Office of Cyber Monitoring and Operations

Diplomatic Security

U.S. DEPARTMENT *of* STATE

Network Detection & Response (NDR) Modernization

Performance Work Statement (PWS)

Version 0.5

Final

Table of Contents

References

1. DEFINITIONS AND ACRONYMS

- **Contracting Officer (CO)**: A person with authority to enter into, administer, and or terminate contracts and make related determinations and findings on behalf of the government. A CO is the only individual who can legally bind the government.
- **Contracting Officer's representative (COR)**: A representative from the requiring activity appointed in writing by the CO to perform surveillance and to act as liaison to the Contractor. This individual has the authority to provide technical direction to the Contractor if that direction is within the scope of the contract, does not constitute a change, and has no funding implications. This individual does NOT have the authority to change the terms and conditions of the contract.
- **Sprint** - A sprint is a two-week cycle derived from Agile methodology that focuses on completing specific tasks or objectives. Each sprint begins with a planning meeting to define objectives and priorities, followed by a review meeting to assess progress and plan next steps. The goal is to ensure continuous development and improvement of deliverables.

2. GENERAL REQUIREMENTS

2.1. Introduction

The Office of Cyber Monitoring and Operations (DS/CTS/CMO) is enhancing the Department of State's cyber defense capabilities to address sophisticated and persistent network-based threats. To support this mission, the Cyber Operations Division (DS/CTS/CMO/COD) is procuring a Network Detection and Response (NDR) solution that delivers advanced capabilities such as AI-driven traffic analysis, encrypted traffic inspection, east-west visibility, and automated threat detection and response. This acquisition supports CMO's broader efforts to modernize network security monitoring and reduce mean time to detect and respond to threats across enterprise and non-enterprise network environments.

2.2. Background

The U.S. Department of State operates one of the largest global IT enterprises in the federal government, supporting diplomatic operations across approximately 275 overseas posts in 175 countries and 150 domestic locations. The Department's networks support over 125,000 users and include approximately 280,000 nodes and 160,000 managed endpoints. Additionally, the Department maintains 356 FISMA systems deployed across its global infrastructure, including on-premises and managed cloud environments comprising more than 200 cloud instances.

This highly distributed and evolving enterprise spans traditional data centers, commercial and government cloud platforms, and third-party hosted services. Ongoing modernization efforts and

expanding mission requirements continue to increase the complexity of securing Department-wide IT assets.

To address these challenges, the Office of Cyber Monitoring and Operations (DS/CTS/CMO) is enhancing its network security monitoring capabilities. This effort aligns with the Department's Target Security Architecture (TSA) and supports broader Departmental cybersecurity modernization initiatives.

2.3. Objectives

The objective of this procurement is to acquire and deploy a fully operational Network Detection and Response (NDR) solution that significantly enhances the Department of State's ability to detect, investigate, and respond to advanced network-based threats across its globally distributed IT enterprise.

Desired Outcomes

- Reduce mean time to detect and respond (MTTD/MTTR) by 50%.
- Achieve real-time threat visibility and automated response across on-premises and cloud environments.
- Ensure compliance with federal cybersecurity mandates, including EO 14028, FISMA, and FedRAMP High.
- Enable proactive threat hunting through AI-driven analytics and enriched context.

Key Objectives

- Improved Network Visibility: Enable deep inspection of raw network traffic and metadata enrichment to support threat detection, correlation, and forensics.
- Advanced Threat Detection: Leverage ML and behavioral analytics to identify abnormal activity and detect sophisticated adversary tactics, techniques, and procedures (TTPs).
- Cloud and Hybrid Support: Provide seamless coverage across on-premises, hybrid, and government/commercial cloud environments.
- Streamlined Incident Management: Automatically correlate related alerts into logical incidents to reduce alert fatigue and accelerate triage.
- Automated Response Capabilities: Support automated actions such as host isolation, traffic blocking, and orchestration through existing SOAR platforms.
- Enhanced Threat Hunting: Provide AI-assisted tools and contextual datasets to empower proactive investigations by SOC analysts.
- Scalability and Interoperability: Ensure the solution integrates with existing cybersecurity infrastructure and scales to meet enterprise needs.

2.4. Type of Contract

DS/CTS/CMO/COD anticipates the award a combination of a Firm Fixed Price (FFP) and Time-and-Materials (T&M) contract. The initial term of the Contract will be one-year base period from the date of award with one, one-year option period that may be exercised solely at the government's discretion.

2.5. Non-personal and Not Inherently Government Services

It shall be the responsibility of the vendor to manage its employees and to guard against any actions that are of the nature of personal services or give the perception of personal services. If the vendor feels that any actions constitute, or are perceived to constitute, personal services, it shall be the vendor's responsibility to notify the Contracting Officer (CO) immediately. These services shall not be used to perform work of a policy/decision making or management nature (i.e., inherently Governmental functions). All decisions relative to programs supported by the vendor shall be the sole responsibility of the Government.

2.6. Place(s) of Performance

- DOS BIMC, 8101 Odell Rd Beltsville MD, 20705
- DOS ESOC West,1 Denver Federal Center, Building 17, Denver, Colorado 80225
- DOS SA-20, 1801 N Lynn Street Arlington VA, 22209
- As needed physical presence at other government locations within the National Capital Region (NCR).
- Remote work can be authorized, as directed by the Contracting Officer or their Representative.

2.7. Performance Period of Delivery Date

This Task Order is a Period of Performance (POP) from date of award one-year base period from the date of award with one, one-year option period that may be exercised solely at the government's discretion.

- Tentatively 30 September 2025 – 29 September 2026 Base Year
- 30 September 2026 – 29 September 2027 Option Year 1

2.8. Kickoff Meeting

Within 7 days of award the Contractor will host a kick-off meeting with the COR, GTM and relevant stakeholder aimed to align and initiate the process for developing and delivering on tasks and requirements outlined in Section 3 - **Scope of Work**, defining communication and reporting protocols, addressing questions and concerns, and outlining next steps.

2.9. Travel

Any business travel required outside of the Place of Performance must be authorized by the COR.

