

How Federal Agencies Can Fuel Innovation With a Secure Digital Ecosystem



Federal agencies cannot discuss innovation without also talking about cybersecurity. That has never been more apparent than it is today, as agencies accelerate their adoption of solutions that leverage cloud and artificial intelligence, each of which presents both challenges and opportunities for agency security teams. Let's dive into some key considerations and best practices for agencies to create a secure digital ecosystem.

Build a Stronger Cyber Foundation

Agencies need to address two givens in today's cyber landscape: that the risk of attacks continues to grow — so they need to adopt better defenses — and that some attacks will succeed — so they need to limit the damage that is done.

The foundational security solution for the modern environment is zero trust. Key aspects of zero trust include:

- Continually authorizing individual users and devices to access resources
- Revoking that access when it's no longer required
- Segmenting the network to limit lateral movement of malicious actors in the environment
- Requiring multifactor authentication
- Enforcing the concept of least privilege

As part of a least privilege policy, agencies also consider more nuanced tactics than simple user authentication. For example, a user's access privileges might be limited to:



The use of specific devices



A user's specific location(s)



The time of day



Specific portions of a dataset

Approach Cyber as a Shared Responsibility

Commercial cloud services provide many well-known benefits that help agencies modernize their operations. But they also require agencies to think about security in a new way: as a shared responsibility between the agency and the cloud service provider.

Here is how the Department of Defense breaks down that shared responsibility across different cloud models:

Customer Cloud Service Provider

Resources	On Prem	IaaS	PaaS	SaaS
Data				
Client Endpoints				
Account & Access Mgmt				
Application				
Operating System				
Network				
Physical Security/ Hardware				

The shift to the cloud can help agencies improve their cyber posture in three ways:

- 1. It requires agencies to expand security measures to the data level,** rather than just relying on perimeter defenses, which aligns with the push toward zero-trust security.
- 2. It enables deployment of thin devices at the edge,** with data remaining within the data center, which reduces the risk of theft or loss.
- 3. It facilitates secure collaboration** across an agency and with external partners.

Ramp Up for AI

Agencies are still at the beginning of their journey toward AI, with a focus on identifying and building out the strongest use cases. But security, compliance and other concerns must be incorporated into the process from the beginning. To assist agencies, the Government Accountability Office has developed an [AI Accountability Framework](#), which is built around four principles:

GOVERNANCE

This principle describes key practices to promote accountability by establishing processes to manage, operate, and oversee AI implementation. For example, Workforce highlights the importance of recruiting, developing, and retaining personnel with multidisciplinary skills and experience in design, development, deployment, assessment, and monitoring of AI systems.

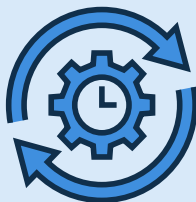


DATA

This principle describes key practices to help entities use data that are appropriate for the intended use of each AI system.

PERFORMANCE

This principle describes key practices to help entities produce results that are consistent with program objectives.



MONITORING

This principle describes key practices to help entities ensure their AI systems remain reliable and relevant over time.

With AI, the key is to maintain high security and compliance standards without hindering innovation.

Jon S Kim, Vice President of Solutions and Services for Presidio Federal, offers the following guidelines for taking a holistic approach:

- ✓ Prioritize zero trust principles.
- ✓ Integrate security in pretty much every stage of this transformation process.
- ✓ Deploy continuous monitoring systems to detect vulnerabilities.
- ✓ Adopt and communicate clearly defined principles and standards agencywide.
- ✓ Learn from the experiences of organizations in the private sector.
- ✓ Leverage the expertise of partner organizations, both in government (e.g., the National Institute of Standards and Technology) and industry partners.

But while AI presents new security challenges, security is also one of the strongest use cases for AI. At present, agencies generate more cyber-related data than they can possibly process. AI closes that gap, enabling your security team to identify and mitigate threats more quickly than ever.

*Cisco has identified **three key areas** in which AI can strengthen the cyber portfolio:*

- 1 ASSISTING SECURITY TEAMS**
Generative AI can help admins through complex tasks, saving them time and eliminating errors, such as misconfigurations
- 2 AUGMENT HUMAN INSIGHT**
AI makes it easier to correlates data across email, web, process, and network domains to detect a real attack with more accuracy.
- 3 AUTOMATE COMPLEX WORKFLOWS**
For example, in the event of ransomware attack, AI-based tools could automatically detect the threat and trigger a snapshot of the environment, providing a point of immediate recovery.

Cybersecurity is not an obstacle to innovation, but an enabler. By ensuring that cloud, AI and related solutions meet the most stringent cybersecurity requirements, agencies can unleash the creativity of their teams and transform the digital ecosystem. *To learn more about how Cisco and Presidio Federal can help to bolster your agencies cyber readiness, please visit presidiofederal.com/partners/cisco.*

