The Federal Cyber AI IQ Test

November 14, 2017

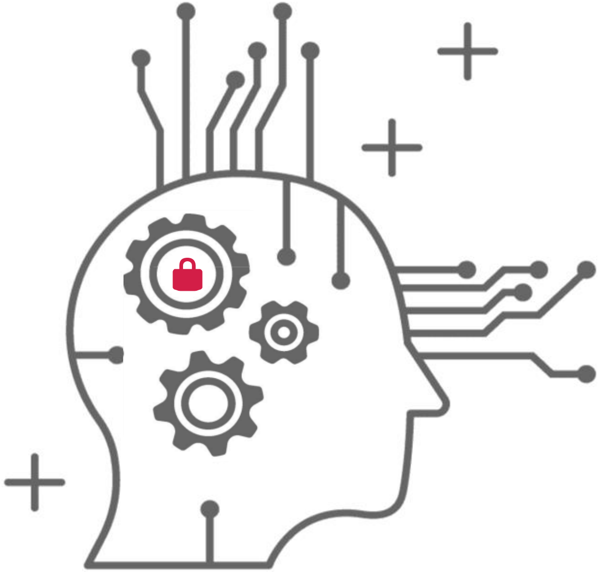
Underwritten by: IBM

Introduction

With the advent of cloud, IoT, and other next-gen technologies, the Federal government's digital footprint is growing at an exponential rate. But as the amount of data explodes, so does the number of **cyber adversaries** and vulnerabilities in our government's networks.

Without the proper resources and capabilities to manually defend against this deluge of cyber attacks, **artificial intelligence (AI)*** could be the missing link in fully securing our government. And though AI still maintains a futuristic connotation, machine learning and cognitive solutions can have an immediate impact on Federal cyber intelligence.

To better understand agencies' aptitude for cyber AI, MeriTalk surveyed 150 Federal IT managers familiar with their agency's current cyber security capabilities and future strategies. The resulting **Federal Cyber AI IQ Test** explores interest, adoption, and expected outcomes.



For the purposes of this research, we define ***AI* as next-generation computer systems that simulate the human intelligence processes to accelerate our ability to create, learn, make decisions, and think.*

Methodology & Demographics

MeriTalk, on behalf of IBM, conducted an online survey of 150 Federal IT managers familiar with their agency's current cyber security capabilities and/or future strategies, in September and October 2017. The report has a margin of error of ±7.97% at a 95% confidence level.

Respondent job titles

CIO/CTO/CISO	5%
Deputy CIO/CTO/CISO	4%
Director, Operations/IT/Intelligence	21%
Analyst, Security/Intel/Fusion/Network	15%
Engineer, Security/Network	17%
Architect, Security/Network	3%
Administrator, Security/Network/Database/Data Center/IT	13%
Scientist, Computer/Data	11%
Other IT Manager	11%

Agency type

Federal Government: Civilian agency	55%
Federal Government: DoD or Intelligence agency	43%
Federally Funded Research or Development Center	2%

Expertise

100% of qualifying Federal IT managers are familiar with their agency's current cyber security capabilities and/or future strategies

Executive Summary

- The Cyber AI Challenge:
  - Federal IT managers see cyber security as **the single biggest opportunity** for AI in the Federal government, but just **21%** say they are "very comfortable" with the idea of using AI for cyber security today
  - Feds are roughly split regarding the ideal adoption pace for AI – **46%** want to be first, **48%** are afraid to take the risk*

- Most Powerful Applications:
  - **90%** of Feds say AI could help prepare agencies for real-world cyber attack scenarios and **87%** say it would improve the efficiency of the Federal cyber security workforce
  - **91%** say their agency could utilize AI to monitor human activity and deter insider threats, including detecting suspicious elements and large amounts of data being downloaded, and analyzing risky user behavior

- AI Outlook:
  - Five years from now, Feds estimate that AI could help detect an average of **44%** of cyber security breaches or hacking attempts
  - To get there, agencies ask for formal Federal guidance or policy on AI adoption and usage, as well as updated infrastructure to support the technology

*The remaining 6% are unsure

The Cyber AI Challenge

- Federal IT managers see cyber security as the single biggest opportunity for AI in the Federal government

What is the biggest opportunity for Federal AI?*

#1 Response: Cyber security

– **86%** say their agency needs AI to keep pace with increasingly sophisticated cyber attackers, *and*

– **79%** say IoT adoption is increasing the need for cyber security efforts with AI

The catch?