2.10. Government-Furnished Property/Equipment and/or Services

The Contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary to provide support as defined in this Performance Work Statement (PWS) except for those items specified below as government furnished property and services:

- DOS Personal Identification Card – The COR will work with Contractor to obtain personal identification / network access cards for Contractor's employees.
- Access to Department of State Networks/Systems
- Workspace and utilities shall be provided if applicable.
    - Location: SA-26, 8101 O'Dell Rd. Beltsville, MD 20708
    - Location: SA-20, 1801 N Lynn Street Arlington VA, 22209
    - Location: DOS ESOC West, 1 Denver Federal Center, Building 17, Denver, Colorado 80225

2.10.1. Proprietary Information

In the event that performance of any work under this task order causes the Contractor to gain access to proprietary or confidential information of other firms/Contractors, the Contractor is required to immediately execute a Non-Disclosure Agreements with those firms/Contractors, in order to protect the information from unauthorized use. The Contractor is required to refrain from using any such information for any purposes other than for which it was furnished. The Contractor must immediately provide the CO with a copy of any such agreements with original signatures affixed.

2.10.2. Access Requirements

The Contractor shall require access to Department of State Networks/Systems to perform work under the contract. The COR will oversee such access.

Building access to SA-20, SA-26, and ESOC West will be requested through the Uniform Security Officer.

All Contractor personnel that will work on the NDR project shall have a current security clearance at a minimum of High Risk Public Trust (HRPT).

This is a Sensitive but Unclassified (SBU) contract. Contractor personnel specifically designated by the Contracting Officer's Representative (COR) will be required to have a High Risk Public Trust (HRPT) determination conducted by the Bureau of Diplomatic Security.

Please note, a DD Form 254 will not be issued for a Sensitive But Unclassified contract

2.11. Onboarding Process

The Contractor shall manage the onboarding of its staff for all Contractor personnel who have not yet been onboarded. Onboarding includes steps to obtain a network and email account, complete training, initiate background investigations, and gain physical and logical access, which may include elevated privileges to the necessary development and test environments for the various systems to be enhanced.

A single Contractor Onboarding point of contact (POC) shall be designated by the Contractor that tracks the onboarding status of all Contractor personnel. The Contractor Onboarding POC shall be responsible for accurate and timely submission of all required onboarding paperwork to the COR. The Contractor shall be responsible for tracking the status of all its staff's onboarding activities and report the status at the staff level during onboarding status meetings. The Contractor shall provide, to the COR, an Onboarding Status Report for any staff with outstanding onboarding requests.

The COR will provide onboarding assistance and guidance for onboarding

2.12. Contractor Personnel Staffing and Assignments

(a) In the event that any of the key personnel named in the Contractor's quotation, as accepted by the Government at award, are unable to perform because of death, illness, resignation from the Contractor's employ, dissolution of agreement, or other reasons, the Contractor shall submit within 24 hours to the CO/COR, detailed written explanations of the circumstances necessitating the proposed substitutions, complete resumes for the proposed substitutes, and any other information that the CO/COR deems pertinent to approve the substitution. No substitution is to be made without the prior written approval of the CO/COR. No increases in pricing will be allowed when substitutions are authorized by the Government.

(b) Personnel possessing unique technical specialties (sec. 3.2.4. Personnel Requirements) may be required for certain services related to the acquisition tasks. Such personnel shall have qualifications as required by the applicable tasks and approved by the CO/COR, which are appropriate to the nature of the services that will be provided.

(c) The CO will have the right to effect removals of any Contractor employees, if those employees are deemed not to possess the proper level of competence or abilities (sec. 3.2.4 Personnel Requirements), or otherwise found to be unsuitable for work required. In such cases, the Contractor must promptly submit the names and any other information pertinent to approvals of substitutions if requested.

(d) Failure or delays by the Contractor in providing qualified personnel who meet the stated requirements of this acquisition, may be deemed sufficient reason by the COR to recommend termination for cause to the CO.

The Contractor shall provide the CO with a primary and alternate administrative point of contact (POC) after award. One of these points of contact must be a Contract Executive. The Contractor shall notify your office of any changes in contact information as expeditiously as possible.

2.13. Compliance with IT Security Policies

DOS programs are pursuant to and the Contractor shall complete all work in accordance with the following security regulations, standards, policies, procedures, and guidelines: Contractors are also required to comply with current Federal regulations and guidance found in the:

1. Federal Information Security Management Act of 2002 (FISMA)
2. Omnibus Diplomatic Security and Anti-Terrorism Act of 1986, as amended.
3. President's National Counter Intelligence Strategy
4. Computer Fraud and Abuse Act of 1986
5. Federal Financial Managers' Financial Integrity Act of 1982
6. Privacy Act of 1974
7. Executive Order 14028
8. National Security Telecommunications and Information System Security Instruction (NSTISSP) 5
9. Office of Management and Budget (OMB) Circulars A-123 and A-130 Appendix III
10. National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and Special Publications (SPs)
11. National Information Assurance Certification and Accreditation Process (NIACAP)
12. National Security Agency Information Security Assessment Methodology (ISAM) and NSA 4016
13. 1 Foreign Affairs Manual (FAM) Authority, Responsibility, and Organization
14. FAM 600 Information Security Technology
15. 12 FAH-6 H-540 Automated Information Systems Security
16. 5 FAM 600 Information Technology Systems
17. 5 FAH-5 H-100 Information Technology Systems
18. National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS)
19. NIST 800-Series Special Publications (SP)
20. Office of Management and Budget (OMB) memoranda

Contractors are required to protect information regarding security issues and associated documentation to limit the likelihood that vulnerabilities in operational software are exposed. If new vulnerabilities are identified after the acceptance of COTS software, the Contractor must review and remediate the vulnerabilities and then present the results for Government approval within the timeframes documented in your office's security policies.

2.14. Special Considerations

Government Identification: The vendor needs to have U.S. citizenship and a valid government identification to access work location.

Contract Business Activities: The Vendor and its employees shall conduct ONLY business covered by this contract during periods paid for by the Government and shall NOT conduct any other business on Government premises.

2.15. Order of Precedence

In the event of inconsistencies, between the Contractor's proposal/quote and PWS, the required work specified in this PWS will take precedence over the Contractor's proposal/quote.

