RON WYDEN
OREGON

RANKING MEMBER OF COMMITTEE ON FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224–5244

United States Senate
WASHINGTON, DC 20510–3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

July 27, 2026

The Honorable Gregory Barbaccia
Federal Chief Information Officer
Office of Management and Budget
725 17th Street, NW
Washington, DC 20503

Nick Andersen
Acting Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
Washington, DC 20528

The Honorable Arvind Raman
Under Secretary of Commerce for Standards and Technology
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Dear Mr. Barbaccia, Mr. Andersen and Dr. Raman:

I write to urge the Office of Management and Budget (OMB), the Cybersecurity and Infrastructure Security Agency (CISA), and the National Institute of Standards and Technology (NIST) to coordinate updates to federal cybersecurity standards to mandate the phaseout of insecure, legacy, internet-facing Virtual Private Network (VPN) and other remote-access systems and require the adoption of modern, secure remote-access technology across the federal government.

Traditionally, large organizations have provided employees with mobile and remote access to enterprise systems, including email, using remote-access tools such as VPNs and remote desktop servers. Legacy remote-access technologies operate a digital "front door" that is accessible to the public internet so that mobile devices and remote employees can log in. Because these entry points are exposed, hackers can easily scan, target, and break into them. Modern remote-access solutions eliminate this vulnerability entirely. Instead of leaving an open door accessible from the public internet, modern solutions provide remote access without broadcasting their presence. This effectively makes these servers invisible, ensuring that hackers cannot attack an entry point they cannot see. The attached Congressional Research Service memorandum goes into greater detail on the threat posed by legacy remote access technologies and the advantages of modern “zero trust” systems.

For too long, federal agencies and government contractors have suffered devastating cyberattacks due to their reliance on legacy, insecure, internet-facing VPN servers to grant employees remote access. Multiple

recent and devastating hacking campaigns have targeted VPN and remote-access systems, including the state-sponsored ArcaneDoor attacks on Cisco firewalls, the massive FortiBleed credential exposures across Fortinet gateways, and the severe vulnerabilities exploited across Ivanti and Check Point VPN appliances. Data from the Travelers Q4 2025 Cyber Threat Report only underscores the scale of this crisis, revealing that 85% of ransomware-related insurance claims during that period originated from the exploitation of a VPN. The federal government has attributed these aggressive operations to sophisticated foreign adversaries, including, most notably, Chinese and Russian state-sponsored hackers. Through these hacks, foreign adversaries gained administrative access to target networks, allowing them to steal sensitive data from U.S. government agencies and companies.

The federal government has become trapped in an endless game of "whack-a-mole" in responding to widespread compromises of legacy remote access technologies. To keep federal networks online, CISA has been forced to repeatedly issue extraordinary Emergency Directives and hyper-accelerated patch mandates. These reactive emergency mandates are unsustainable for federal cybersecurity teams and fail to address the fundamental issue that these flaws are inherent in the use of legacy remote-access appliances.

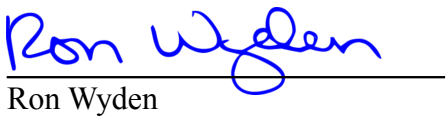
It is no longer acceptable for agencies to use insecure, decades-old technology. Modern remote-access alternatives eliminate the need to run an exposed, public-facing server that adversaries can discover and target. Crucially, the vast majority of critical vulnerabilities exploited in legacy remote-access systems stem from preventable memory management errors, such as buffer overflows, inherent in older programming languages. As the National Security Agency (NSA), CISA, and the Federal Bureau of Investigation have recommended, federal agencies can systematically neutralize this entire class of vulnerabilities by adopting software written in modern, memory-safe programming languages. Agencies should further insulate themselves from third-party supply chain failures by maintaining exclusive control over their encryption keys, ensuring that a compromise at a software provider does not equate to a compromise of federal data. To protect the federal government, we urge your agencies to take the following actions (as applicable):

- **Eliminate Exposed Entry Points:** CISA must issue a Binding Operational Directive setting a two-year deadline for civilian agencies to completely sunset legacy, public-facing remote access systems, in favor of zero trust architecture. Concurrently, utilizing the new authorities granted under National Security Presidential Memorandum 12, the Director of NSA must issue a parallel directive mandating the same two-year sunset timeline for all legacy remote access gateways and perimeter entry points across military, intelligence, and other federal national security networks.
- **Establish Zero-Trust Standards:** NIST must develop and issue implementation standards for agencies transitioning to zero-trust architectures that replace legacy remote access systems. These standards must explicitly mandate:
    - Outbound-only remote access architectures.
    - Software written in memory-safe programming languages.
    - Decentralized, organization-held encryption keys to isolate agencies from third-party vendor breaches.