Today, just **21%** say they are "very comfortable" with the idea of using AI for Federal cyber security purposes

Take away: Agencies Are Informed, But Anxious

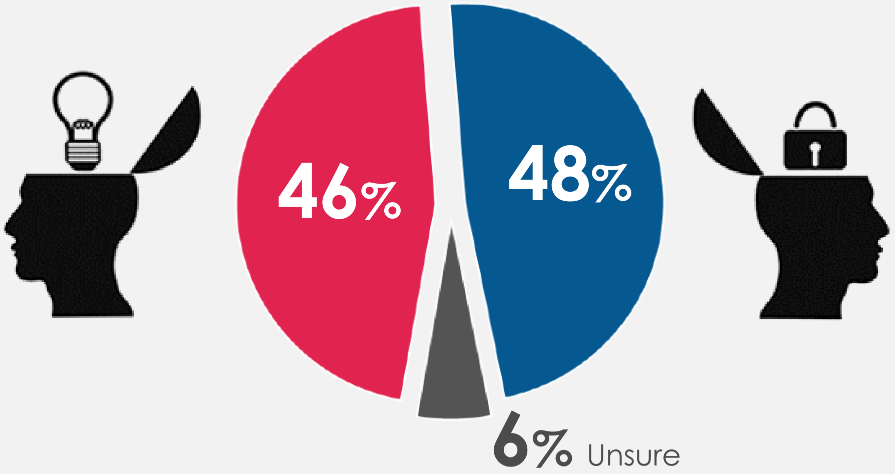
*59% see cyber security as the biggest AI opportunity, followed by data analytics (45%), fraud detection (31%), and risk management (26%)

Right Brain, Left Brain

- Feds are roughly split regarding their agency's pace of adoption of AI for cyber security – some want to be the first, others are afraid to take the risk

Which best represents how you feel about the adoption of AI for cyber security?

I want my agency to be one of the **first** agencies to adopt AI



I want my agency to **wait** for others to adopt and test AI before we incorporate it

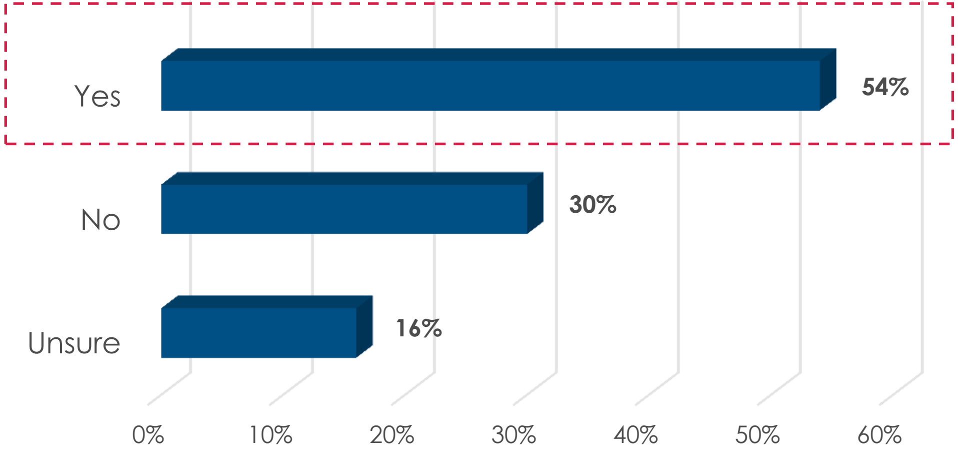
Take away: Two Distinct Testing Personas

Baseline Comprehension

MeriTalk
Improving the Outcomes of Government IT

- The majority of agencies are starting to discuss AI, and some even have a strategy

Has your department begun discussing the use of AI for cyber security?