3. SCOPE OF WORK

3.1. General Scope

The Office of Cyber Monitoring and Operations (DS/CTS/CMO) within the Bureau of Diplomatic Security manages cybersecurity tools to protect the Department of State's networks and data. This section outlines requirements for delivering a scalable, AI-driven Enterprise Network Detection and Response (NDR) system that integrates seamlessly with existing cybersecurity tools, provides comprehensive threat visibility, and supports proactive threat hunting and incident response. The desired end-state is a solution that reduces alert fatigue, improves triage efficiency, and enhances the Department's ability to mitigate sophisticated adversary techniques."

In addition to addressing the functionality requirements referenced in Section 3.2 and 3.3, proposals must include:

- **Sample Implementation Plan**: A high-level phased plan with diagrams for designing, configuring, implementing, and delivering the NDR Solution.
- **Test Plan**: A sample plan for testing and acceptance of the NDR Solution.
- **Training Plan**: A detailed plan for training Agency staff, broken down by role/persona to specify required training levels.
- **Ongoing Maintenance and Support**: A description of post-implementation support and maintenance after transitioning to operations.

3.2. Requirements

The requirements defined in this section establish the minimum functional, performance, and interoperability capabilities that the proposed Network Detection and Response (NDR) solution

must provide to achieve the desired outcomes. These outcomes include real-time threat detection, automated response capabilities, and compliance with federal cybersecurity mandates. Offerors shall demonstrate how their proposed solution meets or exceeds each capability, with a focus on delivering measurable improvements in threat detection and response efficiency. These requirements support the Department's objective to enhance threat detection, investigation, and response across enterprise and non-enterprise networks, while ensuring integration with existing cybersecurity tools and infrastructure.

The solution shall be scalable to accommodate the Department's global IT environment, including over 280,000 nodes and 200+ cloud instances, and shall operate across on-premises, virtual, hybrid, and cloud-native environments. All requirements in this section are mandatory unless otherwise stated, and Offerors shall clearly demonstrate how their proposed solution meets or exceeds each capability.

Each requirement is assigned a unique identifier (UID) to facilitate traceability and ensure alignment with evaluation criteria, system design, testing, and future performance assessments.

These requirements are evaluated under Factor 1 – Technical Approach and are traceable via Offer submission of a Solution Requirements Matrix.

3.2.1. Technical Requirements

The following technical requirements define the mandatory capabilities of the Network Detection and Response (NDR) solution. These capabilities are essential to support enterprise-wide threat detection, incident response, and security operations across the Department's globally distributed and hybrid IT environment.

Offerors shall ensure that all listed requirements are met in full. Each item is assigned a unique identifier (UID) to support evaluation, traceability, and verification during deployment and testing phases. Solutions must be scalable, support cloud and on-premises environments, and integrate with the Department's existing cybersecurity infrastructure.

UID	Name	Requirement
NDR.1	Local Account Management	Provide local user account management on each deployed NDR device or sensor.
NDR.2	EDR/SOAR Integration	Support integration with EDR solutions, including tipping and queuing into SOAR platforms.
NDR.3	Custom Signature Development	Ability to create and deploy custom detection signatures.
NDR.4	Log Generation	Produce high-fidelity logs for ingestion by downstream analytics and SIEM platforms.
NDR.5	Packet and Flow Analysis	Capture and analyze raw network packets and flow data for threat identification and behavioral analysis.
NDR.6	Incident Aggregation	Group individual alerts into correlated incidents to enhance threat

		triage and investigation efficiency.
NDR.7	Alert Correlation	Detect and aggregate logical security incidents using multiple signals such as host, user, or anomaly patterns.
NDR.8	Automated Response	Facilitate automatic isolation hosts or block network traffic based on detected threats across North-South and East-West paths.
NDR.9	Anomaly Detection	Establish baselines of normal network activity and alert on deviations or suspicious anomalies.
NDR.10	Cloud Network Monitoring	Analyze traffic in IaaS environments, including support for major cloud providers.
NDR.11	Traditional Detection Techniques	Utilize detection methods such as IDP signatures, heuristics, and threshold-based rules.
NDR.12	Manual/Automated Response	Offer real-time analyst-triggered and fully automated responses to malicious activity.
NDR.13	Behavioral Analytics and ML	Employ behavioral models and ML-based analytics to identify advanced threats and anomalies.
NDR.14	Data Normalization and Enrichment	Add contextual metadata to captured data for enhanced analysis.
NDR.15	Automated Incident Response	Allow definition and execution of automated workflows for security events.
NDR.16	Centralized Management	Enable centralized management for deployment of updates, configurations, policies, and use cases.
NDR.17	Application Layer Inspection	Inspect Layer 7 traffic to identify threats in application payloads or malformed protocols.
NDR.18	Real-Time Threat Analysis	Collect and analyze live network traffic for detecting patterns, anomalies, and threats.
NDR.19	Vulnerability Identification	Detect system or configuration weaknesses that could be exploited by attackers.
NDR.20	CSP API Monitoring	Ingest and analyze telemetry from cloud provider APIs for additional threat context.
NDR.21	Traffic Flow Analysis	Monitor and analyze North-South and East-West traffic flows across networks.
NDR.22	Network Forensics	Enable deep incident investigation through historical traffic capture and metadata analysis.
NDR.23	Network Replay	Replay captured sessions for retrospective analysis and threat hunting.
NDR.24	Rule/Threshold-Based Alerts	Alert on security events based on custom rules or thresholds.
NDR.25	ML-Based Baseline Detection	Detect anomalies using machine learning models based on expected behavior.
NDR.26	Hybrid Deployment Support	Support deployment across on-premises, virtual, and cloud environments.
NDR.27	SSL/TLS Decryption	Decrypt encrypted traffic for inspection where authorized.
NDR.28	Signature-Based	Identify threats using updated malware signatures.

