Framework Mapping: Cisco Secure Access for Government + NIST CSF 2.0

Overview of the NIST Cybersecurity Framework 2.0

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 is a voluntary set of guidelines developed to help organizations manage and reduce cybersecurity risks. While voluntary, its adoption can significantly improve an organization's security posture by offering a structured approach to risk management.

In February 2024, NIST released the **CSF 2.0**, updating version 1.1 from April 2018. This update incorporates feedback from various industries and stakeholders, enhancing the framework's flexibility, applicability, and relevance. The NIST CSF 2.0 continues to serve as a voluntary, risk-based framework designed to help organizations of all sizes and sectors manage and reduce cybersecurity risks, foster resilience, and align with best practices.

Purpose of the Framework

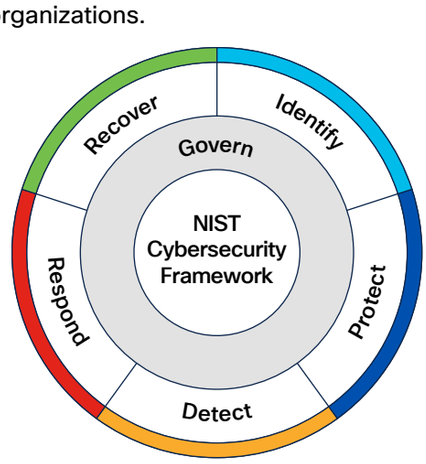
The NIST Cybersecurity Framework provides a structured yet flexible approach to improving an organization's cybersecurity posture. It is used for:

Assessing Risks: Identifying, analyzing, and prioritizing cybersecurity risks.

Guiding Cybersecurity Programs: Establishing or improving cybersecurity strategies in alignment with organizational goals.

Enhancing Communication: Facilitating clear communication about cybersecurity risks and strategies between technical teams, leadership, and external stakeholders.

The framework is particularly valuable for organizations that lack formalized cybersecurity programs or resources, though it is robust enough to benefit even the most mature organizations.



Key Components of the NIST Cybersecurity Framework 2.0

The NIST CSF 2.0 maintains the foundational structure of the original framework while introducing several enhancements. Its key components are:

Core Functions

The Framework Core outlines six **high-level functions** that provide a strategic view of cybersecurity risk management. These functions remain foundational in CSF 2.0 and are as follows:

- **Govern:** Establish and oversee policies, roles, processes, and accountability to align cybersecurity efforts with organizational objectives and regulatory requirements.

  Examples: Risk management policies, executive accountability, cybersecurity governance framework

- **Identify:** Develop an understanding of cybersecurity risks to systems, assets, data, and capabilities. This involves identifying critical resources, threats, and vulnerabilities.

  Examples: Asset management, governance, risk assessments.

- **Protect:** Implement safeguards to ensure the delivery of critical services and mitigate risks.

  Examples: Access control, data protection, training, and maintenance.

- **Detect:** Establish systems to identify cybersecurity events or anomalies in a timely manner.

  Examples: Continuous monitoring, intrusion detection, and threat intelligence.

- **Respond:** Develop and implement appropriate actions to mitigate the effects of a detected cybersecurity event.

  Examples: Incident response planning, mitigation strategies, and communication.

- **Recover:** Develop plans to restore operations and reduce the impact of cybersecurity incidents.

  Examples: Disaster recovery, business continuity planning, and lessons learned.

Implementation Tiers

The framework includes **Implementation Tiers** to help organizations evaluate their current cybersecurity practices and set goals for improvement. These tiers reflect the degree to which an organization's cybersecurity practices are informed by risk management processes, integrated with business needs, and adaptive to evolving risks:

Tier 1 (Partial): Limited awareness and ad hoc implementation of cybersecurity practices.

Tier 2 (Risk-Informed): Risk management practices are formally defined but not fully integrated.

Tier 3 (Repeatable): Cybersecurity practices are consistently applied and documented across the organization.

Tier 4 (Adaptive): Practices are continuously improved and proactively adapted to changing risks.

Profiles

The **Framework Profiles** allow organizations to align the framework to their specific goals, resources, and risk tolerance. A profile compares the current state of an organization's cybersecurity practices to its desired state, serving as a roadmap for improvement.