    - Alignment with established and emerging Post-Quantum Cryptography standardization efforts.
- **Prioritize Zero Trust Investments and Mandate Adoption of NIST Standards:** OMB must issue a memorandum directing federal agencies to prioritize zero-trust infrastructure investments, systematically decommission legacy remote-access systems during the budget cycle, and mandate the swift adoption of the new NIST standards across all federal agencies.
- **Update the Federal Acquisition Regulations (FAR):** OMB, in coordination with CISA and the Department of Defense, should issue a procurement memorandum updating the FAR and Defense Federal Acquisition Regulation Supplement. This update must bar agencies and defense contractors from purchasing network edge, VPN, or other remote access solutions unless the vendor provides a formal attestation verifying compliance with the newly established NIST zero-trust standards.

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian and Daniel Reichert in my office.

Sincerely,



Ron Wyden
United States Senator

CC:

The Honorable Kirsten Davies, Chief Information Officer, Department of Defense
The Honorable General Joshua M. Rudd, Director, National Security Agency

Congressional Research Service
Informing the legislative debate since 1914

MEMORANDUM July 17, 2026

To: Senator Ron Wyden
Attention: Chris Soghoian

From: [redacted]

Subject: **Comparison of Remote Access Technologies, Risks, and Policies**

This memorandum responds to your request for information regarding traditional virtual private network (VPN) architecture and newer zero-trust network architectures (ZTNA). You specifically requested discussions on how each technology works, the security risks associated with each, and considerations federal agencies should contemplate when transitioning from VPNs to ZTNA.

Information contained in this memorandum is of general interest to Congress and may be used in other CRS products. Your confidentiality as a requestor will be preserved in any event. If you have additional questions, please do not hesitate to contact me.

Technology Overview

In the 1990s, most information security leveraged a *castle-and-moat* type strategy. This security model is based on the premise that anyone outside the network (i.e., beyond the castle walls) is not authorized to access an organization's computing resources, but everyone inside is. This strategy was physically enabled through hardware—to access digital resources, desktop computers were physically wired to servers in the organization's facility.

As the internet proliferated and computing devices became mobile (beginning with laptops), organizations needed a way to enable trust and authorize access to the inside of their networks from an outside, physical site. Continuing the castle analogy, *virtual private networks* created a bridge and allowed certain authorized external traffic to flow inside that network. The inherent presumption with this model remained: Everything outside the organization is not authorized to access the network, while users and devices inside the organization are authorized—with the VPN affording internal network access.

Organizations became more geographically dispersed. Workers became more mobile, and computing resources began being hosted offsite or virtually (e.g., through the use of cloud computing and web-based services). As a consequence, those still using the castle-and-moat strategy needed to create more and more virtual bridges to connect authorized users to digital resources. While this happened, adversaries began to exploit the vulnerabilities in VPN appliances (and other edge-of-network equipment, like routers—otherwise known as edge devices). In response, both the government and private sector began developing a new security framework known as *zero-trust architecture* (ZTA) which uses a *never-trust, always verify*

security model.[1] Unlike the castle-and-moat strategy, ZTA does not provide preferential treatment to users inside of a network. Instead, it scrutinizes every attempt to access a computing resource for the appropriateness of that access. Everyone, both inside and outside the castle, is examined as potential threat to the network's security.

Virtual Private Networks

A VPN creates a secure connection between a remote user and the organization's network, to treat the remote user connecting to the organization's network like an internal user. This connection requires a *host* and a *client*. The *host* is a networking device that sits between an organization's private, internal network and the public internet. It negotiates an encrypted connection with the user's device. A VPN appliance (i.e., the host), is typically located at the edge of an organization's network and is internet-facing itself (i.e., it is internet routable and discoverable on the internet). The *client* is an application on the user's device that communicates with the VPN appliance and manages the VPN connection on that client device.

