City of Rockville

INet Switching

Design / Implementation SOW

Statement of Work

Date: July 23rd 2025

DSI Engineer:
Satish Rayanki

Client:
City of Rockville

Contents

1) Document Control

Preparation

Action	Name	Role / Function	Date
Prepared by	Satish Rayanki	Senior Network Engineer	07/23/2025

Release

Version	Date Released	Change Notice	Pages Affected	Remarks
1.0	11-8-2023	Initial Release	All	None

Distribution List

Name	Organization	Title
	City of Rockville	

Approvals

Name	Title	Date	Version	Organization
[Name]	[Job Title]	[mm/dd/yyyy]	[Version #]	[Organization]

2) Introduction

This Statement of Work ("**SOW**") is entered into on 11/8/2024 (the "Effective Date") by and between Disys Solutions, Inc. ("**DSI**"), a Virginia corporation, located at 44670 Cape Court, Suite 100, Ashburn, Virginia 20147 and City of Rockville ("**Client**"), located at 111 Maryland Ave, Rockville, MD 20850. System and product names described in this document are not always accompanied by their trademark symbols (™, ®). All other trademarks are the property of their respective owners.

3) Proprietary and Confidential

This Statement of Work (SOW) includes data that shall not be disclosed outside of [Client] and shall not be duplicated, used, or disclosed - in whole or in part - for any purpose other than to evaluate this proposal or quotation. If, however, a contract is awarded to DISYS Solutions Inc. (DSI) as a result of, or in connection with, the submission of this data, the client shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Client's right to use information contained in this data if it is obtained from another source without restriction.

4) Definitions

- **Deliverable:** For the purposes of this SOW, the term 'deliverable' refers to one specific work product that is the outcome of the engagement. Collectively, deliverables are the product for which the price of this SOW is exchanged. Services or activities (work) will be performed as a part of this SOW in order to produce the deliverables (work product).
- **Documentation:** The terms 'document' and 'documentation' as they relate to this SOW are intended to mean any notes, charts, graphs, diagrams, report outputs, network addresses, passwords, configuration logs, or any other discretionary information deemed by DSI to be relevant to this effort. Documentation is not intended to be, or considered to be, complete, comprehensive, or exhaustive as it relates to the overall Client network or information systems environment. Any documentation provided as a part of the execution of this SOW will be limited to systems, items, or topics specifically referenced in this SOW.
- **Knowledge Transfer:** The term 'knowledge transfer', as it relates to this SOW, is intended to mean conversational discussions about various technical aspects of this effort. Knowledge transfer is not intended to be, expected to be, or considered to be complete, comprehensive, or exhaustive as it relates to the overall Client network or information systems environment. Additionally, knowledge transfer is not intended to replace the need for formal instruction or vendor-supplied training in the operation of any systems installed or configured as part of this SOW.
- **Training:** Unless otherwise specifically stated in this SOW, DSI supplied training is not intended to convey any formal certification or credential and is provided on a 'best effort' basis as a courtesy to the Client.
- **Best Effort:** The term 'best effort' as it relates to this SOW is intended to mean services provided by DSI to the Client with no express warrantee or guarantee implied. A particular outcome of best effort service is not guaranteed, but every effort will be made to ensure the best result possible within the time allowed and with the resources available.
- **IN SCOPE:** The work described in the Activities section of this document, and effort toward the fulfillment and delivery of items described in the Deliverables section of this document are considered to be 'IN SCOPE' as they relate to this effort. The contents of the Assumptions sections of this document provide specific clarification of the scope.
- **OUT OF SCOPE:** Any items, components, materials, efforts, objectives, tasks, or services not described in either the Activities or Deliverables section of this document are considered 'OUT OF SCOPE' as they relate to this effort. OUT OF SCOPE work will not be performed without written authorization by the Client via the project change control process described herein.
- **Testing, Validation, Verification:** The terms 'testing', 'validation' and 'verification' refer to the process of comparing measurements and observations of specific information systems to Client provided expectations or criteria. The Client is responsible to confirm that tests, validation, or verification is successful.