Why Use the NIST Cybersecurity Framework?

Organizations adopt the NIST CSF 2.0 for several reasons:

Flexibility: Its non-prescriptive nature allows organizations to tailor it to their unique needs.

Widely Recognized: The framework is globally acknowledged as a standard for cybersecurity best practices.

Risk Management: It helps organizations prioritize risks and allocate resources effectively.

Compliance Alignment: While voluntary, the framework aligns with various regulatory requirements and standards, simplifying compliance efforts.

Mapping to other Frameworks

The NIST National Online Informative References (OLIR) Program provides a framework for organizations to map cybersecurity standards, guidelines, and frameworks. By leveraging OLIR, Cisco can cross-reference the NIST Cybersecurity Framework (CSF) 2.0 with other standards like NIST SP 800-53, simplifying compliance and security alignment. This approach eliminates the need for separate mappings, saving time and effort while ensuring traceability across frameworks.

For Cisco, this means that once its security solutions, such as Cisco Secure Access for Government, are mapped to NIST CSF 2.0, these mappings can be extended through NIST OLIR to align with other frameworks. This capability is particularly beneficial for public sector and regulated industries, where compliance with multiple frameworks is often required. By using NIST CSF 2.0 as a common backbone, Cisco helps customers achieve compliance efficiently while demonstrating how its solutions align with best practices and regulatory mandates.

This cross-mapping capability strengthens Cisco's position as a strategic enabler of cybersecurity compliance, providing customers with a clear understanding of how its solutions fit into their broader compliance and risk management strategies.

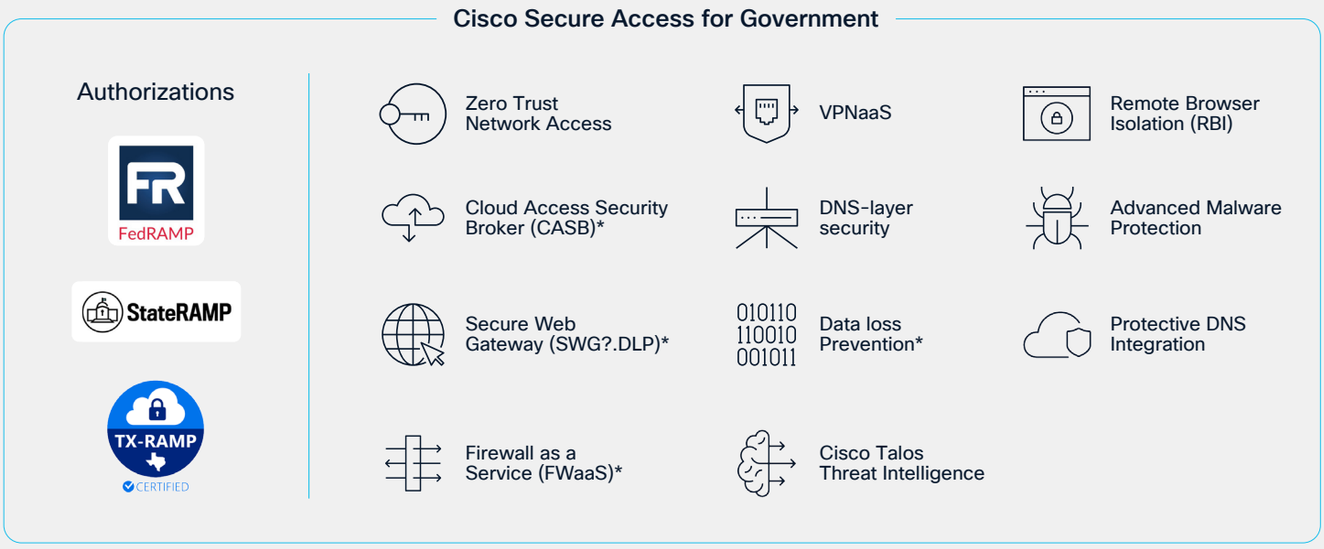


Figure 1: Cisco Secure Access for Government

Understanding Cisco Secure Access for Government

Cisco's Secure Access for Government is designed to provide advanced cybersecurity solutions tailored to meet the stringent requirements of federal and state mandates. This solution that government agencies can protect their workforce and sensitive data both in-office and remotely, leveraging a zero trust cybersecurity framework.

