

Date: September 15, 2026

PR Number: 20153637

1. Agency and Contracting Activity.

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP), Office of Acquisition (OA), Information Technology Contracting Division, and the Office of Information and Technology, Enterprise Infrastructure and Operations Directorate (EIOD), Network Architecture & Engineering Division (NAED), prepared this brand name Justification for Exception to Fair Opportunity.

2. Nature and/or description of the action being approved.

CBP intends to solicit brand-name specifications among holders of Cisco, Meraki, Palo Alto, and IBM stock keeping units (SKUs) and selective annual maintenance, for the FY26 Network Equipment Buy requirement.

CBP requires that brand name delivery orders be awarded for the procurement of Infrastructure Network Equipment and associated licensing. Fair opportunity will be limited to contract awardees under the NASA SEWP indefinite delivery/indefinite quantity (IDIQ), Small Business socio-economic category, who are authorized resellers of Cisco, Meraki, Palo Alto, and IBM products or who have a business relationship with authorized resellers that permit them to provide the required products.

3. A description of the supplies or services required to meet the agency's needs (including the estimated value and the period of performance).

This procurement is for infrastructure network equipment (switches, routers, and other networked hardware) required to implement equipment upgrades at multiple CBP sites throughout the United States. This package is an assortment of equipment required from various manufacturers.

The acquisition will also include any required manufacturer support, software maintenance, licensing, and lifecycle replacement components necessary to ensure the equipment remains operational, secure, and compliant with DHS and CBP technical standards.

CBP's minimum requirements are for network equipment and related support that:

- **Meets CBP enterprise network standards** and is compatible with the existing CBP network architecture, management tools, and security requirements.
- **Maintains operational continuity** for mission-critical CBP systems and facilities, including environments that require high availability, resiliency, and reliable network performance.

¹ In this document, citations to RFO Part 16 are citations specifically to Federal Acquisition Regulation (FAR) Class Deviation 26-04 R1 for FAR Part 16, which was issued as part of the Revolutionary FAR Overhaul (RFO), which was implemented in response to Executive Order 14275, *Restoring Common Sense to Federal Procurement*, signed April 15, 2025.

U.S. Customs and Border Protection
Justification for Exception to Fair Opportunity (JEFO)
[REDACTED] – RFO 16.507-7

- **Supports secure communications** consistent with applicable DHS and CBP cybersecurity, configuration, and supply chain risk management requirements.
- **Provides sufficient capacity, performance, and scalability** to support current and anticipated network traffic, mission applications, users, devices, and connected facilities.
- **Includes required licensing, subscriptions, maintenance, warranty, and technical support** to ensure continued operation, vendor supportability, and timely remediation of defects or vulnerabilities.
- **Supports lifecycle replacement and modernization needs** by replacing aging, unsupported, or end-of-life network equipment that may pose operational, security, or maintenance risks.
- **Can be delivered and supported within the required timeframe** to avoid mission impact, service degradation, or delays to planned network modernization and sustainment activities.
- **Integration with Current Systems, Network Architecture, and Standards**
- **PQC Requirements include:**
 - Multi-plane PQC integration
 - ML-KEM-based quantum-safe handshakes
 - RFC-8784 PPKs with BYOK
 - PQC-enabled secure boot/signing/attestation
 - Software-defined cryptographic algorithm selection
 - Ability to update algorithms through IOS XE, IOS XR, NX-OS, or controller updates
 - Centralized policy control through Cisco management platforms
 - Certificate and key lifecycle management
 - Hardware support sufficient for larger PQC keys and signatures
 - Support for future FIPS-validated cryptographic modules
- Network headend, routers, and switches that support Dynamic Multipoint Virtual Private Network, DMVPN, and Software-Defined Wide Area Network, SD-WAN Viptela environment
- Wireless Access Points (WAPs) that are National Institute of Standards and Technology (NIST)-standardized PQC algorithms and compliant
- IBM Power E1080 or newer compliant model to be integrated with current IBM system

This includes the costs associated with the purchase of hardware equipment along with twelve (12) months of maintenance for non-Cisco items as seen in the Bill of Material (BOM). The required network infrastructure equipment will ensure that all system equipment connected to the DHS/CBP Network Enterprise meets all security regulations and standards.