Traditional, enterprise-level VPNs rely on a perimeter-security model. The VPN appliance sits at the network boundary, listens on one or more public-facing ports (i.e., it is accessible via the public internet and awaits certain communications), and authenticates remote users. It then grants them access to the broad internal network. This architecture carries three fundamental assumptions: (1) the VPN appliance is always reachable from the internet; (2) once authenticated, the user is trusted to access the internal network; and (3) the appliance's software can be kept securely patched and maintained. Each of these assumptions has been systematically exploited in recent years.[2]

The following are key technical characteristics of a VPN:[3]

- **Listening port use**: The VPN gateway must maintain one or more publicly-accessible listening ports (e.g., UDP 500 or 4500) to accept inbound connections from remote clients.[4] This internet-facing posture makes the gateway discoverable and scannable by anyone on the internet.[5]
- **Network-level access**: After authentication, the user's device is assigned an IP address on the corporate network and can typically route traffic to any subnet permitted by firewall rules. Access is controlled at the network layer, not the application layer, using the Open Systems Interconnection (OSI) model.[6]

[1] In this memorandum, ZTA is used to refer to the concept of continuous verification of users, identities, devices, and data on a network. ZTNA is used to refer to the infrastructure and implementation of ZTA for an organization's entire network.

[2] Lazarus Alliance, "What CISA's Emergency Directive 26-01 Means for Everyone," blog post, November 26, 2025, https://lazarusalliance.com/what-cisas-emergency-directive-26-01-means-for-everyone/.

[3] In this memorandum, VPN refers generally to a virtual private network; VPN appliance refers to the hardware device that provides the service for a network; and VPN gateway refers to the two-way communications service operating on the VPN appliance.

[4] A port is a virtual node where network connections begin and end. They are software-based and associated with specific processes and services. Ports allow computers to differentiate between different kinds of network traffic. For more information, see https://www.cloudflare.com/learning/network-layer/what-is-a-computer-port. UDP is the User Datagram Protocol and is used for time-sensitive communications on the internet (like video streams).

[5] National Security Agency, "Configuring IPSec Virtual Private Network," *Cybersecurity Information,* February 2025, https://media.defense.gov/2020/Jul/02/2002355501/-1/-1/0/Configuring_IPsec_VPN_UOO148260_20_V1_2..PDF.

[6] Lukasz Gil, "ZTNA vs VPN: How is Zero Trust Network Access Revolutionizing Secure Remote Access?" website, February 5, 2026, https://nflo.tech/knowledge-base/ztna-vs-vpn-how-is-zero-trust-network-access-revolutionizing-secure-remote-access/ (Hereafter Gil); and International Organization for Standardization, "Information Technology—Open Systems Interconnection—Basic Reference Model: The Basic Model," *ISO/IEC 7498-1:1994*, Edition 1, 1994, https://www.iso.org/standard/20269.html.

- **Centralized traffic routing**: All user traffic is typically routed through the VPN appliance at an organization's facility, potentially creating latency and bandwidth bottlenecks—especially for cloud-hosted applications.[7]
- **One-time authentication**: Most VPN implementations verify user identity at the time of the connection and retain that authorization for the entirety of the session.[8] They do not continuously reassess access during a user's session.[9]

These types of VPNs include Internet Protocol Security (IPsec)-based, secure sockets layer (SSL), and transport layer security (TLS)-based remote access products such as Ivanti Connect Secure, Cisco AnyConnect, Fortinet SSL-VPN, and Pulse Secure.

Zero-Trust Network Architecture

Zero Trust Architecture is a cybersecurity paradigm that assumes no implicit trust is granted to assets or user accounts based on solely on their physical or network location.[10] The National Institute of Standards and Technology (NIST) prescribes the tenets of ZTNA, emphasizing: continuous verification; strict access control; and policy enforcement across users, devices, and workloads.[11]

The NIST ZTA model centers on three core components: the *Policy Engine* (PE), which makes grant/deny decisions; the *Policy Administrator* (PA), which establishes or shuts down sessions; and the *Policy Enforcement Point* (PEP), which enables, monitors, and terminates connections between subjects and resources.[12] This design separates the *control plane* (i.e., where access decisions are made) from the *data plane* (i.e., where data flows).[13]

Modern ZTNA implementations often use overlay networks—software-defined network (SDN) layers that sit atop existing infrastructure. Overlay networks establish encrypted tunnels using outbound-only connections from endpoints. Endpoints initiate connections to overlay routers rather than listening on publicly visible ports, rendering protected resources invisible to unauthorized parties and network scanners.[14]

ZTNA overlay networks can be open, such as those built on WireGuard and OpenZiti, or proprietary solutions, such as Zscaler Private Access, Appgate SDP, or Tailscale.