Cisco Secure Access for Government solutions are built on Cisco's commercial SSE and Zero Trust Network Access (ZTNA) solutions and are attracting growing attention in the federal and state government

- Cisco Umbrella for Government
- Cisco Secure Access for Government

For more detailed information, check out Advancing Government Security with Cisco's Security Service Edge.

Cisco Umbrella for Government Overview

Cisco Umbrella for Government is a cloud-native security solution tailored to meet the unique cybersecurity needs of U.S. Federal, State, and Local government agencies. It provides a comprehensive suite of security features, including DNS-layer security, Secure Web Gateway, and Cloud Access Security Broker (CASB), while adhering to compliance standards such as FedRAMP Moderate, StateRAMP, and TX-RAMP. The platform integrates with CISA's Protective DNS and supports enhanced device security, ensuring robust protection for critical government infrastructure.

Technical Features:

Protective DNS Integration

This feature integrates with CISA's Protective DNS to block malicious domains and prevent threats at the DNS layer, ensuring secure internet access for government agencies.

DNS-layer Security

By enforcing security at the DNS level, Umbrella blocks requests to malicious domains, ransomware, and phishing sites before a connection is established.

Data Loss Prevention (DLP)

DLP capabilities monitor and control sensitive data movement, ensuring compliance with government regulations and preventing unauthorized data exfiltration.

Firewall as a Service (FWaaS)

The cloud-delivered firewall provides visibility and control over internet-bound traffic, enforcing consistent security policies across all locations.

Cisco Talos Threat Intelligence

Powered by Cisco Talos, this feature delivers real-time threat intelligence, blocking millions of malicious events daily and enabling proactive threat mitigation.

Cloud Access Security Broker (CASB)

CASB functionality detects and controls the use of cloud applications, providing visibility into shadow IT and enforcing security policies.

Secure Web Gateway (SWG)

The SWG inspects and filters web traffic, providing granular control and protection against web-based threats.

Remote Browser Isolation (RBI)

RBI isolates web traffic from user devices, allowing safe access to potentially risky websites without compromising endpoint security.

Duo Identity Access Management (IAM)

Duo IAM ensures secure access to applications by verifying user identities and device health, supporting a zero-trust security model.

Cisco Secure Access for Government

In addition to Umbrella for Government, Cisco Secure Access for Government integrates additional advanced security features to provide a robust, unified solution for safeguarding government infrastructure. By leveraging Cisco Umbrella for Government, it ensures compliance with stringent standards like FedRAMP and StateRAMP while delivering DNS-layer security, Secure Web Gateway, and Cloud Access Security Broker (CASB) capabilities.

The Cisco Secure Access for Government solution simplifies management through a single dashboard, enabling seamless access to private and cloud applications while maintaining a zero-trust security model.

Features:

Zero Trust Network Access (ZTNA)

Provides granular, app-specific secure access to private applications using least privilege principles, ensuring that users only access resources explicitly granted to them.

Advanced Firewall-as-a-Service (FWaaS)

Protects against sophisticated threats with multi-layered security, including intrusion prevention and malware sandboxing.

Single Dashboard

Simplifies IT operations by consolidating management of security policies, user access, and threat monitoring into one interface.

VPN-as-a-Service (VPNaaS)

Ensures secure remote access to private applications, complementing ZTNA for non-web traffic.