The total estimated price is [REDACTED].

¹ In this document, citations to RFO Part 16 are citations specifically to Federal Acquisition Regulation (FAR) Class Deviation 26-04 R1 for FAR Part 16, which was issued as part of the Revolutionary FAR Overhaul (RFO), which was implemented in response to Executive Order 14275, *Restoring Common Sense to Federal Procurement*, signed April 15, 2025.

4. Identify the exception to fair opportunity and provide supporting rationale, including a demonstration that the proposed contractor's unique qualifications or the nature of the acquisition requires use of the exception cited.

 X RFO 16.507-7. Brand-name justification for items peculiar to one manufacturer.

Rationale:

This procurement is in accordance with FAR 16.507-7 (FAR Class Deviation Number 26-04). The exceptions at FAR 16.507-6(b) (FAR Class Deviation Number 26-04) do not apply, as this is brand-name justification. However, the justification format at FAR 16.507-6(d)-(e) (FAR Class Deviation Number 26-04) applies and is modified to reflect brand-name justification. This procurement supports the acquisition of critical network infrastructure equipment, including switches, routers, and networked hardware including associated software, necessary to modernize and upgrade network capabilities at multiple CBP sites throughout the United States. These upgrades are required to maintain secure, reliable, and resilient connectivity across CBP operational environments and to support the uninterrupted execution of CBP's border security, trade enforcement, and law enforcement missions.

The package consists of equipment from multiple manufacturers that, collectively, are required to meet CBP's technical, operational, and cybersecurity requirements. The acquisition includes the items as identified in the BOM, to ensure continued vendor support, security updates, and operational sustainment during the initial period of performance.

Upgrading this infrastructure is essential to protecting the DHS/CBP Network Enterprise from cybersecurity risks, equipment obsolescence, and potential service disruptions. The required equipment will help ensure that systems connected to the DHS/CBP enterprise network comply with applicable federal, DHS, and CBP security regulations, policies, and technical standards. By strengthening the security and performance of CBP's network infrastructure, this procurement directly supports mission continuity, safeguards sensitive government information, and enhances CBP's ability to carry out its national security responsibilities.

Cisco

CBP requires network infrastructure equipment to include headend, routers, and switches that can securely integrate with, sustain, and modernize the existing CBP enterprise network environment. The requirement directly supports CBP's national security mission by maintaining secure and resilient connectivity across operational sites, ports of entry, data centers, and other mission-critical locations within the United States and abroad. Because CBP's current enterprise network architecture is built around Cisco routing, switching, security, management, and analytics platforms, the required equipment must be fully interoperable with the existing CBP network baseline to avoid unacceptable cybersecurity, operational, cost, and schedule risks.

¹ In this document, citations to RFO Part 16 are citations specifically to Federal Acquisition Regulation (FAR) Class Deviation 26-04 R1 for FAR Part 16, which was issued as part of the Revolutionary FAR Overhaul (RFO), which was implemented in response to Executive Order 14275, *Restoring Common Sense to Federal Procurement*, signed April 15, 2025.

Cisco routers are required because they are the only routers identified through CBP's technical review that can fully interconnect and operate with CBP's existing Cisco-based Dynamic Multipoint Virtual Private Network, DMVPN, and Cisco Software-Defined Wide Area Network, SD-WAN Viptela environment. These capabilities are foundational to CBP's wide-area network operations and support secure communications across geographically dispersed CBP locations. Introducing a non-Cisco routing platform would require substantial redesign, testing, implementation, and sustainment changes across CBP's field site architecture, increasing the risk of service disruption to mission operations.

