New Booz Allen Survey Finds Federal Agencies Are Accelerating Agentic AI Adoption Despite Significant Trust and Security Gaps

Jul 21, 2026

2026 publication highlights growing concerns around security, accountability, and governance as AI agents move into mission environments

MCLEAN, Va.--(BUSINESS WIRE)--Jul. 21, 2026-- As federal agencies rapidly adopt agentic AI systems capable of acting autonomously, a new Booz Allen survey released today reveals a growing gap between deployment and trust.

The findings are featured in the latest issue of *Velocity*, Booz Allen's regular publication exploring emerging technology and mission innovation. This edition focuses specifically on **how AI is transforming the mission and cyber technology stack** and outlines the systems-level approach organizations need to deploy agentic AI securely. This includes identity governance, continuous monitoring, red teaming, formal validation, and zero trust principles across the AI lifecycle.

Notably, of the more than 100 federal IT and cybersecurity decision makers surveyed, 58% report their agencies have already deployed or are piloting AI agents, yet only 28% express high confidence in their ability to deploy those systems securely.

The findings underscore a critical challenge facing cybersecurity leaders: how to harness the operational advantages of agentic AI while ensuring these systems remain secure and accountable.

The survey found that concern about AI-enabled cyber threats remains high, with 79% of respondents reporting they are “very” or “extremely concerned” about adversaries using AI to accelerate cyberattacks against their agencies over the next 12 to 18 months.

Additional findings:

- The **greatest AI-enabled cyber threat is AI-accelerated vulnerability exploitation**, where AI dramatically shortens the time between discovering and exploiting software vulnerabilities, according to federal leaders surveyed.
- Only **36% of federal cyber and IT leaders are confident** that cyber defenses can keep pace with AI-enabled attackers.
- Just **31% are fully or substantially prepared to employ AI-powered cyber defenses** that integrate with existing security infrastructure.
- The top concerns surrounding agentic AI deployments include **protecting sensitive or classified data** (56%), **preventing unauthorized actions** (50%), and ensuring **resilience against adversarial manipulation and prompt injection attacks** (37%).
- Accountability remains unresolved: 22% of respondents say their organizations have **not clearly determined who bears responsibility when an AI agent causes a security incident** or operational failure.
- Federal leaders say greater visibility into agent behavior (56%), proven risk mitigation frameworks (44%), and demonstrated success in their organization’s environments (42%) would **increase their confidence in expanding agentic AI deployments.**

Read the full edition of *Velocity*.

Survey Methodology

Market Connections and Booz Allen partnered to conduct an online survey of 105 federal government decision makers and influencers involved in IT and cybersecurity strategy. The survey, fielded in April 2026, examined perspectives on AI's impact on government cybersecurity practices and agentic AI adoption.

About Booz Allen Hamilton

Booz Allen is an advanced technology company. We build commercial-grade products and solutions for America’s most critical defense, civil, and national security priorities. For more information, visit www.boozallen.com. (NYSE: BAH)

BAHPR-CO

View source version on businesswire.com: https://www.businesswire.com/news/home/20260721942935/en/

Booz Allen Media: Pappas_Nicole@bah.com
Booz Allen IR: InvestorRelations@bah.com

Source: Booz Allen Hamilton Holding Corporation