Booz Allen

2026 BOOZ ALLEN *VELOCITY* SURVEY – AI RISKS IN FEDERAL CYBERSECURITY

AI is Now the Central Challenge of Federal Cybersecurity

How do federal agencies defend against AI-powered attacks—and how can they securely deploy AI agents of their own?

Survey findings from over 100 federal cyber and IT leaders reveal where the gaps are, what's driving concern, and what it will take to move forward with confidence.

01 REWIRING CYBER FOR AI SPEED

How concerned are federal leaders about adversaries weaponizing AI?

79% of federal cyber and IT leaders are **Extremely or Very Concerned** about adversaries using AI to accelerate cyberattacks against their agency in the next 12–18 months.

How concerned are you with each of the following AI-enabled threats?

% very or somewhat concerned

What AI-enabled threat worries you the most?

#1 AI-accelerated vulnerability exploitation
Compressing the window between vulnerability discovery and weaponized attack to near zero.

Can AI-powered cyber defenses keep pace with AI-enabled attacks?

36% Yes
AI-powered defenses can keep pace with AI-enabled attacks

50% Unsure
Whether AI-powered defenses can keep pace with AI attacks

13% No
AI defenses cannot keep pace with AI-enabled attacks

How would you characterize your agency's readiness to employ AI-powered cyber defenses?

Fully prepared (6%)
We have AI-based cybersecurity systems actively deployed

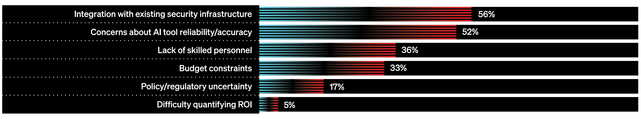
Substantially prepared (25%)
We are building or procuring AI cyber defense capabilities with a clear path to deployment

Partially prepared (48%)
We have a strategy and have begun implementation, but meaningful gaps remain

Early stage (20%)
We are assessing options but do not yet have a formal plan or committed resources

Not yet prioritized (2%)
We have not allocated resources to AI-enabled cyber defense

What are your agency's biggest barriers to implementing AI-powered cyber defense tools (select top two)?



Learn more in the *Velocity* Cover Story "Rewiring Cyber for AI Speed" at BoozAllen.com/Velocity.

02 ZERO TRUST FOR OPERATIONAL TECHNOLOGY

What is the biggest challenge to implementing zero trust in an operational technology (OT) environment (select top two)?

Learn more in the *Velocity* Mission Spotlight "Critical Infrastructure Under Attack: The Zero Trust Imperative" at BoozAllen.com/Velocity.

03 HOW CAN YOU TRUST AGENTIC AI?

Has your agency deployed agentic AI?

7% are in production

51% are actively piloting/testing

22% are planning to deploy in the next 12 months

How confident are you in your agency's ability to securely deploy agentic AI systems?

Extremely Confident (3%)

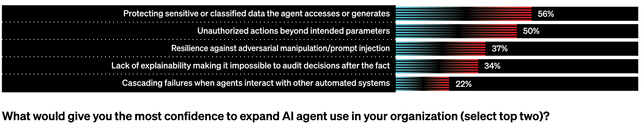
Very Confident (25%)

Moderately Confident (50%)

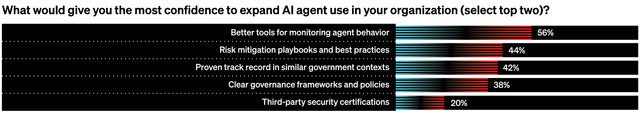
Slightly Confident (19%)

Not Confident (4%)

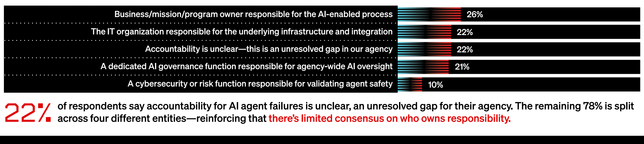
When evaluating AI agents for deployment, which risk factors are most critical to address (select top two)?



What would give you the most confidence to expand AI agent use in your organization (select top two)?



Who in your agency has primary accountability if an AI agent causes a security incident or operational failure?



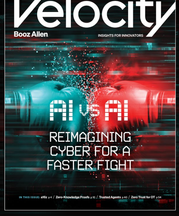
22% of respondents say accountability for AI agent failures is unclear, an unresolved gap for their agency. The remaining 78% is split across four different entities—reinforcing that there's limited consensus on who owns responsibility.

Learn more in the *Velocity* Technology Spotlight "How Can You Trust Agentic AI? Start with Engineering" at BoozAllen.com/Velocity.

Taking Action

Federal agencies face a double-sided AI challenge: defending against adversaries who are already weaponizing AI while simultaneously deploying their own AI agents securely and accountably. The data shows significant focus and active pilot investment—but meaningful gaps in readiness, governance, and confidence remain. Closing those gaps requires a coordinated approach spanning technology, policy, and talent.

METHODOLOGY
Market Connections and Booz Allen partnered to design an online survey of over 100 federal government decision makers/influencers, involved with IT and cybersecurity, regarding AI's impact on government cybersecurity practices. The survey consisted of 14 questions and was fielded in April of 2026. Due to rounding, responses may not add up to exactly 100%.



Read more at BoozAllen.com/Velocity