Cisco SD-WAN (FedRAMP<sup>SM</sup> In Process)
The new landscape of government networking.

**Empower government: More users, more apps, more devices.**

The Federal Risk and Authorization Management Program (FedRAMP) has announced that Cisco’s Software-Defined WAN (SD-WAN) offering has secured a "FedRAMP In Process" designation – this is the first SD-WAN offering to do so.

Cisco SD-WAN empowers Federal agencies, as well as State and Local Government customers, to connect any user to any application and deploy cloud-based applications without compromising on security or user experience. Our SD-WAN offering (winner of CRN’s 2019 Product of the Year) enables a secure, cloud scale architecture that is open, programmable and scalable so that government agencies can have maximum choice and control. Plus, it’s all managed through the Cisco vManage console, so agencies can quickly establish an SD-WAN overlay fabric to connect data centers, branches, campuses, and colocation facilities to improve network speed, security and efficiency.

**Featuring:**
- Predictable application experience
- Best in class integrated security
- Cloud optimized
- Operational simplification
- Rich analytics
Why government agencies should use SD-WAN

Your agency lives in a multi-cloud world where it’s getting harder to manage the complex architectures behind cloud applications. It’s a world where trying to balance application delivery, while optimizing connectivity and security, is a constant battle.

That’s where SD-WAN can help. As your agency’s partner, Cisco can deliver a secure, cloud-scale SD-WAN that can address these and other challenges. With Cisco SD-WAN, you don’t “struggle” with multi-cloud: you master it.

By deploying Cisco SD-WAN, your agency empowers a cloud-delivered overlay that connects WAN infrastructures to multi-cloud environments through a single fabric. The provides your agency with a seamless digital transformation.

Real world experiences: How SD-WAN is already adding value

SD-WAN is already helping our Private Sector customers, and now Public Sector agencies can enjoy the same Enterprise level benefits:

- Reducing throughput costs by over 80%
- Improving Office 365 performance by 500%
- Completing public cloud migration in one week (original estimates were 12 months)
- 100% application uptime during hurricane blackouts
- Reducing application latency by 400%
- Improving change control for 3,000 sites by 1,200%
- Reducing Operating Expenses (OpEx) by $20 million over three years.
- Condensing M&A integration to 2 weeks.

As a “FedRAMP In Process” designated offering, Cisco SD-WAN provides the level of security your agency needs to meet Federal mandates while being able to deploy and maintain 10,000+ WAN sites using its simplified interface. It also enables automated scanning, monitoring, troubleshooting and controller deployment capabilities. And it even has planned future capabilities in AI/ML.

Plus, as a “FedRAMP In Process” offering, Cisco SD-WAN is contributing to the OSCAL framework (developed by NIST) by helping Federal Agencies with mandated reporting.

Key features for government

- **Predictable application experience**
  Cisco SD-WAN provides predictable SLA on your critical enterprise applications plus enables application aware policies with real time enforcement around network problems. It also allows multiple hybrid active-active links.

- **Best in class integrated security**
  SD-WAN gives your agency a Zero-Trust foundation with advanced authentication and encryption technologies. It offers segmentation to isolate and protect critical assets with cloud, partner networks, guest wireless and more. And it empowers your agency with Enterprise firewall, IPS, AMP NGAV, DNS-layer enforcement, URL filtering and SSL decryption proxy.

- **Cloud optimized**
  Our SD-WAN offering lets you seamlessly extend your WAN to multiple public clouds in a single fabric, all with real-time optimized performance for Office365, Salesforce and other SaaS apps. And it optimizes workflows for your existing AWS and Azure installations.

- **Operational simplification**
  Cisco SD-WAN enables a single management dashboard for configuration and management of WAN, cloud and security with template-based, Zero Touch provisioning for all locations. Plus full automation with RESTful integration into your existing tools.

- **Rich analytics**
  Enjoy granular visibility of applications and infrastructure with rapid failure correlation and mitigation, as well as sophisticated forecasting and what-if analysis for effective resource planning. Plus, our SD-WAN also recommends policy changes based on traffic patterns.
Cisco SD-WAN is the most widely deployed SD-WAN across the Fortune 2000, with large deployments in retail, healthcare, financial services and energy. This includes PCI and HIPAA compliant industry sectors.

Cisco’s “FedRAMP In Process” SD-WAN offering can be deployed in virtual, cloud or physical form factors with full cloud management by either in-house IT or as a Managed Service. Pricing is based on hardware and annual subscription licenses. It is also available for two different scenarios:

- Cisco SD-WAN (Viptela) for advanced routing and flexible deployment: https://cisco.com/go/sdwan
- Cisco SD-WAN (Meraki) for all-in-one SD-WAN and security solution for lean IT environments: https://meraki.cisco.com/sd-wan

We also offer Cisco’s SD-WAN Advise and Implement Service to accelerate your deployment success.

Why Cisco

Cisco is uniquely positioned to help enable your agency’s missions in a Cloud Native, Zero Trust world.

By deploying our FedRAMP Authorized solutions, your agency can empower stronger, risk-based security featuring deeper visibility and automation. All while enabling Enterprise level unified communications and collaboration for enhanced productivity.

Through our decades of experience partnering with government, we have developed:

- Unparalleled reliability and security for operations and applications, regardless of where they reside
- A reputation as a proven and trusted provider
- Industry-leading services that comply with Federal security requirements.