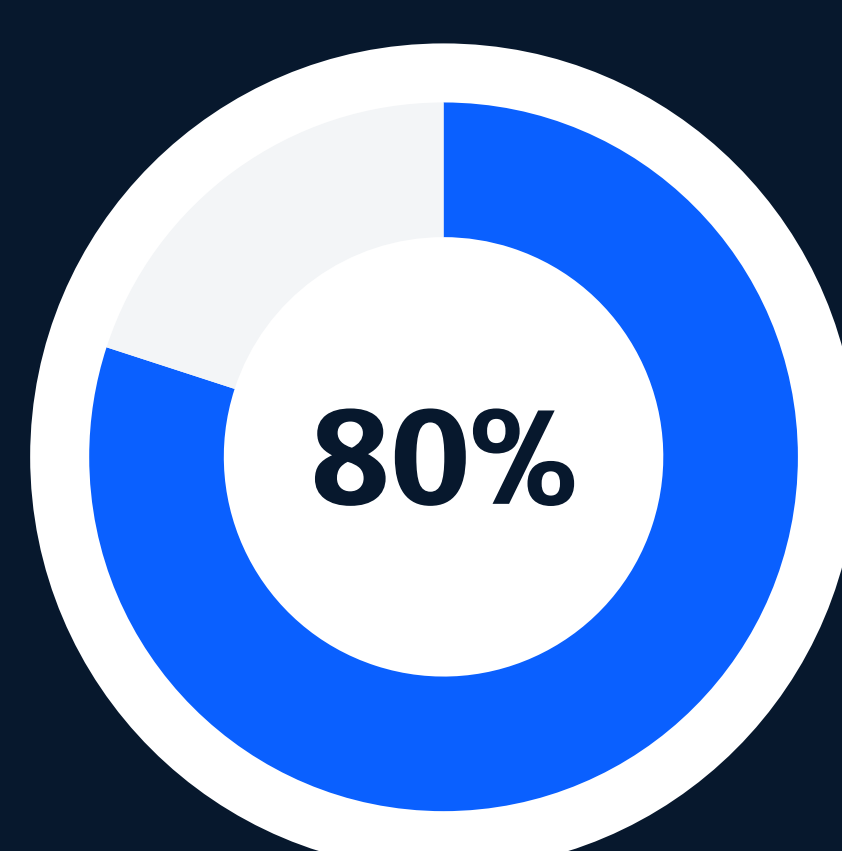# CISCO

# Mission: Modernize

Empowering Federal Networks with
AI-Driven Security and Seamless Simplicity.

Imagine accessing government services through intelligent chatbots that understand your needs instantly. Picture border security systems that can identify threats in milliseconds, or veteran health care platforms that predict medical needs before symptoms appear.

Artificial intelligence (AI) supported by modern networking solutions will help federal agencies realize these capabilities by simplifying operations, supporting infrastructure demands and embedding security at every layer. Yet, for many organizations, these transformative experiences remain out of reach, blocked by decades-old IT infrastructure.

## Federal IT Tech Debt

**80%**

80% of all federal spending on IT goes toward the operation and maintenance of outdated, legacy systems — that's $100 billion on systems that introduce risk!

## As agencies work to reduce tech debt, who is leading the charge?

According to the General Services Administration (GSA)'s IT Portfolio Dashboard, six agencies are increasing investments in development, modernization and enhancement (DME) programs:
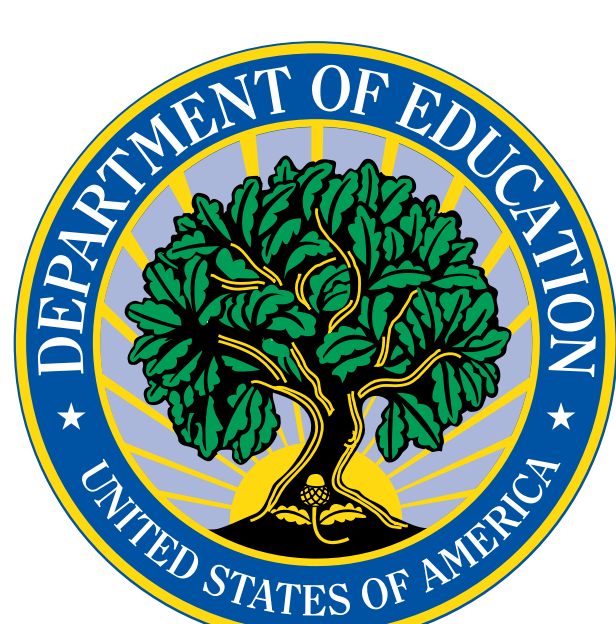
| ↑ **68%** increase | ↑ **47%** increase | ↑ **34%** increase | ↑ **25%** increase | ↑ **24%** increase | ↑ **9%** increase |

