PERFORMANCE WORK STATEMENT (PWS)
CYBERARK PRIVILEGED ACCESS SECURITY INTEGRATION AND IMPLEMENTING PRIVLEGED USER MANAGEMENT
August 2, 2019

1.0 BACKGROUND

1.1 The National Archives and Records Administration (NARA) is an independent Federal agency that helps safeguard and preserve our nation's history by overseeing the management of all Federal records. The stories of our nation and our people are told in the records and artifacts cared for in NARA facilities around the country so that people can discover, use, and learn from this documentary heritage. The mission is to ensure ready access to the essential evidence that documents the rights of American citizens, the actions of Federal officials, and the national experience.

1.2 NARA operates a Wide Area Network (WAN) that provides network services to all NARA facilities throughout the country. This network is known as NARANet. The services of NARA's General Support System (GSS) are provided by Micro Focus (Suse Linux) with Active Directory domains used by specific applications and NARA workstations. NARA's Identity and Access management (IAM) system provides access governance to NARA on premises IT systems. In many cases this access is managed from the NARA Identity Management system (IDMS). CyberArk Privileged Access Security (PAS) will be set up and integrated with NARA's IDMS to provide privileged user management and access to NARA's Network Infrastructure devices and Information Systems/Applications.

2.0 SCOPE OF WORK

2.1 The scope of work includes all personnel and resources necessary to support NARA in the implementation of Privileged Access Management through CyberArk Privileged Access Security. This includes installing and configuring CyberArk Privileged Access Security and implementing and documenting the on-boarding of privileged accounts using CyberArk for NARA's Infrastructure Devices and Applications.

2.2 The Vendor shall be required to perform these services during normal hours of operation at Archives II, 8601 Adelphi Road College Park, MD 20740 or work remotely and be available via email or phone. NARA requires the Vendor to collaborate with U.S. Government personnel and other government Vendors.

2.2.1 For the duration of this contract, normal hours of operation at NARA are between the hours of 6:30 a.m. and 6:30 p.m., Monday through Friday, 52 weeks a year excluding weekends and Federal holidays. During these hours, the Vendor shall provide sufficient staffing levels to perform the required services.

2.2.2 Federal holidays observed by NARA

New Year's Day	Labor Day	Inauguration Day

M L King's Birthday	Columbus Day
President's Day	Veterans Day
Memorial Day	Thanksgiving Day
Independence Day	Christmas Day

2.2.2.1 In addition to the holidays listed above, any day specifically declared by the President of the United States will be considered a Federal holiday.

2.2.2.2 When a holiday falls on a Sunday, the following Monday shall be observed as the Federal holiday. When a holiday falls on a Saturday, the preceding Friday shall be observed as the Federal holiday

2.3 Before 6:30 a.m. and after 6:30 p.m., Monday through Friday, support is deemed on-call. To support emergency operations, maintenance and testing schedules, and to assist with operational uptime for NARANet, Vendor personnel shall be on-call before and after the normal hours of operation, including weekends (Saturday and Sunday) and holidays. After hours support averages 40 hours per year.

2.4 In the event of a NARA facility closure, the Vendor is expected to work remotely and generally be available via email or phone. The Vendor shall check the operating status of the Government at www.opm.gov and/or call (301)-837-0700 to obtain the latest NARA facility status. If the Government operating status at www.opm.gov authorizes unscheduled telework, the Vendor shall report to NARA unless otherwise directed by the Contracting Officer's Representative (COR).

2.5 All services and Electronic Information Technology (EIT) delivered as a result of this task order shall comply with accessibility standards in accordance with FAR Subpart 39.2, Electronic and Information Technology as required by Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended. Information about the Section 508 Electronic and Information Technology Accessibility Standards may be obtained via the Web at the following uniform resource locator (URL): www.Section508.gov.

3.0 DESCRIPTION OF SERVICES

3.1 Objective. NARA's objective is to obtain professional services for the design, testing, implementation, deployment, and support for NARA's Privileged Access Management tool, CyberArk Privileged Access Security.