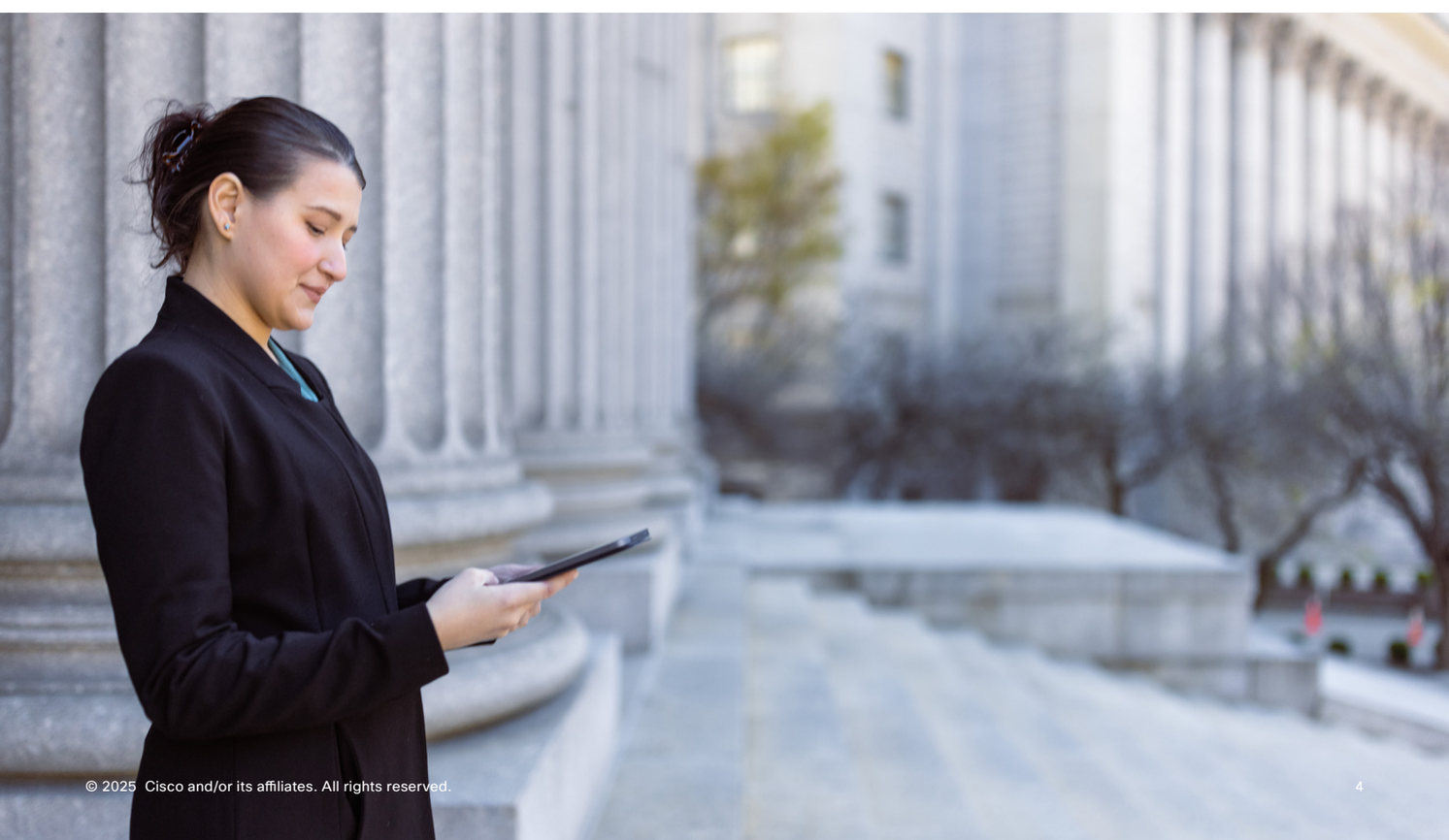
Cisco Single Client

Unifies user access with a single, secure client for seamless connectivity to applications and resources.

Unified Policies

Enables consistent enforcement of security policies across all applications and devices, reducing complexity and enhancing compliance.

Cisco SSE Solutions add a vital dimension to Cisco's commitment to federal, state and local government in supporting their networking, security, and AI needs.



Cisco Secure Access for Government: Key Benefits and Capabilities

Cisco's Secure Access for Government is purpose-built to meet the evolving needs of U.S. public sector organizations – including federal, state, and local agencies, as well as educational institutions. It delivers a comprehensive, secure, and scalable solution with the following core benefits:

Enhanced Security and Compliance

- **Adaptive Threat Defense:** Proactively protects against emerging cyber threats targeting government workforces.
- **Zero-Trust Architecture:** Delivers secure, high-performance access to private applications with granular control and stealth connections.
- **Regulatory Compliance:** Meets stringent federal and state mandates including NIST, TIC 3.0, CISA, CMMC, and Executive Order 14028. Supports FedRAMP and StateRAMP-authorized solutions.