Of this group, **41%** have a formal strategy for integrating AI into their cyber security efforts and another **53%** are working to create one

DoD/Intel agencies are significantly more likely than civilian agencies to say their department has begun discussing the use of AI for cyber security, **60%** to **48%**

Take away: Starting to Share Knowledge

Practical Applications

- Feds see their agencies using AI for detecting breaches/hacking attempts and predicting threats

In what ways could your agency utilize AI for cyber security?*

70%	Detecting breaches/hacking attempts
64%	Predicting threats
51%	Uncovering new patterns
46%	Training/planning for cyber attacks
43%	Automating threat response
38%	Predicting human behavior
35%	Correlating industry data and research

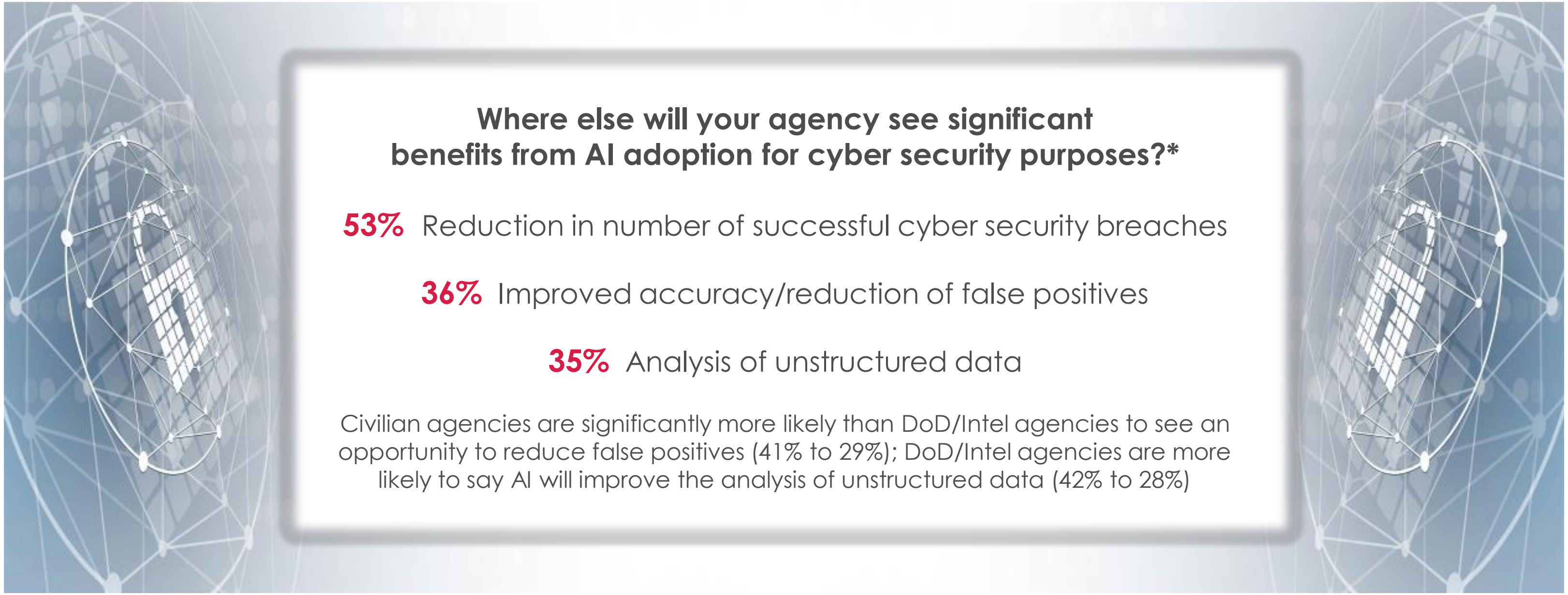
DoD/Intel agencies are significantly more likely than civilian agencies to say they could utilize AI for predicting threats, **71%** to **59%**

Take away: AI Advances Insight

*Respondents asked to select all that apply

Predicting High Marks

- 90% of Federal IT managers say AI can help prepare agencies for real-world cyber attack scenarios



Where else will your agency see significant benefits from AI adoption for cyber security purposes?*