Although other manufacturers provide VPN or SD-WAN solutions, those products are not direct substitutes for the existing DMVPN and Viptela deployment. Introducing another manufacturer's solution would require new architecture, migration planning, reconfiguration of routing and security policies, replacement or redesigning of existing tunnels and overlays, new management tools, additional testing, retraining of support personnel, and possible changes to connected network services. These changes would increase cost, schedule, cybersecurity risk, operational disruption, and would take more than five years to transition and cost [REDACTED]

Currently the CBP Network is not fully PQC capable, Executive Order 14306, titled "*Securing the Nation Against Advanced Cryptographic Attacks*," signed on June 22, 2026, making this a federal requirement for full implementation of PQC for encryption by 2030. For the PQC requirements CBP considered vendors on the Technical Reference Model (TRM) to include Cisco, Juniper, Arista, and Extreme networks device. Cisco was chosen because it was the only manufacturer on the TRM that meets all requirements.

Cisco products are the only option since they have interoperability and are fully compatible with CBP's existing enterprise network management, access control, and security monitoring tools. These tools include Catalyst Center, formerly DNA Center, which CBP uses for network configuration and analytics; Cisco Identity Services Engine, ISE, which CBP uses for Network Access Control, NAC, and Terminal Access Controller Access Control System, TACACS, functions; and Cisco Secure Network Analytics, formerly Stealthwatch, which supports CBP Security Operations Center, SOC, visibility and monitoring. To transition to an alternate product line other than Cisco would require an investment of [REDACTED] and a redesign of the CBP network, neither of which is viable.

Meraki

When testing Meraki WAP models were found to be the only manufacturer that supports NIST-standardized PQC algorithms and compliance. Meraki's current integration with the broader Cisco ecosystem is a critical factor for CBP. CBP's enterprise network already relies extensively

¹ In this document, citations to RFO Part 16 are citations specifically to Federal Acquisition Regulation (FAR) Class Deviation 26-04 R1 for FAR Part 16, which was issued as part of the Revolutionary FAR Overhaul (RFO), which was implemented in response to Executive Order 14275, *Restoring Common Sense to Federal Procurement*, signed April 15, 2025.

U.S. Customs and Border Protection
Justification for Exception to Fair Opportunity (JEFO)
[REDACTED] – RFO 16.507-7

on Cisco infrastructure, including Cisco switching, routing, identity, access control, monitoring, and security tools. Meraki wireless access points are designed to integrate with Cisco network and security capabilities, including identity-based access controls, segmentation, monitoring, and centralized administration. This integration supports secure access to the DHS/CBP network enterprise and ensures that wireless devices are managed in accordance with applicable federal, DHS, and CBP cybersecurity requirements.

Based on market research, Cisco Meraki is the only solution that meets CBP's requirements for architectural compatibility, operational experience, U.S.-based support, and PQC-compliant enterprise wireless security.

Palo Alto

Palo Alto Networks is the required solution for CBP because it provides the compatibility, continuity, and operational alignment necessary to expand existing cybersecurity functionality without introducing risk. The currently deployed Palo Alto Cortex XSOAR (Security Orchestration, Automation, and Response) is a specialized software and hardware solution designed to orchestrate security workflows. You cannot "upgrade" the XSOAR engine by introducing another manufacturer's product because XSOAR is a proprietary platform. Replacing or augmenting the core engine with a different manufacturer's product would constitute a "rip and replace" migration rather than an upgrade and would cost [REDACTED] [REDACTED] require more than two years to purchase and replace, and degrade network security and operations while development, design, and implementation of a new system occurred.

Upgrading or replacing a core security orchestrator is a high-risk operation and would impact operation continuity and introduce unnecessary risks.

- **Security Gaps:** During a transition to a different manufacturer, there would be a risk of "blind spots" where security alerts are not processed or automated responses fail to trigger. This would leave the network vulnerable to an **alien** or unauthorized actor attempting to exploit the transition period.
- **Complexity:** Managing two different SOAR platforms simultaneously is operationally unsustainable. It would require the security team to maintain two separate sets of expertise, two separate automation libraries, and two separate incident response processes.