The key technical characteristics of a ZTNA are:

- **Outbound-only connections**: ZTNA connectors deployed inside the network initiate outbound connections to a cloud-based ZTNA service. No inbound listening ports are opened on the

[7] Gil.

[8] A "session" is "[a] persistent interaction between a subscriber and an end point, either a relying party or a Credential Service Provider. A session begins with an authentication event and ends with a session termination event. A session is bound by use of a session secret that the subscriber's software (a browser, application, or operating system) can present to the relying party or the Credential Service Provider in lieu of the subscriber's authentication credentials." https://csrc.nist.gov/glossary/term/session.

[9] Cato Networks, "ZTNA vs VPN: Which Security Solution Is Right for Your Business?" https://www.catonetworks.com/zero-trust-network-access/ztna-vs-vpn/.

[10] NetFoundry, "Secure Partner Connectivity without VPN Headaches," https://netfoundry.io/resources/partner-connectivity/.

[11] Scott Rose, Oliver Borchert, Stu Mitchel, et al., "Zero Trust Architecture," *NIST Special Publication 800-207*, August 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf. (Hereafter NIST SP 800-207).

[12] NIST SP 800-207.

[13] Terrazone, "Control Plane vs. Data Plane in Modern ZTNA Platforms," May 18, 2025, https://terrazone.io/control-plane-data-plane/.

[14] Greg Shields, "Inside ZTNA: The Secret Sauce of Better Single Packet Authorization," April 3, 2023, https://www.appgate.com/blog/inside-ztna-the-secret-sauce-of-better-single-packet-authorization.

corporate firewall. Applications and infrastructure remain invisible to the public internet. This method is also referred to as a "hole-punch."[15]

- **Application-level, specific tunnels**: Instead of placing a user onto the network, ZTNA creates an encrypted, application-specific micro-tunnel between application and user. The user can only reach the single authorized application for a particular session.[16]
- **Identity-driven policy**: Access decisions are made by a centralized policy engine based on a user's role, device health, and contextual signals—not by network location or user credential alone.[17]
- **Continuous verification**: The Policy Engine evaluates every access request in real time based on user identity, device posture, geolocation, behavioral analytics, and risk scoring. Trust is never implicit and is reassessed throughout the session.[18]

Security Risks

Both VPNs and ZTNA systems face security risks. The risks inherent to VPNs are broader, and they have been studied more thoroughly because the technology has existed longer. This section discusses the risks of these remote connection architectures.

VPN: Inherent Risks for Internet Connected Edge Devices

VPN appliances are, by definition, internet-facing edge devices. They must expose at least one listening port to the public internet in order to accept incoming connections. This architectural requirement makes them permanently visible to adversaries conducting port scans; any unpatched vulnerability on the appliance becomes immediately exploitable from anywhere in the world.[19] The concerns with these types of edge devices have been highlighted by a sequence of operational directives from the Cybersecurity and Infrastructure Security Agency (CISA), as shown in **Table 1**.[20]

Table 1. CISA Emergency and Binding Operational Directives Addressing VPN Appliances

By date, in ascending order

Directive	Date	Appliance	Concern Addressed with Directive
ED 21-03	April 2021	Pulse Connect Secure	Threat actor exploitation of disclosed vulnerabilities in the tool.[a]
ED 22-03	May 2022	VMware	Remote code execution without authentication.[b]
ED 24-01	January 2024	Ivanti Connect Secure	Known instances of threat actor exploitation of vulnerabilities to access networks, steal data, and maintain persistent access.[c]

[15] Bryan Ford, Pyda Srisuresh, and Dan Kegel, "Peer-to-peer Communication Across Address Translators," website, https://bford.info/pub/net/p2pnat/.

[16] Lukasz Gil, "ZTNA vs VPN: How is Zero Trust Network Access Revolutionizing Secure Remote Access?" website, February 5, 2026, https://nflo.tech/knowledge-base/ztna-vs-vpn-how-is-zero-trust-network-access-revolutionizing-secure-remote-access/.

[17] Michael Hendricks, "ZTNA vs VPN: Which Is The Best Solution," June 25, 2025, https://www.rippling.com/blog/ztna-vs-vpn.

[18] Pierre Morel, "ZTNA vs VPN: Why It's Time To Rethink Remote Access," https://www.open-systems.com/blog/ztna-vpn/.