Improved Productivity

- **Seamless Access Anywhere:** Enables secure, productive work environments—whether in the office, in the field, or at home.
- **Consistent User Experience:** Maintains security without compromising performance or accessibility.

Simplified IT Operations

- **Unified Management:** Centralized dashboard and client for streamlined policy management and reduced operational complexity.
- **AI-Driven Automation:** Leverages AI to enhance policy creation, reduce human error, and improve overall efficiency.

Cost Efficiency and Scalability

- **Operational Savings:** Reduces costs through unified security management and automated monitoring.
- **Flexible Scalability:** Designed to support organizations of all sizes, from small local agencies to large federal institutions.

Advanced Threat Protection

- **Real-Time Monitoring:** Ensures safe internet and SaaS access with features like DNS-layer security, secure web gateway, and cloud-delivered firewall.

Comprehensive Visibility and Control

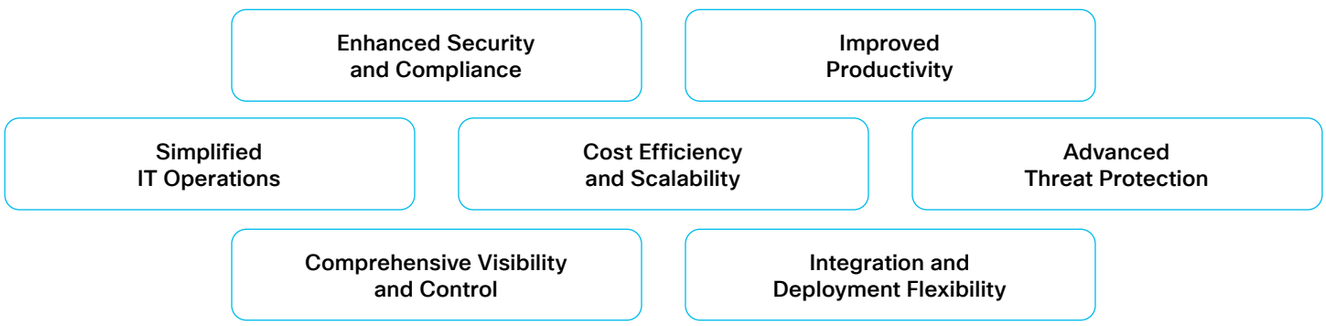
- **Centralized Oversight:** Provides visibility across all applications and devices, ensuring secure access for both managed and unmanaged endpoints.

Integration and Deployment Flexibility

- **Broad Compatibility:** Integrates with Cisco and third-party SD-WAN solutions.
- **Flexible Deployment Options:** Supports ZTNA resource connectors and VPN-as-a-Service for diverse infrastructure needs.

FedRAMP Process

Cisco's Secure Access for Government is undergoing the FedRAMP (Federal Risk and Authorization Management Program) process, which is crucial for ensuring that cloud services meet federal security standards. FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This process is essential for federal agencies to ensure that the cloud services they use are secure and compliant with federal regulations.