53% Reduction in number of successful cyber security breaches

36% Improved accuracy/reduction of false positives

35% Analysis of unstructured data

Civilian agencies are significantly more likely than DoD/Intel agencies to see an opportunity to reduce false positives (41% to 29%); DoD/Intel agencies are more likely to say AI will improve the analysis of unstructured data (42% to 28%)

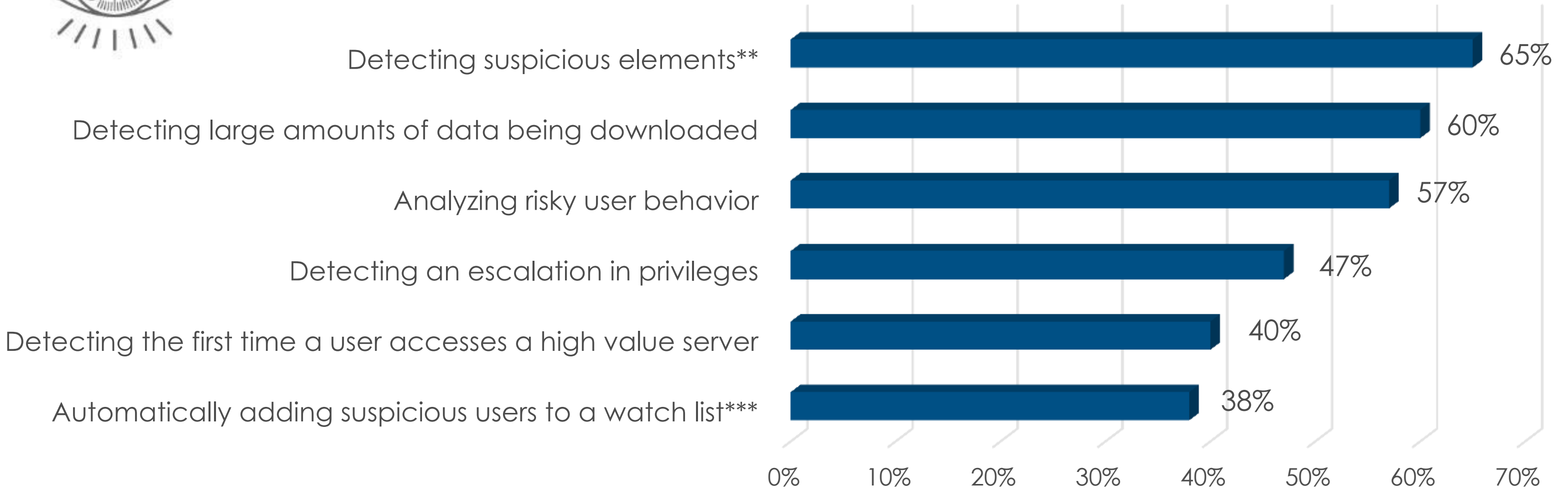
Take away: AI Improves Planning and Outcomes

*Respondents asked to select all that apply

Increasing Internal IQ

- 91% of Feds say their agency could utilize AI to monitor human activity insider threats

In what ways could your agency utilize AI to monitor human activity and deter insider threats?*



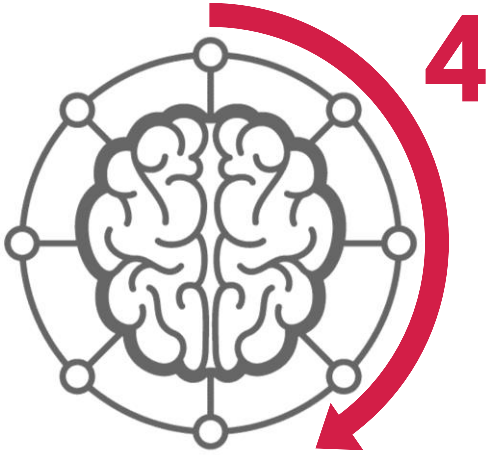
Take away: AI Senses Early Warning Signs

*Respondents asked to select all that apply **ex: foreign IP addresses, websites, etc. ***Civilian agencies are significantly more likely than DoD/Intel agencies to see this as an opportunity, 43% to 31%

