



Global Acquisitions

U.S. DEPARTMENT *of* STATE

JUSTIFICATION FOR EXCEPTION TO FAIR OPPORTUNITY

SECTION 1: IDENTIFICATION OF THE AGENCY AND THE CONTRACTING ACTIVITY

Department of State Contracting Activity

☒ Acquisition Management

Requiring Activity

Bureau of Intelligence & Research Technology & Innovation Office (INR/TIO)

SECTION 2: NATURE AND/OR DESCRIPTION OF THE ACTION BEING APPROVED

Approval is requested to solicit and award a new Task Order under NASA SEWP using a Firm Fixed Price (FFP) contract type. The Task Order will be subject to exception to fair opportunity limiting competition to authorized resellers of Corelight, Inc., 548 Market St, PMB 77799, San Francisco, CA 94104-5401 brand-name software and/or services described in Section 3 on behalf of the Requiring Activity.

SECTION 3: DESCRIPTION OF SUPPLIES/SERVICES REQUIRED TO MEET THE AGENCY'S NEEDS

The Bureau of Intelligence and Research (INR) requires specialized commercial services to enhance and maintain the Cross Domain Solution (CDS) for the Department of State. A CDS is a specialized hardware and software system that controls and sanitizes the transfer of sensitive data between networks of different security classifications. Because these systems guard the boundaries of critical national security enclaves, they are subject to strict federal regulations and rigorous oversight. Consequently, any deployed CDS must pass extensive lab-based testing to meet the evolving "Raise the Bar" (RTB) standards developed by the National Security Agency (NSA). This procurement focuses on acquiring NSA RTB compliant hardware and software to monitor the CDS.

INR's minimum requirements for CDS monitoring are:

- NSA RTB compliant passive inspection of all traffic traversing CDS boundaries.
- Integration with existing enterprise detection analytics, detection engineering, and SOC workflows, which consume Corelight-specific Zeek metadata.

Accordingly, INR will procure:

- Proprietary CoreOS & Hardware Acceleration: VMware virtual appliance sensor and bundle subscription license featuring open-source security tools Zeek, Suricata, SPCAP, YARA, Threat Intelligence, ET Pro, and Fleet for 1 Gbps of capacity.
- Proprietary Appliance Customization Services: Professional services to configure and optimize the Corelight appliance to continuously monitor enterprise network traffic, generate high-fidelity network metadata, detect malicious activity, support threat hunting, and enable rapid incident investigation and response.
- Training and U.S. based support: Expert support with intensive training for personnel using Corelight Inc. product and 24/7 technical assistance and direct access to cybersecurity experts well-versed in strict NSA regulations.

The estimated value for the 12-month period of performance for CoreOS & Hardware Acceleration, associated appliance customization services, training, and USA based support is .

SECTION 4: IDENTIFICATION OF THE EXCEPTION TO FAIR OPPORTUNITY AND THE SUPPORTING RATIONALE

This acquisition is conducted pursuant to 41 U.S.C. 4103 and 4106 as implemented by FAR 16.507-6 and substantiated by the following:

☒ FAR 16.507-7 – Items peculiar to one manufacturer.

The specific brand-name, product, or feature is essential to the INR's requirements and Market research indicates that there are sufficient resellers capable of providing the Corelight brand name.

Department of State's existing cyber network defense (CND) architecture relies on an established, high-assurance network enclaving and visibility framework that uses both the Zeek software package and the Suricata software package to be compliant with NSA's RTB standard. Corelight solution bundles Zeek and Suricata into a single software package to achieve compliance with RTB.

Procuring an alternative NDR platform presents substantial cost, technical complexity, and risk. The Department has invested significant resources developing the existing enterprise detection content, correlation rules, dashboards, incident response playbooks, analyst training, and

historical baselines that depend upon Corelight-generated Zeek metadata. Migration to an alternate platform would require redevelopment, testing, validation, and operational transition of these capabilities, resulting in substantial duplication of Government cost and increased operational risk that would not be recovered through competition.

