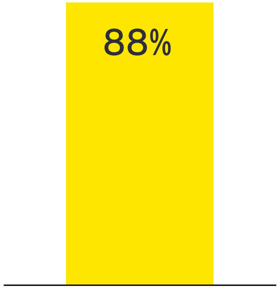
Cyber for AI: Securing intelligent systems



already or plan to conduct stress tests on their AI models

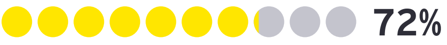


have at least partial risk mitigation strategies in place

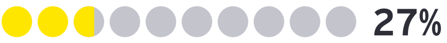


say protecting data privacy and confidentiality is critical to their AI (92% of civilian agencies)

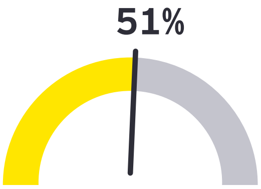
AI risk: The widening readiness gap



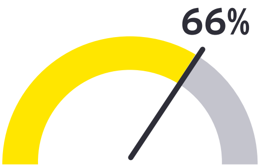
plan to expand AI use in the next 1-3 years



are confident in their organization's ability to manage AI-related cyber risks



say that a lack of internal technical expertise is a top barrier



say that skill shortages are a major barrier to innovation

AI's potential to drive security, reduce cost, and improve efficiency is not self-executing. Without experts who understand both its capabilities and its limitations, AI can introduce as much risk as it mitigates. Automation without oversight risks creating "black box" systems – fast, but not transparent; efficient, but not accountable. The success of AI in cybersecurity will depend on how effectively agencies combine human expertise with intelligent automation to create systems that are both adaptive and trustworthy.

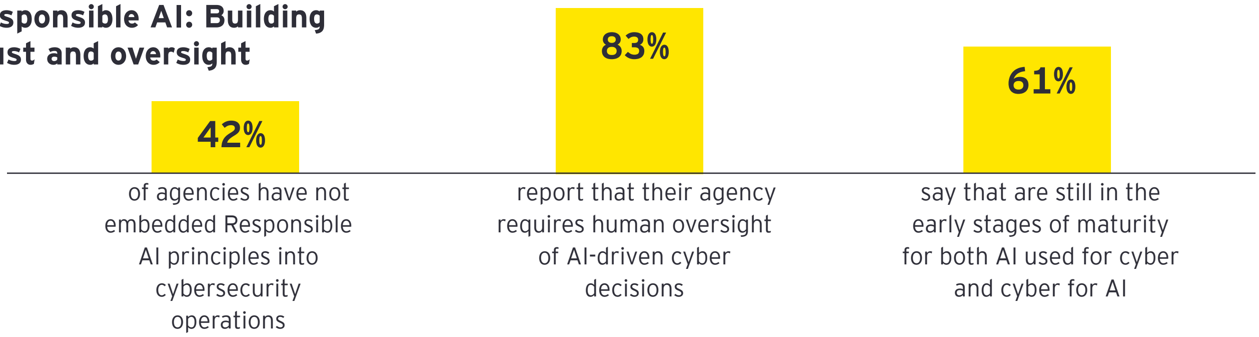
STRATEGIC RECOMMENDATIONS: BUILDING THE EXPERTISE TO SECURE THE FUTURE

AI is a powerful tool for both cyber defense and mission enablement – but harnessing that power requires sustained investment in people, processes and Responsible AI principles. The path forward to navigate the convergence of AI and cybersecurity must focus on capability-building as much as technology deployment. Agencies looking to take advantage must:

1. Balance innovation with risk by scaling governance alongside deployment.
2. Invest in human expertise to support secure and effective AI integration.
3. Institutionalize Responsible AI by embedding principles of:
    - **Transparency:** Make AI systems understandable and traceable
    - **Accountability:** Define clear ownership and oversight
    - **Human agency and oversight:** Maintain meaningful human control
    - **Privacy and security:** Protect data and model integrity
    - **Societal well-being:** Align AI use with public interest
    - **Reliability and robustness:** Maintain consistent performance under stress
4. Align AI security with mission objectives by tailoring protections to the criticality of systems supporting public services, defense and regulatory functions.
5. Foster collaboration across agencies and sectors to share threat intelligence and leading practices.
6. Prioritize training and awareness to build a workforce capable of managing AI risks and opportunities.

By investing deliberately into both expertise and technology, agencies can transform AI from a pilot-stage experiment into an operational advantage – one that both improves resilience and reduces long-term cost.

Responsible AI: Building trust and oversight



CONCLUSION

AI must be both secured and secure. Both imperatives are essential for protecting federal missions, data and public trust. Yet neither can succeed without responsible human expertise.

The survey data makes the challenge clear: the tools are advancing faster than the workforce. To close this gap, agencies must view expertise as the foundation of readiness. Technology can amplify capacity, but only skilled professionals can ensure AI is used ethically, securely and effectively.

Federal leaders who prioritize workforce capability, Responsible AI, and cross-agency collaboration will not only protect against AI-driven threats — they will define the next era of secure innovation.

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.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

US SCORE no. 29359-251US.

2512-10304-CS
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com