[19] Dragos, "Why Adversaries Target VPN Appliances: The Pathway from IT to OT Cyber Attack," blog post, September 30, 2024, https://www.dragos.com/blog/why-adversaries-target-vpn-appliances-the-pathway-from-it-to-ot-cyber-attack.

[20] *Emergency operational directives* and *binding operational directives* are an authority found in 44 U.S.C. §3553(f) to identify risks to federal agency IT systems and compel actions for remediation.

Directive	Date	Appliance	Concern Addressed with Directive
ED 26-01	October 2025	F5 Devices	Nation-state actor compromised F5's systems, stealing source code and vulnerability information.[d]
ED 26-03	February 2026	Cisco Catalyst SD-WAN	Threat actor exploiting vulnerable systems.[e]
BOD 26-02	February 2026	End-of-Service edge devices	Unsupported devices creating a persistent risk.[f]

Source: CRS analysis.

Notes:

a. Jordan Smith, "CISA Alerts Agencies to Check Pulse Connect Secure Products," *MeriTalk*, April 21, 2021, https://www.meritalk.com/articles/cisa-alerts-agencies-to-check-pulse-connect-secure-products/.

b. "CISA Issues Emergency Directive Requiring Federal Agencies Mitigate Vulnerabilities in VMware Products," press release, May 18, 2022, https://www.cisa.gov/news-events/news/cisa-issues-emergency-directive-requiring-federal-agencies-mitigate-vulnerabilities-vmware-products.

c. CISA, "ED 21:01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities," *ED 24-01*, January 19, 2024, https://www.cisa.gov/news-events/directives/ed-24-01-mitigate-ivanti-connect-secure-and-ivanti-policy-secure-vulnerabilities.

d. CISA, "ED 26-01: Mitigate Vulnerabilities in F5 Devices," *ED 26-01*, October 15, 2025, https://www.cisa.gov/news-events/directives/ed-26-01-mitigate-vulnerabilities-f5-devices.

e. CISA, "ED 26-03: Mitigate Vulnerabilities in Cisco SD-WAN Systems," *ED 26-03,* February 25, 2026, https://www.cisa.gov/news-events/directives/ed-26-03-mitigate-vulnerabilities-cisco-sd-wan-systems.

f. CISA, "BOD 26-02: Mitigating Risk of End of Support Edge Devices," *BOD 26-02*, February 5, 2026, https://www.cisa.gov/news-events/directives/bod-26-02-mitigating-risk-end-support-edge-devices.

In addition to the VPN concerns above, an undisclosed, state-sponsored threat group targeted Cisco ASA VPN appliances in a campaign that became known as ArcaneDoor. The threat actors deployed the Line Dancer and Line Runner custom backdoors to intercept traffic, modify authentication processes, and maintain persistent access to government and critical infrastructure networks.[21]

VPN: Listening Port

The most fundamental architectural difference between traditional VPNs and modern ZTNA solutions lies in their connectivity models. A VPN appliance must bind to a public IP address and listen on known ports—creating a permanent, scannable target. An attacker may use commonly available scanning tools to discover VPN endpoints, identify their software version, and attempt exploitation.[22] Tools like Nmap and Shodan can make this scanning easier and readily available to attackers and defenders alike.

VPN: Legacy Code Bases

Software is stored on a computing device's drive (e.g., a hard drive) and runs in a computing device's memory, called *random access memory* (RAM). Software running in memory may be unintentionally modified, creating a security risk. Some VPN vulnerabilities stem from the fact that certain VPN implementations are written in older code languages susceptible to memory corruption via buffer overflows.[23] A buffer overflow attack causes a program to overwrite the amount of allocated memory in the RAM for a computer program. Breaking from predefined memory storage allotments can allow an attacker to insert code into that memory that would allow them to gain control of the system.[24] For

[21] Jun Hirata, Sareena Karapoola, and Pooja Natarajan, "ArcaneDoor," C0046, March 10, 2025, https://attack.mitre.org/campaigns/C0046/.

[22] Palo Alto Networks, "What is a Port Scan?" https://www.paloaltonetworks.com/cyberpedia/what-is-a-port-scan.

[23] For an example, see https://www.cve.org/CVERecord?id=CVE-2025-7775.