Mapping Cisco Secure Access for Government to NIST CSF 2.0

Secure Access for Government Capability Mapping to NIST CSF 2.0 and NIST 800-53

		Secure Access for Government NIST CSF 2.0 Mapping		Secure Access for Government NIST 800-53 Mapping	
Function	**Category**	**Yes**	**Supports**	**Yes**	**Supports**
Govern (GV)		Non-technical controls			
Identify (ID)	Asset Management (ID.AM)	**ID.AM-01, ID.AM-04**	ID.AM-02, ID.AM-03, ID.AM-08	**CM-08, PM-05, AC-20, SA-09, SR-02**	AC-20, CM-08, PM-05, SA-05, SA-09, AC-04, CA-03, CA-09, PL-02, PL-08, PM-07, CM-09, CM-13, MA-02, MA-06, PL-02, PM-22, PM-23, SA-03, SA-04, SA-08, SA-22, SI-12, SI-18, SR-05, SR-12
	Risk Assessment (ID.RA)	**ID.RA-02, ID.RA-03**		**SI-05, PM-15, PM-16, PM-12, PM-16, RA-03, SI-05**	
	Improvement (ID.IM)	Non-technical controls			
Protect (PR)	Identity, Management, Authentication, and Access Control (PR.AA)	**PR.AA-03, PR.AA-04, PR.AA-05**	PR.AA-01	**AC-07, AC-12, IA-02, IA-03, IA-05, IA-07, IA-08, IA-09, IA-10, IA-11, IA-13, AC-01, AC-02, AC-03, AC-05, AC-06, AC-10, AC-16, AC-17, AC-18, AC-19, AC-24, IA-13**	AC-01, AC-02, AC-14, IA-01, IA-02, IA-03, IA-04, IA-05, IA-06, IA-07, IA-08, IA-09, IA-10, IA-11
	Awareness and Training (PR.AT)	Non-technical controls			
	Data Security (PR.DS)	**PR.DS-02**	PR.DS-01, PR.DS-10	**AU-16, CA-03, SC-04, SC-07, SC-08, SC-11, SC-12, SC-13, SC-16, SC-40, SC-43, SI-03, SI-04, SI-07,**	CA-03, CP-09, MP-08, SC-04, SC-07, SC-12, SC-13, SC-28, SC-32, SC-39, SC-43, SI-03, SI-04, SI-07, AC-02, AC-03, AC-04, AU-09, AU-13, CA-03, CP-09, SA-08, SC-04, SC-07, SC-11, SC-13, SC-24, SC-32, SC-39, SC-40, SC-43, SI-03, SI-04, SI-07, SI-10, SI-16
	Platfrom Security (PR.PS)	**PR.PS-04, PR.PS-05**		**AU-02, AU-03, AU-06, AU-07, AU-11, AU-12, CM-07(02), CM-07(04), CM-07(05), SC-34**	
	Technology Infrastructure Resilience (PR.IR)	**PR.IR-01**	PR.IR-03, PR.IR-04	**AC-03, AC-04, SC-04, SC-05, SC-07**	CP, IR, SA-08, SC-06, SC-24, SC-36, SC-39, SI-13, CP, IR, SA-08, SC-06, SC-24, SC-36, SC-39, SI-13
Detect (DE)	Continuous Monitoring (DE.CM)	**DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09**		**AC-02, AU-12, CA-07, CM-03, SC-05, SC-07, SI-04, AC-02, AU-12, AU-13, CA-07, CM-10, CM-11, CA-07, PS-07, SA-04, SA-09, SI-04, AC-04, AC-09, AU-12, CA-07, CM-03, CM-06, CM-10, CM-11, SC-34, SC-35, SI-04, SI-07**	
	Adverse Event Analysis (DE.AE)	**DE.AE-02**	DE.AE-03, DE.AE-04, DE.AE-06, DE.AE-07	**AU-06, CA-07, IR-04, SI-04**	AU-06, CA-07, PM-16, IR-04, IR-05, IR-08, SI-04, PM-09, PM-11, PM-18, PM-28, PM-30, IR-04, PM-15, PM-16, RA-03, RA-10, PM-16, RA-03, RA-10
Respond (RS)	Incident Management (RS.MA)	Non-technical controls			
	Incident Analysis (RS.AN)		RS.AN-03, RS.AN-07, RS.AN-08		AU-07, IR-04, AU-07, IR-04, IR-06, IR-04, IR-08, RA-03, RA-07
	Incident Response Reporting and Communication (RS.CO)	Non-technical controls			
	Incident Mitigation (RS.MI)	**RS.MI-01**		**IR-04**	
Recover (RC)	Incident Recovery Plan Execution (RC.RP)	None		None	
	Incident Recovery Communication (RC.CO)	Non-technical controls			

Get Started

The NIST Cybersecurity Framework 2.0 offers a flexible, scalable approach to managing cybersecurity risks. Cisco Secure Access for Government aligns with NIST CSF 2.0 and NIST 800-53, helping public sector organizations enhance security, ensure compliance, and maintain operational resilience. With features like zero-trust access, AI-driven policy management, and FedRAMP-authorized solutions, Cisco's offerings enable secure, efficient operations across diverse environments.

Learn more:

Cisco Secure Access for Government

Cisco Umbrella for Government

Advancing Government Security with Cisco's Security Service Edge