Furthermore, not all vendors or products are RTB compliant. RTB compliance requires NSA approval for specific software versions and configurations. Acquisitions must explicitly verify that the specific brand, model, and version being procured are currently approved by NSA. The specific Corelight product version being acquired has been assessed and approved by NSA for deployment in accordance with RTB standards.

INR evaluated Cisco Secure Network Analytics, ExtraHop Reveal(x), Darktrace, Vectra AI, Elastic Packetbeat, Security Onion, and native Zeek deployments. Corelight is the only company that develops and manufactures a Zeek-Suricata software bundle that meets NSA RTB standards.

Based on this research, Corelight is the only solution that seamlessly integrates with the existing solution through a closed-source operating system, proprietary behavioral analytics, encrypted traffic analysis, and threat-hunting signatures. Corelight's proprietary Smart PCAP indexing and optimized Zeek integration produce metadata that can be directly consumed by existing INR SOC analytics. Competing solutions cannot generate identical metadata without redesigning detection content.

Market research included a review of Corelight technical documentation, GSA and SEWP product listings, vendor capability statements, and publicly available product documentation. Specifically, the NASA SEWP Market Research Tool was used to perform a preliminary search using the criteria of “Corelight” as the Provider. There were 79 contractors with Corelight products on SEWP catalog, of which 65 were small businesses.

		
Click to Show/Hide details of availability by Contract Holder >>		
		
Group A		Groups B, C, D
8 (4 SB)		79 (65 SB)

Then based on the initial query results, a sub-search by Corelight part numbers was initiated using four (4) product samplings. The output showed between 10 to 45 small businesses with these products already on their SEWP catalog; the details are displayed on the next page:

Product Requests from Various Providers	Group A	Groups B,C,D
	Availability Varies	
SBSS-XAPPLSURI-1G-1Y	Group A 2 (2 SB)	Groups B,C,D 30 (26 SB)
SBSS-FEED-ETP-1G-1Y	Group A 5 (2 SB)	Groups B,C,D 56 (45 SB)
SBSS-XAPPLSPCAP-1G-1Y	Group A 0	Groups B,C,D 11 (10 SB)
FLMGMT-1G-1Y	Group A 4 (2 SB)	Groups B,C,D 34 (28 SB)

Thereafter and based on the overall market research findings, formal Request for Information #387963 was published on the SEWP portal to 127 contract holders in Groups B, C, and D. The bulleted list below shows the nine (9) Contractor Holders who responded to the RFI along with their socio-economic classification:

1. Dynamic Systems, Inc.; Woman-owned small business
2. Federal Resources Corporation; Small business
3. GovSmart, Inc.; HUBZone
4. New Tech Solutions, Inc.; Small business
5. Ogis Communication Group, Inc.; Small business
6. Optiv Federal Inc.; Other than small
7. Software Information Resource Corp; Woman-owned small business
8. Standard Blazar, LLC; Small business
9. Sterling Computers Corporation; Other than small

The RFI results demonstrate there is sufficient evidence that the Corelight requirement should be set-aside for small businesses.

SECTION 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 price to the Government is fair and reasonable by evaluating competitive quotes received from authorized Corelight resellers and comparing proposed pricing to the manufacturer's established federal contract price lists (e.g., NASA SEWP). Based on these mechanisms, the Contracting Officer will ensure that the final price of _____ is fair and reasonable prior to award.

SECTION 6. 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.

NR/TIO will:

- Conduct periodic market research to identify emerging NSA-approved CDS monitoring solutions.
- Evaluate future commercial products capable of generating metadata compatible with existing enterprise detection analytics.
- Reassess whether future commercial products satisfy NSA RTB implementation requirements without requiring proprietary Corelight functionality.
- Evaluate whether future migration can be accomplished without substantial redevelopment of Government-owned detection content.
- Reassess the requirement before exercising any option periods or initiating a follow-on acquisition.

INR/TIO expects to obtain a technical data package or develop a performance specification that will support competition for future acquisitions of the same or similar items.