Quantifying AI’s Impact

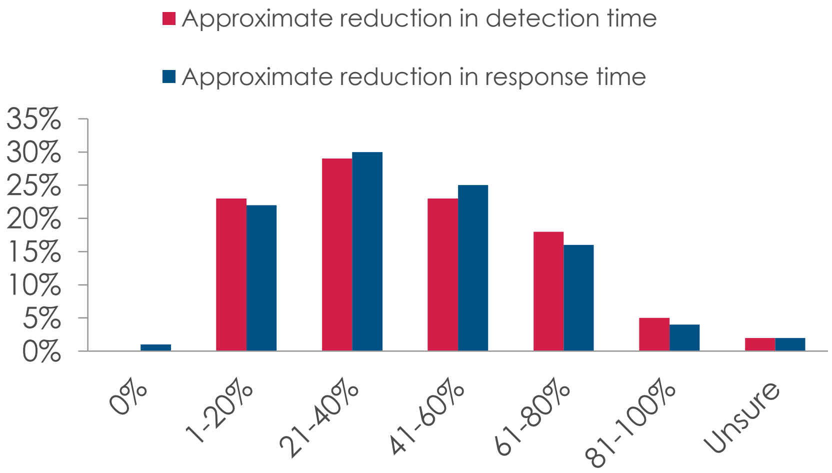
- Five years from now, Feds estimate AI could help detect nearly half of cyber security breaches

In five years, Feds say AI could help detect 44% of cyber breaches or hacking attempts



44%

Nearly all expect AI to help reduce breach detection and response times as well:



Take away: Prodigy Potential

Assessing Workforce Wit

- 87% say AI can improve the efficiency of the Federal cyber workforce, and Feds say AI is more likely to add jobs to the workforce than eliminate them – including 39% who say it will help close the cyber security skills gap

87% say AI can improve the efficiency of the Federal cyber workforce. How?*

58%	Allowing cyber workers to react to attacks more quickly
50%	Allowing cyber workers more time for advanced investigations
40%	Improving strategic planning and scenario training
39%	Helping close the cyber security skills gap
33%	Allowing cyber workers to focus on more creative tasks

Still, just **24%** of Feds fear cyber security jobs will be lost to AI

In fact, **40%** say it would require *additional* skilled hires and/or additional training

Take away: Building on, Not Replacing, Brain Power

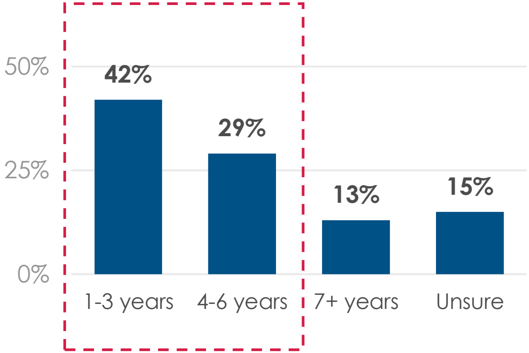
*Respondents asked to select all that apply

Aptitude for Adoption

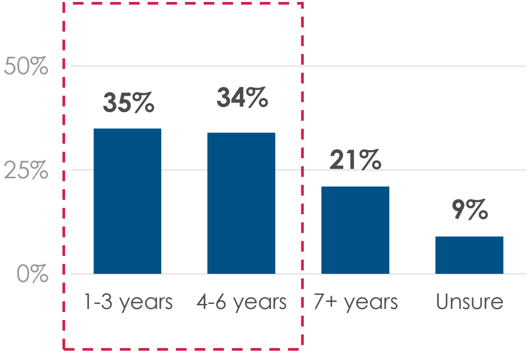
MeriTalk
Improving the Outcomes of Government IT

- Despite limited use to date, Feds – especially DoD – say AI adoption will move quickly