	Malware Detection	
NDR.29	Behavioral Malware Detection	Identify unknown malware through behavior analysis.
NDR.30	Command and Control Detection	Identify outbound communications that resemble C2 traffic.
NDR.31	Data Exfiltration Detection	Detect attempts to move sensitive data outside the network.
NDR.32	Encrypted Threat Detection	Identify malicious activity in encrypted traffic, even without full decryption.
NDR.33	Incident Reporting	Generate and export incident summaries to ticketing systems.
NDR.34	Audit Trail and Forensics	Maintain logs and metadata for compliance and investigation.
NDR.35	Compliance Reporting	Support compliance with RMF, FISMA, EO 14028, and OMB M-21-31.

3.2.2. Software Integration Requirements:

The Contractor shall ensure that the proposed NDR solution integrates natively or via supported APIs with the Department of State's existing cybersecurity and IT platforms. At a minimum, the NDR solution shall support integration with the following tools and platforms:

UID	Name	Requirement
NDR.36	**Splunk**	Forward parsed or raw events and log data for centralized analysis and alert correlation.
NDR.37	**Zeek**	Ingest and enrich network metadata from Zeek for behavioral and protocol-level insights.
NDR.38	**Suricata**	Correlate Suricata alert data to support threat detection and validation workflows.
NDR.39	**ServiceNow**	Automatically generate incident tickets and update status fields via bi-directional APIs.
NDR.40	**Palo Alto Networks**	Ingest firewall telemetry and enable automated response actions (e.g., IP blocking).
NDR.41	**Syslog**	Send logs and event data using standard syslog protocols (e.g., RFC 5424, RFC 3164).
NDR.42	**Cribl**	Support integration into log pipelines and enrichment workflows managed via Cribl.
NDR.43	**Microsoft Defender Products**	Integrate with Defender for Endpoint and Defender for Identity for alert sharing and correlation.

3.2.3. Compliance Requirements:

To ensure alignment with federal cybersecurity mandates and Departmental policy, the NDR solution and associated contractor services must meet the compliance requirements outlined in this section. These requirements are intended to safeguard sensitive information, support system accreditation, and ensure adherence to applicable laws, regulations, and executive directives.

At a minimum, the proposed solution shall comply with requirement NDR-44, by being either FedRAMP High authorized or actively undergoing FedRAMP High authorization with a formal submission to the FedRAMP PMO or a sponsoring agency. Solutions under review must demonstrate technical readiness to operate within a FedRAMP High environment.

The solution must be offered by a U.S.-based vendor, using personnel and infrastructure located within the United States.

The contractor shall also support the Department's compliance obligations under applicable federal cybersecurity frameworks, including the Risk Management Framework (RMF), FISMA, Executive Order 14028, and OMB Memorandum M-21-31. This includes the timely provision of required documentation, security artifacts, and direct support for achieving and maintaining an Authority to Operate (ATO) or Authority to Use (ATU).

UID	Name	Requirement
NDR.44	FedRAMP High	The NDR solution shall be either: • FedRAMP High authorized, with current certification issued by the PMO, or • Actively undergoing FedRAMP High authorization, with a formal package submitted to the PMO or a sponsoring agency. The Offeror shall provide verifiable documentation of its status, such as: • A FedRAMP authorization letter or marketplace listing, a sponsor letter confirming JAB or agency review, or a submission confirmation with a System Security Plan (SSP) aligned to FedRAMP High baselines. Solutions still in review must also demonstrate technical readiness to operate within a FedRAMP High environment, including alignment with applicable security controls and architectural requirements.
NDR.45	U.S.-Based Vendor & Services	All services and personnel supporting the NDR solution must be U.S.-based. All infrastructure must be located within the United States.
NDR.46	FIPS Compliance	All cryptographic functions must use FIPS 140-2 or FIPS 140-

		3 validated modules, in accordance with federal standards and Department policy.

3.2.4. Key Personnel Requirements:

The success of the Network Detection and Response (NDR) solution depends not only on the capabilities of the technology, but also on the expertise of the personnel responsible for its implementation, integration, and ongoing support. This section defines the minimum qualifications for contractor personnel who will support the Department throughout the NDR lifecycle, including planning, deployment, configuration, tuning, training, and maintenance.

Each labor category includes a description of responsibilities, minimum education and certification expectations, and required experience. Offerors shall propose qualified personnel that meet or exceed the stated requirements and shall clearly map proposed staff to the labor categories defined below.

UID	Labor Category	Duties	Education	Certifications	Experience	Minimum clearance level
NDR.47	Project Manager	Serves as the contractor's task manager overseeing personnel and supporting the NDR project.	A Bachelor's Degree in Computer Science, Information Systems, Engineering, Telecommunications, or other related scientific or technical discipline is desirable. Five (5) additional years of general experience may be substituted for the degree.	PMP or CISSP	Specialized Experience: Seven (7) years of experience in network security with a focus on cyber threat analysis and advanced network security analysis. Five (5) years of technical task management and supervisory experience.	High-Risk Public Trust (HRPT)

NDR.48	Cybersecurity Architect	Designs and define system architecture for new or existing complex networks. Determines systems specifications, input/output processes, and working parameters for hardware/software compatibility and maintenance of system security. Successfully coordinates design of subsystems and integration of total system. Identifies, analyzes, and able to resolve project support deficiencies.	A Bachelor's Degree in Computer Science, Information Systems, Engineering, Telecommunications, or other related scientific or technical discipline is desirable. Five (5) additional years of general experience may be substituted for the degree.	CASP+ CE CCNA-Security CISSP (or Associate) CND CSSLP CySA+ GICSP GSEC Security+ CE SSCP	5 Years with Bachelors in Science; 3 Years with Masters; 0 Years with PhD.	High-Risk Public Trust (HRPT)

NDR.49	Senior Engineer/Analyst	Performs technical planning, system integration, verification and validation, cost and risk, and supportability and effectiveness analyses for total systems. Skilled at performing analysis at all levels of total system product to include: concept, design, fabrication, test, installation, operation, maintenance and disposal. Has background of skills to ensure the logical and systematic conversion of customer or product requirements into total systems solutions that acknowledge technical, schedule, and cost constraints.	A Bachelor's Degree in Computer Science, Information Systems, Engineering, Telecommunications, or other related scientific or technical discipline is desirable. Five (5) additional years of general experience may be substituted for the degree.	CASP+ CE CCNA-Security CISSP (or Associate) CND CSSLP CySA+ GICSP GSEC Security+ CE SSCP	5 Years with Bachelors in Science; 3 Years with Masters; 0 Years with PhD.	High-Risk Public Trust (HRPT)