[24] NIST, "Buffer Overflow," https://csrc.nist.gov/glossary/term/buffer_overflow.

example, the C programming language permits direct memory manipulation, making it susceptible to buffer overflow, use-after-free conditions, double-free errors, and use of uninitiated memory—all of which can lead to arbitrary code execution.[25] In a VPN context, that memory often belongs to a privileged process, or even a kernel-level operation, so a successful buffer overflow attack can enable remote code execution or full device compromise, depending on what gets overwritten. For instance, in August 2024, Microsoft researchers disclosed four memory management vulnerabilities in OpenVPN that, when chained, enabled remote code execution and local privilege escalation—allowing an attacker unfettered access to a system.[26] Other VPN-based buffer overflow attacks include those against SoftEther VPN as well as the Ivanti Connect Secure appliance vulnerability listed in **Table 1**.[27]

VPN: Key-Exchange Issues

To maintain a secure connection, VPNs use symmetric encryption keys. But, to establish that key, the VPN host and client need to negotiate that shared key through a cryptographic handshake (i.e., the protocol of synchronizing operations between two systems). This handshake is susceptible to attack and has been exploited in the past. Researchers have demonstrated that a man-in-the-middle attacker could downgrade connections, enabling decryption of intercepted traffic.[28] Other researchers were able to exploit key reuse across VPN sessions to impersonate devices.[29] Finally, even if an attacker does not access a VPN's data, they can attack the VPN appliance by forcing computationally expensive key calculations, leading to a denial-of-service against the VPN service.[30]

VPN: Lateral Movement

Many attackers seek to compromise a VPN to gain access to a target network. They can do this by stealing a user's legitimate VPN credential and logging into the VPN appliance as that user (exploiting a vulnerability with the VPN client or host), or by hijacking a legitimate VPN client's session (e.g., gaining access to the laptop and waiting for that user to log in). Regardless of how the attacker gets past the VPN, the traditional VPN model grants them broad access to the internal network. This appears to be a popular attack method against VPNs.[31]

ZTNA: Control Plane

ZTNA is not without its own risks—particularly concerning the control plane. In a ZTNA architecture, the control plane (where the policy engine rests) is the centralized component responsible for authenticating

[25] CISA, et al., "The Case for Memory Safe Roadmaps: Why Both C-Suite Executives and Technical Experts Need to Take Memory Safe Coding Seriously," December 2023, https://www.cisa.gov/sites/default/files/2023-12/The-Case-for-Memory-Safe-Roadmaps-508c.pdf.

[26] Microsoft Threat Intelligence, "Chained for Attack: OpenVPN Vulnerabilities Discovered Leading to RCE and LPE," research blog, August 8, 2024, at https://www.microsoft.com/en-us/security/blog/2024/08/08/chained-for-attack-openvpn-vulnerabilities-discovered-leading-to-rce-and-lpe/?msockid=0691a0dde427607e18d6b7c9e54f6189.

[27] National Vulnerability Database, "CVE-2005-25567 Detail," June, 17, 2026, https://nvd.nist.gov/vuln/detail/CVE-2025-25567.

[28] Bruce Schneier, "The Logjam (and Another) Vulnerability against Diffie-Hellman Key Exchange," *Schneier on Security*, May 24, 2015, https://www.schneier.com/blog/archives/2015/05/the_logjam_and_.html.

[29] Dennis Felsch, Martin Grothe, Jörg Schwenk, et al., "The Dangers of Key Reuse: Practical Attacks on IPsec IKE," *USENIX Security Symposium*, August 15-17, 2018, https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-felsch.pdf.

[30] SentinelOne, "CVE-2022-40735: Diffie-Hellman Key Exchange DoS Vulnerability," alert, February 24, 2026, https://www.sentinelone.com/vulnerability-database/cve-2022-40735/.

[31] Kurt Baker, "Lateral Movement Explained," February 12, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/lateral-movement/.

users, verifying device compliance, enforcing access policies, and orchestrating connections between subjects and resources.[32]

Subversion of the ZTA decision process (by compromising elements of the control plane) is a primary threat. If an attacker compromises the Policy Engine or Policy Administrator, they can manipulate access control decisions—granting unauthorized access to resources or denying access to legitimate users. This risk is particularly acute because the control plane is typically centralized and/or cloud-based, allowing an attacker to target the vendor (the ZTNA provider) instead of the organization, and still achieve their results.[33]