3.2 CyberArk Implementation. The Vendor shall install the following components of the CyberArk Privileged Access Security ("PAS") solution:

- Enterprise Password Vault ("EPV"),
- Disaster Recovery ("DR"),
- EPV, Central Policy Manager ("CPM"),
- Password Vault Web Access ("PVWA"),
- Privileged Session Manager ("PSM"), and
- Privileged Session Manager Proxy ("PSMP").

3.2.1 The Vendor shall install and configure the following components with CyberArk PAS solution on servers hosting the following components:

- Primary Standalone Vault
- DR Standalone Vault
- Front End Servers consisting up to:
    - 1x CPM
    - 2x PVWA with Customer configured Network Load Balancing
    - 2x PSM with Customer configured Network Load Balancing
    - 2x PSMP with Customer configured Network Load Balancing
- CyberArk Backup Utility
- DR Front End Servers consisting up to:
    - 1x CPM (inactive)
    - 1x PVWA with Customer configured Network Load Balancing
    - 1x PSM with Customer configured Network Load Balancing
    - 1x PSMP with Customer configured Network Load Balancing

3.2.2 The Vendor shall provide a CyberArk Architectural Diagram

3.2.3 The Vendor shall perform system hardening after installation of the components of the CyberArk PAS solution. This includes installing the latest supported security patches for the CyberArk PAS solution. Evidence of completion will be a Nessus Security scan.

3.2.4 The Vendor shall perform the following integrations:

- Security Information and Event Management (SIEM) - Tenable Log Correlation Engine (LCE)
- Event Notification Engine - Tenable LCE
- Lightweight Directory Access Protocol over SSL (LDAP)[S] Integration - NARA's WIN Active Directory (AD)

3.2.5 The Vendor shall test the following components and troubleshoot as needed:

- CPM (account management) and PSM (secure connections)
    - Connect up all privileged accounts for each of the following platforms in production:

        - Windows (Local/Domain) - NARA's WIN Active Directory (AD)
        - Unix (Root)
        - Database (MSSQL SA and Oracle SYS)
        - Amazon Cloud (Secret Keys and Accounts)
        - Microsoft Azure
        - NARA Infrastructure devices/Cisco Identity Services Engine (ISE)
        - CMRS
        - ARCIS
        - ERA 2.0
        - VMWare vSphere
    - Basic Accounts Discovery scan
    - Validate audit data has been generated
- PSMP
    - Secure Connect for the SSH Protocol
    - Validate audit data has been generated and review

3.2.5.1 The Vendor shall provide written instructions on how to connect any new components of platforms listed in section 3.2.5.

3.3. CyberArk Privileged Access Management Onboarding. The vendor shall perform privileged access management and onboard privilege credentials for local administrator, domain administrators, service accounts, usages, and local Unix accounts using CyberArk.

- Connect all privileged accounts per each of the following platforms in production:
    - Windows (Local/Domain) - NARA's WIN Active Directory (AD)
    - NARA Infrastructure devices/Cisco ISE
    - CMRS
    - ARCIS
    - ERA 2.0
    - VMWare vSphere
    - Amazon Cloud
    - Microsoft Azure

3.3.1 The Vendor shall provide written instructions on how to connect any accounts components of platforms listed in section 3.3.

3.3.2 The Vendor shall provide written instructions on how a NARA user can request, approve, and receive access to privileged account credentials in CyberArk.