		Proficient with performing functional and timeline analysis.				
NDR.50	Mid-Level Engineer/Analyst	Performs technical planning, system integration, verification and validation, cost and risk, and supportability and effectiveness analyses for total systems. Skilled at performing analysis at all levels of total system product to include: concept, design, fabrication, test, installation, operation, maintenance and disposal. Has background of	A Bachelor's Degree in Computer Science, Information Systems, Engineering, Telecommunications, or other related scientific or technical discipline is desirable. Five (5) additional years of general experience may be substituted for the degree.	CASP+ CE CCNA-Security CISSP (or Associate) CND CSSLP CySA+ GICSP GSEC Security+ CE SSCP	2 Years with Bachelors in Science; 0 Years with Masters.	High-Risk Public Trust (HRPT)

		skills to ensure the logical and systematic conversion of customer or product requirements into total systems solutions that acknowledge technical, schedule, and cost constraints. Proficient with performing functional and timeline analysis.				

3.3. Tasks

NDR Deployment

The Contractor shall plan, deploy, and operationalize a modular and scalable Network Detection and Response (NDR) solution that is compliant with Department security standards and compatible with the Department's enterprise architecture. The initial implementation shall be driven by Government stakeholder priorities and funding availability, with the expectation that the solution will support expansion in future phases.

Deployment shall prioritize, as directed by the Government, the following network environments:

- Department of State (DOS) Data Centers
- Trusted Internet Connections (TIC) and Internet Gateways
- Demilitarized Zones (DMZs)
- Foreign and Domestic DOS Posts
- Non-Enterprise Networks (NENs)

The Contractor shall:

- Develop and deliver a comprehensive NDR Implementation Plan, to include timelines, phased deployment strategy, and milestone tracking.
- Execute a prioritized, phased deployment in accordance with stakeholder direction and available resources, ensuring the architecture supports future scaling.
- Provide hands-on-keyboard technical support for:
    - Deployment of sensor nodes, agents, and physical/virtual appliances
    - Configuration of management consoles and tuning of sensor parameters
    - Development and deployment of operational dashboards for analyst use
- Coordinate and conduct pilot testing and functional validation of the solution in collaboration with designated Government stakeholders.

Compliance and Authorization Support

The Contractor shall support the Department's efforts to achieve and maintain system authorization under the Risk Management Framework (RMF), including activities required for Authority to Operate (ATO) or Authority to Use (ATU). The Contractor shall ensure the NDR solution aligns with FedRAMP High baselines and Department-specific security requirements.

At a minimum, the Contractor shall:

- Support all RMF lifecycle steps, including control implementation, assessment preparation, and continuous monitoring readiness.
- Provide documentation and security artifacts necessary for system boundary accreditation, including but not limited to:
    - System Security Plans (SSP)
    - Risk Assessment Reports (RAR)
    - Security Control Traceability Matrix (SCTM)
    - Configuration Management Plans (CMP)
    - Privacy Threshold Analyses (PTA), if applicable
- Assist in preparing ATO/ATU packages, including participation in stakeholder reviews and information exchanges with the Information System Security Officer (ISSO), Authorizing Official (AO), and System Owner.
- Demonstrate compliance with requirement NDR-44, by either:
    - Providing documentation of FedRAMP High authorization, or
    - Providing proof of active submission to the FedRAMP PMO or sponsoring agency, along with a deployment approach and system architecture that is fully capable of operating within a FedRAMP High environment.
- Deliver evidence of compliance or capability to operate within a FedRAMP High-authorized environment, including FedRAMP-compliant architecture, control inheritance documentation, and any subcontractor authorization materials.
- Draft and maintain a Deployment Risk Register, identifying and tracking risks associated with accreditation, including proposed mitigation strategies and resolution timelines.

System Management and Sustainment

The Contractor shall support the operational readiness, sustainment, and optimization of the deployed Network Detection and Response (NDR) solution during the transition period and in coordination with Government stakeholders. The Contractor shall ensure the system is properly configured, documented, and transitioned for Government-led operations, while maintaining Tier 3-level subject matter expertise (SME) support for complex or escalated issues.

At a minimum, the Contractor shall:

- Support Transition to Operations (TTO) by:
    - Coordinating with Government personnel to plan and execute the transition of system ownership
    - Providing technical walkthroughs, documentation, and shadowing opportunities for Government staff
    - Delivering a finalized Transition to Operations Plan including milestones, artifacts, and post-transition responsibilities
- Deliver all system documentation, including:
    - System architecture and design documents
    - Sensor and appliance configuration baselines
    - Standard operating procedures (SOPs), tuning guides, and dashboard playbooks
- Ensure centralized system management capability across all deployed components to support configuration changes, rule updates, and health monitoring during transition
- Implement automated workflows for:
    - Patching and signature updates
    - Policy distribution and performance tuning
- Provide role-based training and knowledge transfer, tailored for SOC analysts, ISSOs, and system administrators
- Assign a Tier 3 NDR Subject Matter Expert (SME) to provide ongoing expert-level technical support to the Government post-transition, including:
    - Complex troubleshooting
    - Advanced detection tuning and analysis
    - Integration support for new data sources or threat intelligence feeds
    - Strategic advisory on future enhancements or scalability
    - Support for unplanned outages or system degradation events, including after-hours availability on an on-call basis when required by the Government

The Tier 3 SME resource shall remain available as a designated resource throughout the contract period of performance.

3.4. Desired Outcomes

The desired outcomes of the Network Detection and Response (NDR) solution include:

- Real-time detection and automated response to advanced network-based threats.
- Enhanced threat visibility across on-premises, cloud, and hybrid environments.
- Reduction in alert fatigue through advanced incident aggregation and triage capabilities.
- Compliance with federal cybersecurity mandates, including Executive Order 14028, FISMA, and FedRAMP High standards.
- Improved scalability and interoperability with existing Departmental cybersecurity infrastructure.
- Offerors shall clearly demonstrate how their proposed solution will achieve these outcomes and provide measurable benchmarks for success.