A way of reducing ZTNA control plane compromise is by adding an extra later of security by requiring that every device's node be cryptographically signed by a trusted device prior to allowing other devices to communicate with it. In such cases, each node generates its own public/private key pair locally, but its public key must be signed by a designated, trusted signing node. In more secure implementations, that trusted signing node is controlled by the user, to reduce reliance on the ZTNA provider. Only when that node accepts the key will the control plane permit connections. This design reduces the cascading risk of compromise to the ZTNA provider's infrastructure that could potentially result in exposure of an entity's connections and networks. Tailscale Tailnet Lock (Tailscale Lock) is an example of this type of system. [34]

Considerations for Agencies Adopting ZTNA

Agencies investigating whether to continue investing in VPN architectures or transition to ZTNAs must consider existing federal polices; the programming, planning, budgeting, and execution process; and technical limitations.

Federal Policies

The transition from VPN to ZTNA may not reflect a technological preference by agencies—rather, executive orders, Office of Management and Budget (OMB) memoranda, NIST guidance, and CISA guidance are seen as signaling a *need* for the federal government to adopt zero-trust architectures.

- **NIST Special Publication 800-207** (August 2020): This document defines the foundational principles, logical components, and deployment models for ZTA. Its seven tenets include: all data sources and computing services are resources; all communication is secured regardless of network location; access is granted per-session with least privilege; access is determined by dynamic policy; all assets are continuously monitored; authentication and authorization are dynamic and strictly enforced; and the enterprise collects maximum information to improve its security posture.[35]
- **Executive Order 14028** (May 12, 2021): President Biden's executive order *Improving the Nation's Cybersecurity* directed federal agencies to adopt Zero Trust architecture, implement multifactor authentication, and migrate to secure cloud services. The order recognized the growing threats posed by cyber adversaries and mandated modernization of federal cybersecurity practices across all federal civilian executive branch agencies.[36]

[32] NIST SP 800-207.

[33] NIST SP 800-207.

[34] Tailscale, "Tailnet Lock," December, 2, 2025, https://tailscale.com/docs/features/tailnet-lock.

[35] NIST SP 800-207.

[36] Executive Office of the President, "Improving the Nation's Cybersecurity" *Executive Order 14028*, May 12, 2021, https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

- **OMB Memorandum M-22-09** (January 26, 2022): *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* set forth a Federal ZTA strategy requiring agencies to meet specific cybersecurity standards and objectives by the end of FY 2024. It established five pillars—Identity, Devices, Networks, Applications and Workloads, and Data—and required enterprise-wide MFA, encrypted traffic, and isolated agency systems.[37] CRS was unable to determine the extent to which agencies have met their M-22-09 objectives.[38]
- **CISA Trusted Internet Connections (TIC) 3.0** (December 2023): TIC 3.0 modernized the original TIC program to support decentralized network perimeters, cloud services, and zero trust architecture. Unlike TIC 2.0's strictly perimeter-based approach, TIC 3.0 divides agency architectures by trust zones, shifts emphasis to boundaries within an agency environment, rather than at a single physical perimeter, and includes sample architectures for agencies to adopt policy enforcement points.[39]

Programming, Planning, Budgeting, and Execution

Programming, planning, budgeting, and execution (PPBE) is a process agencies follow for resource allocation. Agencies considering a VPN to ZTNA transition might use this process as a framework to accomplish their goals. This may include a phased approach that factors in the following.

- **Assessment:** Inventory all existing VPN deployments, and identify applications as well as user populations, to include specific user roles. It also may be necessary to catalog legacy systems that may not support modern authentication protocols to ensure that the requirements of a ZTNA system do not preclude access to a critical agency resource. The assessment need not be exclusively technical. Reviewing applicable policies may force agencies to adopt a certain course of action over another.
- **Parallel deployment:** Deploy ZTNA alongside existing VPN infrastructure, beginning with lower-risk applications and user groups. Both systems may operate concurrently during the transition. This would allow the agency to gain experience with the new tools, optimize their network and architecture for deployment, test the system, and discover lessons for broader implementation.
- **Progressive migration:** Move applications to ZTNA individually, starting with cloud-native workloads and high-security assets, while also maintaining VPN as a fallback. This transition period may be burdensome for end-users and administrators as they manage both systems.
- **VPN decommissioning**: Once all applications and users have been migrated and validated, decommission VPN infrastructure.