The current CBP deployment of the Palo Alto Cortex XSOAR platform was identified as the only solutions capable of providing a Security Orchestration, Automation, and Response capability to improve incident response times and operational efficiencies without requiring CBP to dedicate additional full-time resources solely for this function. XSOAR provides vendor-agnostic orchestration and integration capabilities that allow CBP to automate workflows across multiple security and network technologies. This capability is essential to CBP because XSOAR

¹ In this document, citations to RFO Part 16 are citations specifically to Federal Acquisition Regulation (FAR) Class Deviation 26-04 R1 for FAR Part 16, which was issued as part of the Revolutionary FAR Overhaul (RFO), which was implemented in response to Executive Order 14275, *Restoring Common Sense to Federal Procurement*, signed April 15, 2025.

was selected to provide the integration between Palo Alto GlobalProtect VPN and Infoblox DNS in order to resolve hostnames for GlobalProtect VPN clients and provide DNS resolution for users accessing CBP mainframe applications.

This XSOAR capability is unique and mission-critical to CBP's current environment. Without the integration provided by XSOAR, VPN users using the GlobalProtect client would be unable to access required CBP mainframe applications. These applications support critical CBP business, law enforcement, border security, trade, travel, and homeland security functions. Any loss of access to these systems could negatively affect CBP's operational readiness, continuity of operations, and ability to execute mission-essential responsibilities.

As part of the testing and evaluation it was determined that several manufacturers provide next-generation firewall, VPN, and security orchestration capabilities, including Cisco, Fortinet, Check Point, Juniper, Zscaler, Microsoft, IBM, Splunk, and Swimlane. These products are not compatible with CBP's existing Palo Alto infrastructure, including the Palo Alto 7500 Firewall, GlobalProtect VPN, Cortex XSOAR workflows, and related software currently deployed within CBP's network without significant investment in network redesigning and new hardware costs.

Palo Alto is the only solution for this requirement because it preserves compatibility with existing CBP hardware and software, maintains continuity of cybersecurity operations, supports existing XSOAR automation workflows, enables GlobalProtect VPN and Infoblox DNS integration, and helps ensure continued access to CBP mainframe applications.

IBM

CBP's current IBM Power server infrastructure is processing over 11 billion trade and tariff transactions daily, significantly exceeding its rated capacity of approximately 6 billion. This volume discrepancy is causing nationwide processing delays. To address the nationwide processing delays caused by transaction volumes exceeding our 6 billion capacities, CBP must expand its infrastructure. The IBM Power E1080 is the only solution capable of meeting this demand while ensuring operational continuity.

Because the E1080 is purpose-built for the IBM Power ecosystem, it integrates directly into our existing environment without requiring costly and disruptive architectural redesign. By maintaining full compatibility with our established IBM-specific processor architecture, firmware, virtualization, operating system support, and partitioning, the E1080 ensures seamless interoperability. Furthermore, this solution preserves our existing investments in management interfaces, high-availability configurations, licensing, monitoring tools, and maintenance procedures, allowing for an immediate increase in capacity without the need to replace our current infrastructure. Market research confirms that non-IBM server solutions cannot provide the necessary integration or functional equivalence required for CBP's existing IBM-specific infrastructure. The IBM Power E1080 is essential to support, maintain, and scale the current environment.

¹ In this document, citations to RFO Part 16 are citations specifically to Federal Acquisition Regulation (FAR) Class Deviation 26-04 R1 for FAR Part 16, which was issued as part of the Revolutionary FAR Overhaul (RFO), which was implemented in response to Executive Order 14275, *Restoring Common Sense to Federal Procurement*, signed April 15, 2025.

Non-IBM hardware lacks the proprietary architecture required to interface with our existing firmware, virtualization, and management tools, rendering the current software stack and partitioning configurations unusable. Replacing the current environment with non-IBM equipment would necessitate a complete architectural redesign, resulting in prolonged system downtime and a significant interruption to critical trade and tariff processing. This introduces unacceptable risks to system stability and continuity of operations. Without the seamless integration provided by the E1080, CBP would be unable to scale capacity to meet the current 11 billion daily transaction volume, leading to persistent, nationwide delays in trade processing. Because other manufacturers cannot provide the specific IBM-proprietary components required for our environment, only IBM or its authorized resellers can provide the equipment necessary to meet the Government's requirements. network architecture while meeting operational availability, compatibility, and sustainability requirements.