4. Deliverables and Schedule

This section outlines the required deliverables, reporting, and support expectations for the Network Detection and Response (NDR) solution. All deliverables shall be submitted to the COR and CO, unless otherwise specified.

UID	Deliverable	Description	Due Date
D-01	Kickoff Meeting	Orientation on implementation strategy and goals	Within 7 days of contract award
D-02	Onsite Discovery & Requirements Validation	Contractor-led onsite discovery with ISSOs and analysts to validate requirements and inform planning	Within 10 business days
D-03	Baseline Assessment	Review of current detection posture, log architecture, and threat landscape	Within 15 business days
D-04	Initial NDR Rollout	Begin phased deployment of NDR sensors, agents, and appliances	Within 30 days of contract award
D-05	Platform Configuration	Configure detection rules, dashboards, RBAC, and anomaly thresholds	Within 60 days
D-06	Integration Testing	Integrate NDR with Splunk, ServiceNow, SOAR, and other security tools	Within 60 days
D-07	Help Desk & IR Workflow Setup	Establish escalation matrix, KBAs, and incident response workflows	Within 90 days
D-08	Training Sessions	Deliver tiered training for SOC analysts and engineers	By Day 90 and as requested
D-09	Monitoring Setup	Enable telemetry, packet capture optimization, and alert tuning	Within 90 days
D-10	Engineering,	Complete engineering, deployment, and	By Day 180

	Configuration, and Installation of NDR	system configuration	
D-11	Final Acceptance Testing	Joint validation of NDR capabilities and simulation of core use cases	By Day 180
D-12	Transition to Operations & Maintenance	Turn over system to Government with finalized architecture documentation and SOPs	By Day 180
D-13	Ongoing Operational Support	Provide Tier 2/3 support, tuning, and SOC optimization, including onsite presence as needed	Day 180 through contract duration
D-14	Security Compliance Support	Support FedRAMP Authorization, RMF, and FISMA compliance including SSPs and POA&Ms	Award through contract duration
D-15	Audit & Performance Validation	Conduct periodic audits to validate operational, security, and performance metrics	Ongoing
D-16	Roadmap Planning	Collaborate with stakeholders to plan enhancements and scalability improvements	Ad hoc, as requested
D-17	Weekly Status Meeting Minutes	Provide minutes capturing status, blockers, actions, and sprint priorities	Weekly

Table 1 List of Deliverables

4.1. Monthly Performance Reports

The Contractor shall submit a Monthly Performance and Progress Report by the 5th of each month, summarizing:

- Accomplishments, risks, and mitigation actions
- Project milestones and deliverables status
- Cost reporting and cumulative performance data
- Analysis to support monthly COR review meetings
- Format must be approved by the COR within 10 business days of award.

4.2. Delivery

All deliverables will be submitted to the acquiring agency's Contracting Officer's Representative (COR) with a copy to the acquiring agency's Contracting Officer (CO). Inspection and acceptance of all work performance, reports, and other deliverables under this task order shall be performed by the COR. In addition, the Vendor shall provide deliverables to the following electronic mail addresses:

- Contract Officer Representative (COR),

- Cyber Operations Deputy Division Chief,
- Cyber Operations Division Chief,

4.3. Operations and Maintenance

The Contractor shall provide post-deployment support and sustainment services including:

- Include US-based OEM support accessible 24 hours a day x 7 days a week, by phone, web, email, and include a dedicated account subject matter expert (SME) for DoS, as well as a clearly defined escalation and resolution process included within the solution.
- Deliver detailed description of warranty, license, and maintenance support services to include service level agreements and mean time to resolution projections for standard and severe support incidents.
- Dedicated account SME with defined escalation process
- Warranty and maintenance support with SLAs and MTTR metrics
- Training options: admin, analyst (Jr/Mid/Sr), virtual or in-person
- Customer web portal with:
    - Asset/version tracking
    - SOPs, guides, white papers
    - Searchable KBAs
    - Ticketing and historical incident tracking
- Outline clearly defined Returned Merchandise Authorization (RMA) processes, with 4-hour drop shipment of replacement components.
- Secure software updates, including:
    - Security patches
    - Feature updates
    - IOCs, threat signatures, AI/ML model updates
- Contractor shall assume and accept that DOS will not return any hard drives.

5. Quality Assurance Surveillance Plan (QASP)

5.1. Acceptance Criteria and Inspection

The oversight provided for in the order and in this plan would help to ensure that service levels reach and maintain the required levels throughout the contract term. Further, this plan provides the COR with a proactive way to avoid unacceptable or deficient performance and provides verifiable input for the required Past Performance Information.

Assessments or Contractor Performance Assessment Reports (CPARS). Inspection and acceptance of all work performance, reports, and other deliverables under this task order shall be performed by the DOS COR at the COR designated work location.

All documents and deliverables (‘work products’) produced by the Contractor as part of performance shall meet the following general acceptance criteria. Additionally, the Contractor shall ensure that the NDR solution achieves the following performance metrics:

- False positive rate below 5% under normal traffic conditions.
- False negative rate below 2% under known attack conditions.
- System uptime of 99.9% or higher.
- Reduction in mean time to detect and respond to threats by 50%. Deliverables that fail to meet these metrics will be subject to corrective action as outlined in Section 5.2.

The Contractor and its Sub-Contractors must meet the quality measures, described below, for any and all work products and deliverables submitted to the Government.

- Timeliness – Work products and deliverables shall be available at the time required and generated on or before specified due dates as stated in the Contractor or issued task order.
- Quality – Quality consists of the two elements, value and accuracy, as described below.
- Value – Work products shall directly address objectives as directed by the COR.
- Accuracy – Work products and deliverables shall be free errors and mistakes; and be developed in accordance with applicable laws, regulations, policies, and procedures.
- Completeness – Work products and deliverables shall address all content as directed by the COR.
- Clarity – Work products and deliverables shall be easy to understand. Work products and deliverables shall be designed to achieve agreed-to objectives, tailored to identified audiences, avoid materials not germane to the objective, and be of high quality with regard to grammar and sentence structure.
- Format – Work products and deliverables shall be submitted in soft copy via email, unless otherwise required by the COR.

