STATEMENT OF OBJECTIVE

BUILDING 1044: Mount Rack Storage Filer System Acquisition & Integration (SCIF Environment)

New Mexico Air National Guard

2251 Air Guard Drive S.E. Kirtland AFB, NM 87117

Date: 21 July 2026

Table of Contents

1 Purpose 1
2 Scope 1
3 Current Equipment 1
4 Technical & Operational Objectives 2
a. System Equivalency & Capacity 2
b. Disaster Recovery & Data Management 2
c. High Availability & Connectivity 2
5 Logistics, Safety & Site Operations 2
a. Workplace Safety & SCIF Migration 2
b. Material Disposition & Training 3
6 Security & Military Installation Access 3
a. Personnel Clearances & Base Access 3
b. AFNet, Supply Chain, & Data Sovereignty 4
7 Schedule, Work Hours & Execution 4
a. Work Hours & Holidays 4
b. Execution Window & Work Planning 4
8 Deliverables, Testing & Quality Assurance 4
a. Quality Control & System Testing 4
b. Operations & Maintenance Manuals 5
9 Contracting & Regulatory Compliance 5
a. Subcontracting Opportunities 5
b. SAM Registration 5

Statement of Objectives (SOO)

Mount Rack Storage Filer System Acquisition & Integration (SCIF Environment)

1 Purpose

The purpose of this acquisition is to procure, install, configure, and migrate a highly available, redundant Enterprise Storage Filer solution. The primary objective is to ensure resilient, high-performance data storage, tiering, archival, and disaster recovery (DR) capabilities while maintaining strict compliance with Air Force Network (AFNet) standards, Defense Intelligence Agency (DIA) supply chain security, and physical workplace safety protocols within a Sensitive Compartmented Information Facility (SCIF).

2 Scope

This requirement encompasses hardware delivery, logical configuration, network integration, disaster recovery implementation, robust system testing, and system administration training for a minimum 100TB storage environment distributed across three separate filers. The scope includes rigorous work planning, quality control, and the physical tear-down of legacy materials. The contractor shall un-rack and stage all legacy hardware as directed by the Government; however, no legacy materials, components, or e-waste are authorized to leave the facility. All physical installation, migration, logical configuration, and material handover will occur strictly within the SCIF.

3 Current Equipment

The current Storage Area Network (SAN) infrastructure supporting the 250 IS environment is composed of three (3) HPE MSA 2050 storage arrays and two (2) dedicated management servers configured as follows:

System Component	Hardware Model	Quantity	Role / Configuration	Storage Media Per Array
Primary SAN Storage	HPE MSA 2050	2	Primary storage pool configured in a mirrored (high availability) architecture.	• 10 x 12 TB SAS Hard Drives• 2 x 2 TB SAS Management Drives
Disaster Recovery (DR) SAN	HPE MSA 2050	1	Dedicated Disaster Recovery Site (DRS) node utilizing software-based replication to back up the primary configuration.	• 10 x 12 TB SAS Hard Drives• 2 x 2 TB SAS Management Drives
Primary Management Server	HPE ProLiant DL325 Gen10	1	Dedicated management server hosting orchestration software for the primary mirrored SAN configuration.	N/A (Compute/Mgmt)

DRS Management Server	HPE ProLiant DL360 Gen9	1	Dedicated management server hosting replication and backup software for the DRS SAN.	N/A (Compute/Mgmt)

4 Technical & Operational Objectives

The contractor shall offer and implement a solution that achieves the following operational capabilities, ensuring at a minimum that the offered system possesses the exact same capabilities, functions, and performance metrics as the legacy system, or better:

a. System Equivalency & Capacity

The minimum offered solution must meet or exceed all current legacy system functions, capabilities, and performance baselines. The architecture must deliver a minimum of 100TB Usable Total Storage distributed across three separate filers, featuring a minimum of 2TB SLC Flash Storage (or equivalent performance) and enabling full storage virtualization.

b. Disaster Recovery & Data Management

The contractor must integrate a comprehensive DR solution to support Continuity of Operations (COOP), including secure data replication, automated failover, and robust backup/restore processes. Data management must support automatic tiered storage, allow the allocation of multiple RAID levels on the same storage tier, and implement independent archival capabilities.

c. High Availability & Connectivity

The system must ensure high availability through redundant control modules, redundant power supply units (PSUs), redundant cooling modules, and redundant internal storage, alongside redundant iSCSI capability with seamless controller failover. Connectivity requirements mandate a minimum of four 10Gbit SFP network connections per system, capable of utilizing fiber adaptors.