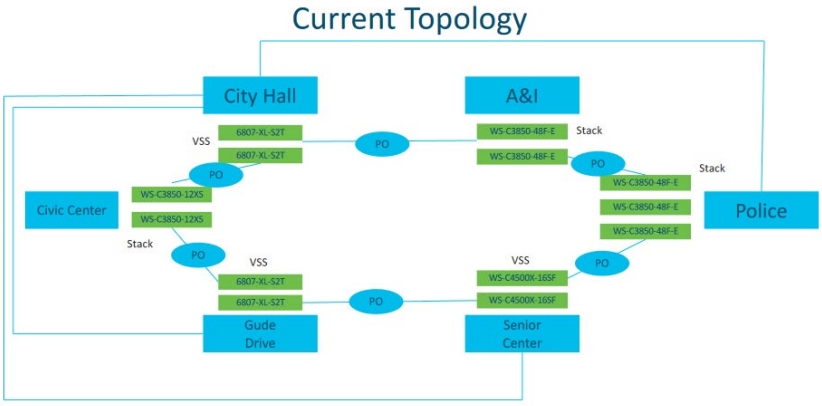
- **Client:** means entity who is authorized to receive or use the service or solution described in this SOW.
- **Normal Business Hours:** are Monday-Friday, 8:00am to 5:00pm local time excluding state, local and national holidays.
- **Milestone:** A specific goal, objective, or event pertaining to services described under the terms of this SOW.
- **Site Survey:** An assessment by partner of the readiness of the client site for the implementation of the product as further defined below.
- **Staging:** The assembly and software loading of product prior to Installation at client site.

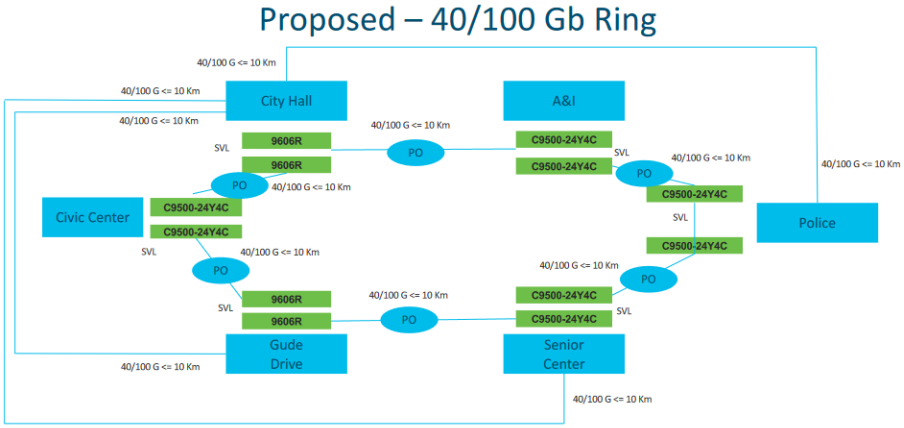
5) Scope

The purpose of this project is to enhance the current network infrastructure by addressing end-of-support equipment, increasing bandwidth capabilities, and optimizing the network design to support future scalability and performance. Specifically, this initiative aims to:

1. **Replace Last Day of Support (LDoS) Equipment**:
    - Propose new, high-performance Cisco Catalyst 9610 and 9500 series switches to replace existing LDoS equipment in the network.
    - Ensure that all equipment is up-to-date and supported by the manufacturer to maintain reliable operations, facilitate ongoing maintenance, and support advanced features in line with modern network requirements.
2. **Upgrade Bandwidth Between Locations**:
    - Enhance inter-site connectivity by upgrading the bandwidth from 10 Gbps to 40 Gbps or 100 Gbps, depending on specific site requirements and projected data demands.
    - Improve overall network performance to support data-intensive applications, minimize latency, and provide greater capacity for future network expansions.
3. **Optimize Network Design by Separating End Devices from Core/Distribution Equipment**:
    - Redesign the network topology to prevent end-user devices from connecting directly into Core/Distribution equipment, thereby reducing congestion, simplifying troubleshooting, and strengthening network security.
    - Implement a dedicated Access layer for end-user connections, isolating critical Core/Distribution functions and enhancing network segmentation and resilience.

By accomplishing these goals, this project will create a modern, scalable network infrastructure capable of handling increased data flows and supporting current and future organizational needs. A list of network devices that will be worked upon, updated, and/or upgraded are included in *"Inventory county by location.xlsx*" document.





Note: The Model as been changed and will be using the devices in the latest BOM, C9606 to C9610

1. Preparation and Planning for Each Site

- **Site Survey**: Conduct a detailed site survey to understand the current network layout, rack space, power, cabling, and other environmental factors.
- **Pre-Installation Checklist**:
  - Review the current network topology and gather details on existing switch configurations.
  - Prepare equipment lists for Catalyst 9610 and 9500, along with necessary cabling, transceivers, and accessories.
  - Verify VLAN, IP addressing, and other network design requirements.
- **Migration Plan**:
  - Develop a migration plan for each site, detailing cutover steps, expected downtime, and rollback procedures.
  - Define a schedule with stakeholders to minimize operational impact.