5. Determination by the contracting officer that the anticipated cost to the Government will be fair and reasonable.

The Contracting Officer has determined that the anticipated prices will be fair and reasonable based on adequate price competition among the NASA SEWP V small business vendors. NASA SEWP V is a Best-in-Class, category management-approved strategic sourcing vehicle to acquire commercially available IT commodities to support DHS business units in accomplishing their assigned missions. The Contracting Officer will use various price analysis techniques to determine a fair and reasonable price, including a comparison of proposed prices received and a comparison to the Independent Government Cost Estimate.

6. Any other facts supporting the justification.

None.

7. A statement of the actions, if any, the agency may take to remove or overcome any barriers that led to the exception to fair opportunity before any subsequent acquisition for the supplies or services is made.

CBP will continue to conduct market research to determine if the market has changed and if a better solution becomes available.

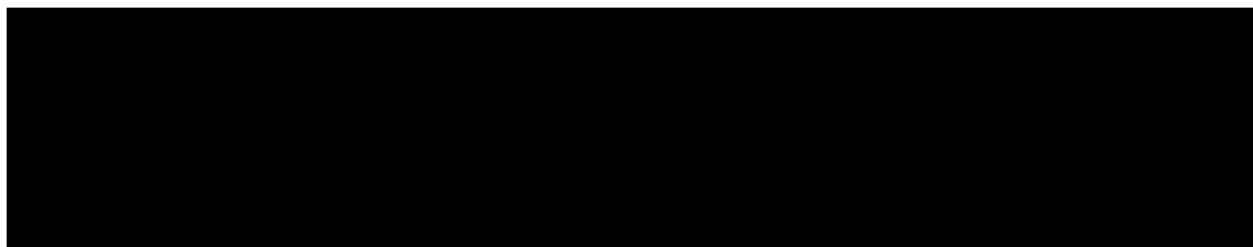
8. CBP intends to post this justification on www.sam.gov pursuant to RFO 16.507-6(f).

¹ In this document, citations to RFO Part 16 are citations specifically to Federal Acquisition Regulation (FAR) Class Deviation 26-04 R1 for FAR Part 16, which was issued as part of the Revolutionary FAR Overhaul (RFO), which was implemented in response to Executive Order 14275, *Restoring Common Sense to Federal Procurement*, signed April 15, 2025.

U.S. Customs and Border Protection
Justification for Exception to Fair Opportunity (JEFO)
[REDACTED] – RFO 16.507-7

9. Technical/Requirements Personnel Certification:

Pursuant to RFO 16.507-6(d)(2)(ix), I certify that this requirement meets the Government's minimum need and that the supporting data, which form a basis for the justification, are accurate and complete.



10. Contracting Officer Certification and Approval:

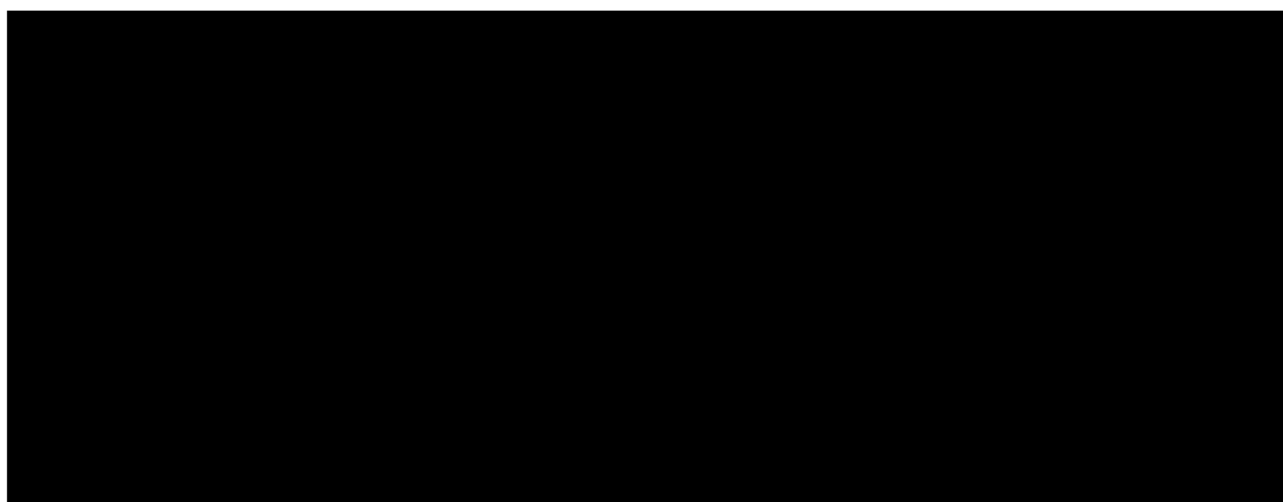
Pursuant to RFO 16.507-6(e)(1), I certify that this justification is accurate and complete to the best of my knowledge and belief and hereby determine that the circumstances for an exception to fair opportunity exist and legal review was obtained when required based on dollar value.