The COR will review draft and final work products for completeness, accuracy, and appropriateness. If the COR identifies or encounters any significant deficiencies, and is therefore considered non-acceptable, then the COR will return the work product to the Contractor.

For all work products or deliverables that the COR deems unacceptable or deficient, the Contractor will be required to correct or augment the deficiency as required.

The Contractor shall submit a revised, corrected work product or deliverable within two (2) business days from initial notification by the COR (or as otherwise specified by the COR).

Unacceptable deficiencies that would require Contractor resubmission at no extra cost to the Government include, but are not limited to, the following examples:

- Omitting required documents or information;
- Non-conforming documents (according to pre-stated or mandatory standards regarding

content and format);
- Disorganized or poorly organized review packages;
- Non-adherence to review protocols and accepted procedures;
- Making material errors or allowing substantial inadequacies; and,
- Any other fundamental error or mistake on the part of the Contractor.

The COR may delegate responsibility for review of any work product and/or deliverable to other Government employees who possess the appropriate expertise for their consideration and input regarding acceptability or deficiencies.

All Contractor deliverables and work products produced as part of performance under this contract become Government property. As Government property, such deliverables and work products shall not be used by the Contractor for any other purposes.

5.2. Basis of Acceptance

The basis for acceptance shall be in compliance with the requirements set forth in the statement of work, the Contractor's proposal and other terms and conditions of the Contract. Deliverable items rejected shall be corrected in accordance with the applicable provisions.

- Reports, documents, and narrative type deliverables will be accepted when all discrepancies, errors or other deficiencies identified, in writing, by the Government have been corrected.
- If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.
- All of the Government's comments to deliverables must either be incorporated in the succeeding version or the Contractor must demonstrate, to the Government's satisfaction, why such comments should not be incorporated.
- If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, improper format, or otherwise does not conform to the requirements stated within this Contract, the document may be immediately rejected without further review and returned to the Contractor for correction and re-submission. If the Contractor requires additional Government guidance to produce an acceptable draft, the Contractor shall arrange a meeting with the COR.

5.3. Review

During the performance of this order, the COR will take periodic performance reviews, conduct meetings with DOS analysts and stake holders and analyze contractor provided reporting and observed performance, and will determine whether the performance meets the requirements set forth in this PWS. The COR will also perform random checks of the work products, files, and other outputs provided by the contractor.

5.4. Contract Closeout

Contract closeout procedures will be issued upon 90 days after this task order has ended. The determination of final costs for this effort shall be requested. This does not preclude the Contractor's right to funds invoiced but not collected, if any. (FAR 42.708) A release of claims document shall be submitted within 90 days of completion of this task by the Contractor.

6. Evaluation Process

Proposals will be evaluated based on the criteria described in this solicitation to determine the offeror's ability to fulfill the Department's requirements for a Network Detection and Response (NDR) solution. The Government will use a best-value tradeoff process, considering both technical merit and overall risk. Technical proposals will be evaluated independently against the stated factors and subfactors; they will not be compared directly to other offers.

Technical Submission Instructions

Formatting Requirements:

- The technical submission shall include a Table of Contents identifying all sections and subsections with corresponding page numbers.
- All files must be compatible with Microsoft Office 2019 or later and shall not be password-protected.
- Pages shall be numbered using a consistent scheme that applies to all documents, figures, and tables.
- Paper size shall be 8.5 x 11 inches.
- Font shall be 12-point, single-spaced Times New Roman. Graphics may use no smaller than 9-point font; tables no smaller than 10-point font.
- Margins shall be a minimum of one inch on all sides. Header/footer content is permitted but shall not include any evaluative material.

Page Limitation

The response to Factor 1 – Technical Approach, including the Proof of Concept and Deployment Strategy, shall not exceed 15 pages. This limit does not include appendices (e.g., the completed Solution Requirements Matrix) or pre-printed product literature.

Offerors are expected to provide sufficient detail within the page limit to clearly demonstrate their technical solution and deployment approach.

6.1.1. Factor 1 - Technical Approach

The Offeror shall submit a clear, complete, and technically sound description of its approach for delivering the required Network Detection and Response (NDR) solution and services. The submission shall demonstrate how the proposed solution aligns with the Department's

cybersecurity modernization objectives, integrates with existing systems, and supports scalable deployment across enterprise environments.

6.1.2. Solution Requirements Matrix

The Offeror shall complete and submit a Solution Requirements Matrix that maps directly to the requirements outlined in this Performance Work Statement (PWS), specifically:

- Section 3.2.1 – Technical Requirements (35)
- Section 3.2.2 – Software Integration Requirements (8)
- Section 3.2.3 – Compliance Requirements (3)
- Section 3.2.4 – Personnel Requirements (4)

For each listed requirement, the Offeror shall indicate one of the following implementation statuses:

- *Fully Meets*
- *Partially Meets*
- *Requires Additional Modules*
- *Does Not Meet*

The completed matrix must be submitted as a standalone attachment. Narrative explanations are not required and will not count toward the 15-page Technical Volume limit.

6.1.3.Proof of Technology (POT)

The Offeror shall submit a high-level Proof of Technology (POT) that demonstrates how the proposed Network Detection and Response (NDR) solution meets Departmental requirements. The POT shall include the following elements:

- A "to-be" architecture diagram illustrating the proposed NDR solution integrated within the Department’s enterprise architecture.
- A description of NDR components, including sensors, agents, cloud-native or on-premises appliances, and management consoles.
- A summary of alerting and automated response capabilities.
- A description of AI/ML features used for threat detection, anomaly detection, and behavioral analytics.
- A list of required ports, protocols, and encryption standards.
    - A description of integration methods with the following existing tools:Splunk
    - Zeek
    - Suricata
    - ServiceNow

- Palo Alto Networks
- Syslog
- Cribl
- Nutanix Robo
- Microsoft Defender products

The Government will evaluate the Proof of Technology (POT) based on the overall **completeness, feasibility, technical maturity**, and **relevance** of the proposed solution elements. Emphasis will be placed on how well the POT demonstrates:

- Seamless integration with existing Department tools and infrastructure.
- Advanced detection and automated response capabilities.
- Use of AI/ML for enhanced behavioral analysis.
- Clear articulation of deployment architecture and operational fit.