2. Hardware Installation: Rack and Stack

- **Physical Installation**:
  - Position Catalyst 9610 and 9500 switches in designated racks, ensuring proper airflow and clearance.
  - Secure switches using rack-mount kits and cable management accessories as needed.
  - Power up the switches, checking power redundancy if applicable.
- **Cabling**:
  - Connect power cables to redundant power sources if available.
  - Connect network cables (fiber or copper) as per the topology, ensuring proper connectivity to existing infrastructure.

3. Software Configuration

- **VSS Configuration (if applicable)**:
  - Configure Virtual Switching System (VSS) between the Catalyst switches to enable redundancy and high availability.
  - Configure Virtual Port Channels (VPC) or Link Aggregation for trunk and uplink connections.
- **Initial Setup**:
  - Set up device management IPs, hostname, and login credentials.
  - Configure base settings such as SNMP, logging, NTP, and AAA.
  - Install the latest IOS-XE version as required and verify feature compatibility.
- **Layer 2 and Layer 3 Configuration**:
  - Configure VLANs, IP routing, DHCP settings, and other necessary features per the design.
  - Set up routing protocols replace EIGRP with BGP as applicable, ensuring correct neighbor relationships and path selection.
  - Netflow configuration

4. Migration Steps

- **Pre-Migration Testing**:
  - Confirm connectivity to Catalyst switches from management devices and verify baseline metrics.
- **Traffic Migration**:
  - For each site, migrate connections from old switches to Catalyst 9610 and 9500 in a phased manner.
  - Validate L2/L3 configurations on the Catalyst switches align with previous switch configurations.
  - Carefully monitor traffic and connectivity for critical applications during the migration.
- **Decommissioning Old Switches**:
  - Once migration is complete, decommission old switches as per company policy or re-purpose them as necessary.
  - Remove physical connections and update documentation to reflect the new topology.

5. Testing and Validation

- **Post-Migration Connectivity Testing**:
  - Perform end-to-end connectivity tests to confirm that all services and applications function as expected.
  - Verify VSS failover functionality and redundancy to ensure high availability.

- Test key network services (DNS, DHCP, Internet, and internal applications) for proper connectivity and performance.

- **Performance Verification**:
  - Monitor switch performance (CPU, memory, interface utilization) to confirm stable operation.
  - Conduct a network load test, if feasible, to validate performance under typical load conditions.

6. Documentation and Knowledge Transfer

- **Documentation**:
  - Update network diagrams, IP address maps, and device inventories to reflect the new setup.
  - Record all configurations and make them accessible to the network operations team.
- **Knowledge Transfer**:
  - Provide an overview of the new setup, explaining key changes and features.
  - Train relevant team members on how to manage and troubleshoot the Catalyst switches.

7. Day 2 Support

- **Monitoring**:
  - Set up network monitoring tools to continuously monitor switch health, performance, and critical alerts.
  - Implement automated notifications for potential issues (CPU spikes, link failures, etc.).
- **Support and Optimization**:
  - Offer remote or on-site support for any initial post-installation issues.
  - Perform routine checks during the first week to ensure stable operation.
  - Fine-tune configurations as needed based on performance data and user feedback.

Security – Firewalls, FMC, ISE, FTD

Scope

- Migrate VLANs to VRFs/firewall zones
- Reconfigure multi-instance Firepower deployments
- Consolidate FMC policies
- Upgrade FMC, FTD, and ISE to the latest which we are working on implementation.

- Migrate the Firepower Management Center (FMC) from the Senior Center to Equinix.
- Upgrade Cisco ISE to the latest supported version and best practices IE: install/update endpoint authentication certificates to ensure compatibility and secure onboarding of end devices and AAA and Dot1X
- Upgrade all Firepower Threat Defense (FTD) appliances and FMC to the latest Cisco-recommended version at the time of implementation.