Additionally, the cost for migrating to ZTNA may present challenges for agency budgeting. VPN costs are primarily capital expenditures (e.g., hardware appliances and user licenses); ZTNA shifts costs to an operational expenditure model (i.e., per-user software-as-a-service subscriptions). This introduces reoccurring cost for agencies that have traditionally kept remote

[37] Office of Management and Budget, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," *OMB M-22-09*, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[38] It does not appear that the Executive Office of the President, or the Government Accountability Office has performed a government-wide survey of ZTA adoption. GAO did review the ZTA work of the U.S. Secret Service (https://www.gao.gov/assets/gao-23-105466.pdf), but it is unclear if the recommendations made there are broadly applicable to the entirety of the federal civilian executive branch agencies.

[39] CISA, "Trusted Internet Connections (TIC) 3.0 Core Guidance Documents," website, December 26.2023, https://www.cisa.gov/resources-tools/resources/trusted-internet-connections-tic-30-core-guidance-documents.

network access costs fixed. Agencies may have to determine if the total cost of ZTNA reduces risk in an acceptable way (or if keeping a VPN increases unacceptable risks). The total cost of ownership of one solution may also need to account for inadvertent costs created during incident response.

Technical Limitations

While agencies are considering which remote access solutions to pursue, they must also consider how those solutions would comply with the agency's post-quantum cryptography (PQC) requirements.[40] Agencies may be hesitant to transition to a ZTNA provider, if that provider does not also support PQC protocols to which the agency is also subject.

NIST approves cryptographic standards for agency use.[41] Some remote access solutions may not use approved NIST cryptographic standards, or they may use NIST-approved standards for a portion of their chain to establish a secure connection (e.g., symmetric key exchange) but not another (e.g., key negotiation). NIST uses a deliberate process to review and approve cryptographic standards for federal agencies.[42] Notably, NIST only approves algorithms and protocols, which precludes an approval for a profile built atop a cryptographic algorithm or protocol. Some cryptographic products use these profiles (e.g., the Noise Protocol Framework, based on Diffie-Hellman key exchange), as such approval of the profiles is outside the scope of NIST's standards work.[43]

In addition to broad NIST standards, federal agencies have specific standards. Federal Information Processing Standards (FIPS) are standards applicable to all federal agencies.[44] FIPS 140-3 describes the cryptographic modules federal agencies are allowed to operate (or have a vendor operate on their behalf).[45] FIPS 197 designates the Advanced Encryption Standard (AES) as the block cipher federal agencies must use to assure the confidentiality of data. This standard allows for cryptographic keys of 128-, 192-, and 256-bit lengths.[46] FIPS 203 specifies Module-Lattice (ML) as the key encapsulation mechanism (KEM) federal agencies are to use to establish a shared secret key over public communications channels. It also sets the parameters that federal agencies are to use for ML-KEM. As of the publishing of the standards, AES-256 and ML-KEM are believed to be secure against quantum computing threats.[47]

Given the cloud-based nature of ZTNA solutions, a federal agency seeking to use those products would also need to ensure that the products are FedRAMP approved.[48] Some commercial solutions, (e.g., Zscaler) do have products approved on the FedRAMP marketplace.[49] Zscaler claims that 14 Cabinet-level

[40] For more information, see https://www.crs.gov/Reports/IN11921.

[41] 15 U.S.C. 278g-3. For a list of approved standards and guidance, see https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines.

[42] Cryptographic Technology Group, "NIST Cryptographic Standards and Guidelines Development Process," *NISTIR 7977*, March 2016, https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7977.pdf.

[43] Trevor Perrin, "The Noise Protocol Framework," July 11, 2018, https://noiseprotocol.org/noise.html.

[44] 15 U.S.C. §278g-3.

[45] NIST, "Security Requirements for Cryptographic Modules," *FIPS PUB 140-3*, March 22, 2019, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf.

[46] NIST, "Advanced Encryption Standard (AES), *FIPS 197*, May 9, 2023, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf.

[47] NIST, "Module-Lattice-Based Key-Encapsulation Mechanism Standard," *FIPS 203,* August 13, 2024, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf

[48] For further information, see https://www.fedramp.gov/docs/authority/.

[49] For an example, see https://marketplace.fedramp.gov/products/FR1719759604.

agencies are using their ZTNA products.[50] CRS was unable to determine the extent to which agencies have implemented these products.

[50] Zscaler, "Efficiency in Government Delivered with Zero Trust," white paper, 2025, https://govciomedia.com/wp-content/uploads/2025/05/government-efficiency-delivered-with-zscalers-zero-trust-network-architect-ztna.pdf.