6.1.4.Deployment Strategy

The Offeror shall provide a Deployment Strategy that clearly articulates how the proposed NDR solution will be implemented in a phased, scalable, and operationally efficient manner across Department's on-premises and cloud IT environments.

The strategy shall include:

- Implementation Timeline using Agile methodologies or similar iterative approaches.
- Phased Deployment Plan, including:
  - Base Year: Deployment to DOS Data Centers
  - Option Year 1: DOS Internet gateways (TIC), Demilitarized Zones (DMZs)
  - Year 2 and beyond: Foreign and Domestic Posts, Non-Enterprise Networks (NENs)

Additionally, the strategy shall address:

- Support for RMF compliance and achieving full Authority to Operate (ATO)
- Development of Deployment Plans, Change Requests (CRs), and Firewall Access Board (FAB) submissions
- Participation in Testing and Pilot phases
- Hands-on-keyboard support for deployment and configuration of sensors, appliances, and agents
- Sensor tuning, console configuration, and dashboard/workflow setup
- Automation of patching, updates, and tuning
- Training and certification by user role or persona

- Development of a Risk Register with mitigation strategies for deployment risks

The Government will evaluate the Deployment Strategy based on the overall completeness, feasibility, scalability, and operational readiness of the proposed approach. Emphasis will be placed on how well the strategy demonstrates:

- Phased implementation that aligns with Department deployment priorities.
- Operational integration with Department infrastructure and change control processes.
- Support for RMF compliance, ATO readiness, and secure configuration practices.
- Readiness to support pilot testing, hands-on deployment, and tuning activities.
- Use of automation to streamline deployment, patching, and tuning.
- Training and transition planning to ensure knowledge transfer and long-term maintainability.

Factor 2 - Management Approach

The Offeror shall describe its approach for managing the contract and delivering services defined in the Performance Work Statement (PWS). The submission shall demonstrate the Offeror's ability to coordinate technical and operational tasks, mitigate risks, manage resources, and communicate effectively with Government stakeholders.

The management approach must address:

- Project and task management processes (including Agile methodologies, if applicable)
- Change and configuration management
- Risk management and mitigation strategies
- Schedule and milestone tracking
- Resource and financial planning
- Quality control and contract performance monitoring
- Communication, reporting, and stakeholder engagement

The Offeror shall include a Contract Quality Control Plan (QCP) that describes how the Offeror will ensure consistent delivery of high-quality services and deliverables throughout the period of performance.

The Government will evaluate the Management Approach based on its completeness, clarity, and suitability for ensuring successful contract performance. Emphasis will be placed on the following:

- Effectiveness of the proposed project and contract management structure
- Demonstrated ability to manage technical complexity and evolving requirements
- Risk mitigation strategies that minimize schedule or operational impact
- Quality control processes that ensure consistent, high-quality outcomes

- Clarity of roles, responsibilities, and stakeholder communication methods

6.1.5. Factor 3 - Key Personnel

The Offeror shall propose Key Personnel who are qualified and capable of performing the roles required to deliver the NDR solution successfully. At a minimum, the Offeror shall propose the following roles:

- Project Manager
- Cybersecurity Architect
- Cybersecurity Security Engineer, Solutions Engineer, or Solution SME

For each proposed Key Personnel, the Offeror shall submit a résumé that includes:

- Name
- Role (e.g., Project Manager, Cybersecurity Architect, Lead Engineer)
- Security Clearance (e.g., Secret; expires Jan 1, 2026)
- Experience (1 paragraph detailing relevant experience with NDR implementations or similar enterprise cybersecurity programs)
- Education (e.g., MS in Information Systems, University of Virginia)
- Certifications (e.g., PMP, CISSP, CISM)
- Professional Profile Link (LinkedIn or equivalent, if applicable)

All proposed Key Personnel shall possess a minimum of a current High Risk Public Trust (HRPT) security clearance.

The Government will evaluate the qualifications, relevant experience, and alignment of proposed Key Personnel with the roles and responsibilities required for successful contract execution. Emphasis will be placed on:

- Demonstrated experience deploying enterprise-scale NDR or cybersecurity solutions
- Technical depth and leadership capability in complex, mission-critical environments
- Alignment of personnel expertise with the Department's mission and operational environment
- Active security clearance and certification relevance
- Stability and availability of proposed personnel

6.1.6. Factor 4 - Past and Present Performance

The Offeror shall provide past performance information for three (3) contracts performed within the last three (3) years, with federal civilian government agencies, that are similar in scope, size, and complexity to the NDR solution described in this solicitation.

For each contract, the Offeror shall provide:

- Agency or organization name
- Contract number and period of performance
- Contract type and total value
- Description of services and capabilities delivered
- Relevance to the current requirement
- Government point of contact (name, title, email, and phone number)

The Government will evaluate the relevance, quality, and outcomes of the Offeror's past and present performance in delivering solutions similar in size and complexity to the NDR requirement. Emphasis will be placed on:

- Demonstrated success in deploying enterprise-scale cybersecurity or NDR solutions
- Evidence of strong customer satisfaction, timely delivery, and effective performance
- Relevance of technical and operational environments to the Department's needs
- Proven ability to operate in secure and mission-critical federal environments

Factor 5 - ***Certifications (FedRAMP, C-SCRM)***

The Offeror shall provide verifiable documentation demonstrating its FedRAMP High authorization status. The Government will evaluate the Offeror's submission based on the following criteria:

- Current certification issued by the FedRAMP Program Management Office (PMO), or
- A FedRAMP authorization letter or marketplace listing, or
- A sponsor letter confirming Joint Authorization Board (JAB) or agency review, or
- Submission confirmation with a System Security Plan (SSP) aligned to FedRAMP High baselines.
- Solutions still under review must demonstrate technical readiness to operate within a FedRAMP High environment, including alignment with applicable security controls and architectural requirements.
- All services and personnel supporting the solution must be U.S.-based.
- All infrastructure must be located within the United States.

6.1.7. All cryptographic functions must use FIPS 140-2 or FIPS 140-3 validated modules, in accordance with federal standards and Department policy.