When will your agency **adopt** AI for cyber security purposes?*



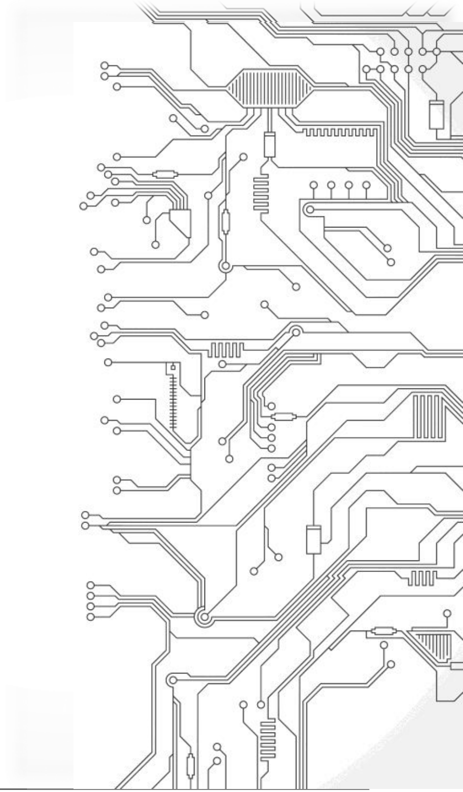
When will AI have a **noticeable impact** on Fed cyber security efforts?**



DoD/Intel agencies are significantly more likely than civilian agencies to say they will adopt AI for cyber security purposes in the next 1-3 years, **49%** to **34%**

Take away: Approaching the Tipping Point

*1% said they would not adopt AI for cyber security **1% said AI would not have a noticeable impact

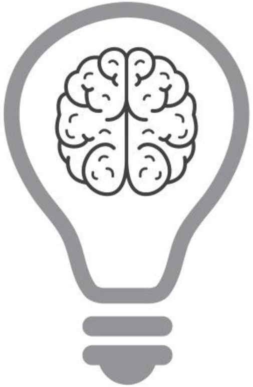


Barriers to Brilliance

- More than half of Feds (52%) say that the lack of Federal policy or other formal guidance around AI is holding them back

What is holding your agency back?*

52%	Lack of Federal policy or other formal guidance
34%	Lack of internal skills/competency to implement
29%	Lack of necessary processes/methods to implement
28%	Not ready from an infrastructure perspective
15%	Too difficult to communicate benefits to decision-makers with a lack proof points or use-cases
15%	Not convinced of the value added to current cyber security solutions and capabilities



Outside of funding, what does your agency need most to move forward?*

#1	Formal Federal guidance or policy on adoption
#2	Formal Federal guidance or policy on usage
#3	Updated infrastructure to support the technology
#4	Increase in skilled IT professionals
#5	Support from executive leadership**

Take away: Support Will Raise the Score

*Respondents asked to select all that apply **Civilian agencies are significantly more likely than DoD/Intel agencies to say they need support from executive leadership, 37% to 25%

The 10 Year Outlook

- Moving forward, agencies are looking to adopt AI for a variety of cyber security needs, including threat detection, visualization of their network traffic, and employee training

Where would you most like to see your agency adopt AI for cyber security purposes over the next 10 years?

- "**Threat detection** (reducing false positives) so analysts can figure out and focus on the real breaches"
- "**Visualization** of network traffic to highlight potential breaches or hacking events to the analysts for final determination"
- "Automated threat detection to **improve incident response times**"
- "Spam and **malicious email detection**; network intrusions"
- "As a **training** tool… to close the knowledge gap in the workforce"

Take away: Make Way for Mensa

Recommendations

Improve AI Comprehension

Feds are encouraged by the potential benefits of AI for cyber security, but few are very comfortable with the idea today. Take time to discuss the opportunity with your agency – explain the technology, how you plan to scale, and what impact it will have on the workforce. Leverage insight from DoD/Intel early adopters to help shape the conversation.

Evaluate Agency Potential

Feds should examine their core technology early and often to ensure it's ready for the rapid pace of expected AI adoption. Defining and organizing data streams, eliminating silos, and implementing scalable storage solutions will be key to enabling future AI applications and improving Feds' overall cyber health.

Request a Meeting of the Minds

Many agencies seem to be waiting for formal Federal policy on cyber AI adoption and usage before making a move. Study the 2016 White House report, *Preparing for the Future of Artificial Intelligence**, and ask senior leadership for additional cyber-specific guidance.

*"Preparing for the Future of Artificial Intelligence" Executive Office of the President National Science and Technology Council Committee on Technology, 2016

Thank You

MeriTalk
Improving the Outcomes
of Government IT

www.meritalk.com

egarber@meritalk.com

703-883-9000 ext. 146