JOHN D
MARSCHALL

Digitally signed by
JOHN D MARSCHALL
Date: 2026.09.18
07:40:31 -04'00'

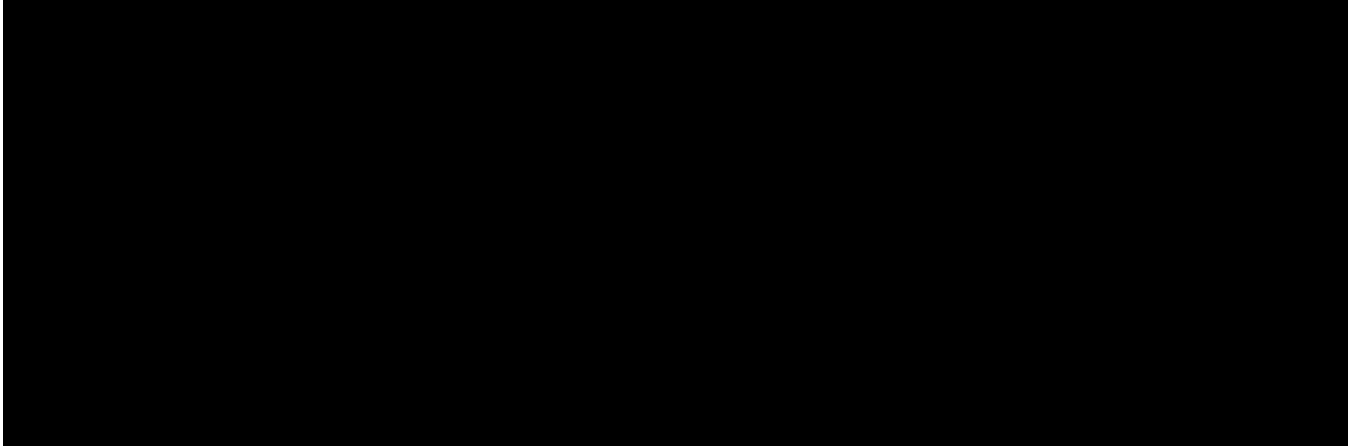
John Marschall
Contracting Officer

Date



¹ In this document, citations to RFO Part 16 are citations specifically to Federal Acquisition Regulation (FAR) Class Deviation 26-04 R1 for FAR Part 16, which was issued as part of the Revolutionary FAR Overhaul (RFO), which was implemented in response to Executive Order 14275, *Restoring Common Sense to Federal Procurement*, signed April 15, 2025.

U.S. Customs and Border Protection
Justification for Exception to Fair Opportunity (JEFO)
[REDACTED] – RFO 16.507-7



¹ In this document, citations to RFO Part 16 are citations specifically to Federal Acquisition Regulation (FAR) Class Deviation 26-04 R1 for FAR Part 16, which was issued as part of the Revolutionary FAR Overhaul (RFO), which was implemented in response to Executive Order 14275, *Restoring Common Sense to Federal Procurement*, signed April 15, 2025.