

Attachment 4
U.S. Customs and Border Protection
Justification for Exception to Fair Opportunity (JEFO)
[REDACTED] – RFO 16.507-6

Date: 8/26/2026

PR Number: 20153373

1. Agency and Contracting Activity.

The U.S. Department of Homeland Security, U.S. Customs and Border Protection, Office of Acquisition, prepared this Justification for an Exception to Fair Opportunity for the acquisition of the ThreatLocker Zero Trust Platform.

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

CBP intends to solicit a requirement using brand-name specifications among holders of the NASA SEWP V multiple-award indefinite-delivery, indefinite-quantity contract. Pursuant to RFO 16.507-7, restricting consideration to the ThreatLocker Zero Trust Platform is justified as the product is peculiar to one manufacturer.

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

CBP requires 95,000 licenses for the ThreatLocker Zero Trust Platform (AllowListing, Ringfencing, Elevation Control, Network and Storage Control, ThreatLocker Detect (EDR), Patch Management and Configuration Management) and associated maintenance and support. The solution will be deployed on-premises within the CBP secure environment. The platform will be managed exclusively by internal CBP personnel and cleared SOC services contractors. No vendor access, remote connectivity, or cloud-based management is permitted or required.

The total estimated value is [REDACTED] for a 12-month period of performance.

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.

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 a 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.

Rationale:

The ThreatLocker Zero Trust Platform provides an essentially unique integrated "default-deny" architecture that can be deployed in a fully air-gapped, on-premises environment. Unlike other security tools that require external cloud connectivity or vendor-managed portals, ThreatLocker allows CBP to maintain full data sovereignty and operational control. This is a mandatory requirement for our secure, closed-network segments where external cloud dependencies are

Attachment 4
U.S. Customs and Border Protection
Justification for Exception to Fair Opportunity (JEFO)
[REDACTED] – RFO 16.507-6

prohibited. ThreatLocker's ability to block unauthorized software execution by default, while providing a streamlined "Request Access" workflow for end-users, is a unique capability that cannot currently be replicated by disparate security tools. Other companies' similar products, such as CrowdStrike or other EDR type solutions, do not and currently cannot be modified to meet the agency's needs.

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

The Contracting Officer will determine that the anticipated cost is fair and reasonable using price analysis techniques via FAR 15.404-1, including competition among NASA SEWP V contract holders, comparison against the Independent Government Cost Estimate (IGCE), and review of the manufacturer's published commercial price list for software licenses.

6. Any other facts supporting the justification.

- **Operational Security and Data Sovereignty:** By deploying ThreatLocker on-premises, CBP eliminates supply-chain risks associated with other SaaS-based tools. The platform is managed entirely by internal engineering teams, ensuring no sensitive enforcement data or system telemetry leaves the CBP-controlled environment.
- **Alignment with Federal Cybersecurity Mandates:** ThreatLocker provides the technical enforcement required to demonstrate compliance with Executive Order 14028 and OMB M-09 within a closed-network architecture.
- **Proactive Defense:** ThreatLocker is engineered to prevent the execution of malicious code before it can compromise the system, which is critical for protecting PII and CUI related to border enforcement operations.

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.

The agency will conduct continuous market research and periodic re-evaluations of the endpoint security market. Should market research indicate that other vendors have achieved technological parity for on-premises, air-gapped Zero Trust enforcement, the agency will update its requirements to enable a competitive procurement process for future acquisitions.

8. CBP intends to post this justification on www.sam.gov pursuant to RFO 16.507-7(c)(1).

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. ■

[REDACTED]

Attachment 4
U.S. Customs and Border Protection
Justification for Exception to Fair Opportunity (JEFO)
[REDACTED] – RFO 16.507-6

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.

MARY W
CARSON

 Digitally signed by MARY W
CARSON
Date: 2026.08.19 12:39:31 -04'00'

Contracting Officer

8/19/26
Date