5 Logistics, Safety & Site Operations

The contractor shall execute the physical deployment in strict accordance with military safety and SCIF security protocols:

a. Workplace Safety & SCIF Migration

All physical work, heavy lifting, and rack installation must comply with the US Army Corps of Engineers (USACE) Safety and Health Requirements Manual EM 385-1-1, as well as applicable OSHA standards. The contractor is responsible for physically executing and

coordinating the movement of legacy filers/racks and the installation of new equipment inside the secure facility, working in close coordination with the Special Security Officer (SSO).

b. Material Disposition & Training

The contractor is responsible for the removal and off-base environmental disposition of all non-salvageable materials, packaging, and legacy e-waste, excluding any storage media governed by security mandates. Additionally, the contractor must provide comprehensive administrative and operational training for two designated Government personnel within the secure facility.

6 Security & Military Installation Access

Contractor personnel must operate within strict DoD, Air Force, and Intelligence Community (IC) constraints:

a. Personnel Clearances & Base Access

At a minimum, all contractor personnel performing on-site work must possess and maintain an active Secret clearance for the duration of the contract. Personnel must comply with all host Military Installation security directives, vehicle search protocols, and unescorted access procedures prior to arriving at the SCIF.

For Contractors that do not require CAC but require access to a DoD Facility and/or Installation. Contractor and all associated sub-contractors employees shall comply with adjudication standards and procedures using the National Crime Information Center Interstate Identification Index (NCIC-III) and Terrorist Screening Database (TSDB) (DODIO 2000.16V1_DAFI 31-145, DAFI 31-101 and DODM 5200.08v3_DAFMAN 31-101v3), applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by government representative), or, at OCONUS locations, in accordance with status of forces agreements and other theater regulations.

For Contracts that require Handling or Access to Classified Information. For contracts that require handling or access to classified information, the contractor shall comply with FAR Clause 52.204-2, Security Requirements, including the National Industrial Security Program Operating Manual (DoD 5220.22-M) and applicable updates/changes. This clause involves access to information classified “Confidential/Secret/Top Secret” and requires contractors to comply with visitor Group Security Agreement (VGSA) when designated as a Visitor Group at all contractor operations located on Air Force/Air National Guard installations in accordance with this PWS. Contract personnel must be entered into the Defense Information

System for Security (DISS) and vendor will comply with paragraph1.6h above. A DD 254, DoD Contract Security Classification Specification, is required for all classified contracts. Completion of localized security training (information protection related material) will be accomplished at the Wing/Unit level. Derivative Classification and Marking Classified CBTs may also be required as per assigned duties (i.e., SIPRNet).

b. AFNet, Supply Chain, & Data Sovereignty

The entire system offered must be actively listed on the Air Force Approved Product List (APL). Furthermore, all equipment must be successfully vetted through the Defense Intelligence Agency (DIA) Supply Chain Risk Management (SCRM) process. To ensure strict data sovereignty, the system warranty must include a "Keep Your Drive" provision where failed drives will not be returned to the vendor.

7 Schedule, Work Hours & Execution

To minimize mission impact, all execution must adhere to a strict operational schedule:

a. Work Hours & Holidays

All on-site work must be performed during normal operational hours, defined as Monday through Friday, 0700 to 1630 (7:00 AM to 4:30 PM) local time. No work shall be performed on observed Federal Holidays unless explicitly pre-authorized in writing by the Contracting Officer (KO) and coordinated with the SSO.

b. Execution Window & Work Planning

All on-site execution, including tear down, rebuild, testing, training, and final hand-off, must be completed *within thirty (30) days* following the documented receipt of all physical hardware. Prior to the commencement of this 30-day window, the contractor must submit a formal Work Plan detailing daily milestones, SCIF coordination steps, safety measures, and lead time accounting.

8 Deliverables, Testing & Quality Assurance

The contractor must validate the system's operational readiness and provide formal documentation prior to hand-off:

a. Quality Control & System Testing

The contractor shall implement a Quality Control Plan (QCP) to govern the installation, ensuring all hardware and network integrations meet OEM specifications and AFNet standards. Comprehensive system testing, including HA failover, DR validation, and load

testing must be conducted, with results documented and provided to the Government for User Acceptance Testing (UAT).

b. Operations & Maintenance Manuals

Upon final hand-off, the contractor must deliver complete, site-specific Operations and Maintenance (O&M) Manuals that include detailed architectural diagrams and administrative procedures.

9 Contracting & Regulatory Compliance

The contractor must maintain full compliance with federal acquisition standards:

a. Subcontracting Opportunities

In accordance with Section 8(d) of the Small Business Act (15 U.S.C. § 637(d)), the contractor shall agree to carry out the policy that small business concerns, veteran-owned, and minority-owned businesses shall have the maximum practicable opportunity to participate in the performance of contracts let by any Federal agency. If the contract exceeds the regulatory threshold, a formal Subcontracting Plan may be required.

b. SAM Registration

In accordance with the Federal Acquisition Regulation (FAR), all prospective contractors must be registered and maintain an active status in the System for Award Management (SAM.gov) database prior to the award of any federal contract, basic agreement, basic ordering agreement, or blanket purchase agreement.