Investments in DME programs are foundational to meeting the goals outlined in President Trump's AI Action Plan. The plan's three pillars: **innovation**, **infrastructure** and **international diplomacy**, hinge upon the creation of a modern network capable of accelerating "AI adoption in government."
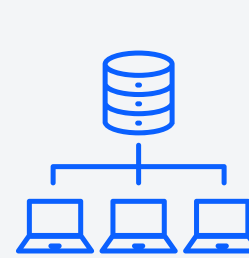
Cisco Meraki does this by providing agencies with a scalable, secure foundation as required by OMB M-25-21 by:

**Innovation**

Scaling to meet development and deployment demands
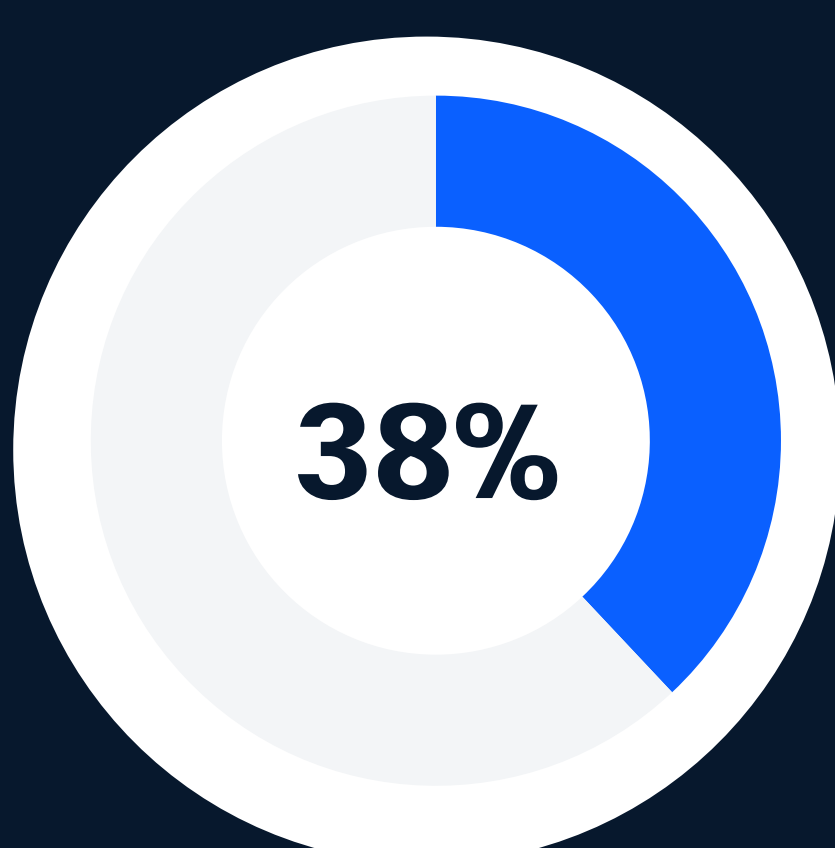
**Infrastructure**

Protecting AI workloads at the mission's edge and at home

**International Diplomacy**

Building trust through secure network architectures

Modern networks are the first step toward securing federal data. Unlike legacy systems, these platforms look to protect data wherever it lives via dynamic policy enforcement.

**38%**

Data from the US Government Accountability Office reveals that 38% of information security incidents stem from improper usage or poor governance controls.

Threat actors seek to exploit these gaps in order to exfiltrate data, but contemporary networking solutions can help agencies secure AI workloads. For example, solutions like Cisco ThousandEyes equip agencies with comprehensive visibility into their tech stack.

Understanding the evolving threat landscape and the trends reshaping how organizations must approach cybersecurity, learn how Cisco Security bolsters protection.

Moreover, Cisco's Trust Center demonstrates the company's commitment to supporting agencies as they build modern networks that meet OMB M-25-21's requirements for building public trust and advancing AI.

In short, modern networks aren't just infrastructure solutions — they're the key to driving the mission forward. As explained by Former Federal CIO Suzette Kent:

> **Today modernization success can be unlocked for every agency across government. Systematic elimination of legacy process barriers and automation of critical processes combined with leveraging commercially proven tools makes modernization less complex, less costly and lowers the risk profile."**

Suzette Kent, Former Federal CIO

With modern networking solutions, agencies can unlock a future powered by possibility. Emergency response networks could help FEMA employees pre-position resources. Intelligent workflows and chatbots could help the Department of Defense make informed decisions that protect the warfighter at the mission's edge.

## Whatever the mission is, it starts with the network.

Ready to transform your agency's capabilities?

[ See how Cisco can help. ]

# CISCO