3.3.3 The Vendor shall provide written instructions on how to set up password vaulting for the components listed in Section 3.3

3.4 CyberArk Environment Configuration. The vendor shall configure the CyberArk environment per project requirements in areas of:

- Access Management and Control Model
    - Authentication
    - Authorization
    - Define CyberArk specific permissions based on roles-based groups
- Safe and Data Permissions Structure
- Create new Safe and Permissions structure in Vault based on Safe Naming and Safe Permissions conventions, incorporating specific technical requirements
- Master Policy Configurations and Platforms Management
    - Configure policies based on Policy Creation procedure to manage new account groups based on specific technical requirements and test with test accounts
    - Workflows and Privilege Account Controls
    - Define CyberArk controls need to be implemented for different groups of accounts
    - Define CyberArk specific workflows

3.4.1 The Vendor shall document the CyberArk configurations and policies listed in 3.4.

3.5. CyberArk Reporting. The Vendor shall provide the following monthly reports:

- Privileged Account Inventory report
- Application Inventory report
- Privileged Account Compliance Status
- Entitlement Report

3.5.1 The Vendor shall provide additional Activity Log Report on an ad-hoc basis. This will not exceed more than five (5) reports per month.

4.0 NARA IT Security Requirements

The Vendor must comply with NARA IT Security Requirements, per Attachment A. These requirements establish and implement specific NARA IT security requirements.

The Vendor must comply with the NARA IT Security Requirements for Cloud-based systems, per Attachment B. These requirements apply to all contractors and subcontractors, including cloud service providers ("CSPs"), and personnel of contractors, subcontractors, and CSPs that may access, collect, store, process, maintain, use, share, retrieve, disseminate, transmit, or dispose of NARA Information. These requirements establish and implement specific NARA security requirements applicable to the reference contract.

5.0 DELIVERABLES AND PERFORMANCE MEASURES AND STANDARDS

All written deliverables shall be subjected to government review and approval before final acceptance on the due date in the Deliverables Table. The review and approval period will occur

before the due date and will proceed as follows. The Vendor will submit deliverables for review and approval no less than 10 business days prior to the due date in the Deliverables Table. Government will respond within five (5) business days of receipt of delivery with comments and suggested corrections. The Vendor shall provide agreed upon corrections within 5 business days of receipt of Government comments. Any changes to this timeline must be approved by the Contracting Officer.

PWS PARAGRAPH	DELIVERABLE	FORMAT	DUE
3.2.2	CyberArk PAS Architectural Diagram	Microsoft Visio	30 days after award of contract
3.2.3	System hardening after installation of the components of the CyberArk PAS solution	Tenable Nessus report	50 days after award of contract
3.2.5.1	Instructions on how to connect any new components of platforms listed in section 3.2.5	Google Doc or MS Word	60 days after award of contract
3.3.1	Instructions on how to connect any accounts components of platforms listed in section 3.3	Google Doc or MS Word	60 days after award of contract
3.3.2	Instructions on how a NARA user can request, approve, and receive access to CyberArk.	Google Doc or MS Word	60 days after award of contract
3.3.3	Instructions on how to set up password vaulting for the	Google Doc or MS Word	60 days after award of contract

	components listed in Section 3.3		
3.4.1	CyberArk configuration policy document	Google Doc or MS Word	90 days after award of contract
3.5	Monthly privileged account management reports	Google Doc or MS Word	1st day of each month
3.5.1	Activity Log Report	Adobe PDF or Microsoft CSV	ad-hoc

6.0 Government Furnished Equipment (GFE)

The Government may provide Government Furnished Equipment, if needed (1) each: desk, telephone, and computer at Archives. All GFE shall be returned to the COR within five (5) business days after completion of the project.

NARA will provide any servers for the proposed system.
NARA will provide the base Operating System for any servers for the proposed system.

7.0 Government Furnished Information (GFI)

Prior to release and during the course of contract execution, NARA will provide the Vendor with access to information about NARA's network architecture and operational procedures that relate to and are required to successfully complete the contract. These documents are available upon signing a Non-Disclosure Agreement.

Tenable Nessus Security scans for CyberArk servers
NARA Information System Inventory
List of privileged users for each Information System

Vendors are required to comply with NARA's security policies and procedures at all times with respect to protecting and controlling the use of this information.

Additional GFI will be provided to the Vendor as needed.