Deliverables

- Hardened FMC policies across all sites
- Multi-instance Firepower setup for Police and Equinix
- ISE patching and DAC implementation
- Gold image upgrades for FMC/FTD

Multi-Instance Firepower Deployment

Scope

- Design and implement multi-instance architecture for FPR 4215/4125 Deliverables
- Instance provisioning and resource allocation
- Routing and segmentation per instance
- HA validation and failover testing

Note: All changes and upgrades will be assessed in alignment with Cisco security advisories and published vulnerability bulletins. No major architectural redesigns are anticipated. The scope of work will primarily focus on repurposing the existing external firewalls for a multi-instance deployment—creating one instance to secure internal traffic and another for external perimeter control. Existing firewall policies will be retained and supplemented with additional rules to enhance the overall security posture.

Switching (Cisco Devices)– VLAN, OSPF, Failover, Segmentation

EIGRP to OSPF

Pre-Migration Checklist

- Identify all routers running EIGRP per Each Site
- Document current EIGRP neighbors and route tables
- Confirm OSPF design (areas, router roles, DR/BDR logic)

- Plan redistribution if needed (during transition)

Migration Steps

1. **Deploy OSPF in Parallel**
    - Configure OSPF on all routers without removing EIGRP
    - Use higher AD for OSPF (default 110) to avoid route takeover
2. **Verify OSPF Adjacencies**
    - Use show ip ospf neighbor and show ip ospf database
    - Confirm DR/BDR elections on multi-access segments
3. **Redistribute EIGRP into OSPF**
4. **Redistribute OSPF into EIGRP**
5. **Switch Routing Preference**
    - Lower OSPF AD or remove EIGRP
    - Monitor route tables (show ip route)
6. **Clean-Up**

- Remove EIGRP configs
- Validate OSPF convergence and failover

Configuration or Verification:

Access Control

- Disable unused ports (shutdown)
- Enable **port security** with MAC limits
- Use **AAA with TACACS+/RADIUS**
- Restrict VTY access with ACLs:

Management Plane

- Enable SSH, disable Telnet
- Use secure SNMPv3
- Configure logging:

logging buffered 4096 logging host

🔧 Control Plane

- Enable **BPDU Guard**, **Root Guard**, **Loop Guard**
- Disable CDP/LLDP if not needed
- Use **storm control** on access ports

- DOT1x configuration verification

- **Dynamic ARP Inspection (DAI) and IP Source Guard and DHCP Snooping, CoP, OSPF deployment and all other configurations will be set up as per Cisco Best practice.**

Design and implement a guest network that is segmented from the main network and isolates guest devices from each other, providing only internet access.
Design and implement a dedicated imaging segmented network that is segmented and isolated from the main production network, intended solely for imaging devices and related infrastructure.
Design and implement new IoT network that is segmented both from the main network and internally among its own devices.
Migrate VLANs from the core switch to the designated data center switches to align with the updated network architecture.
Design and implement new IoT network that is segmented both from the main network and internally among its own devices.
Migrate VLANs from the core switch to the designated data center switches to align with the updated network architecture

Note: All changes and upgrades will be assessed in alignment with Cisco guidelines and advisories and published vulnerability bulletins. No major architectural redesigns are anticipated. The scope of work will primarily focus migrating to OSPF and Layer 2 hardening with industry standard configuration with security in mind.

Active Directory – AD Connect, LAPS, O365

AD Connect – Hybrid Identity Synchronization

Scope

- Synchronize on-premises AD with Microsoft Entra ID (Azure AD)
- Enable password hash sync or pass-through authentication
- Support hybrid join for Windows devices

Implementation Tasks

- Install **Microsoft Entra Connect** on a dedicated server
- Configure sync rules, OU filtering, and attribute mapping
- Enable **password hash sync** or **pass-through authentication**
- Validate sync health via Synchronization Service Manager
- Enable **password write-back** (requires Entra ID P1 or M365 Business Premium)

Microsoft LAPS – Local Admin Password Management

Scope

- Automatically rotate and store local admin passwords for domain-joined devices
- Store passwords securely in AD or Microsoft Entra ID
- Support Windows LAPS (native) or legacy LAPS (via MSI)

Implementation Tasks

- Extend AD schema with ms-Mcs-AdmPwd and ms-Mcs-AdmPwdExpirationTime
- Set permissions for computer objects to update their own attributes
- Assign read access to authorized admin groups
- Deploy LAPS client via GPO or endpoint management
- Configure GPO:
- Enable password management
- Set password complexity and expiration

Define managed admin account name

DUO Self Service Portal

Duo Self-Service Portal Offers

- **Device Management**: Users can add, rename, or remove authentication devices (phones, security keys, etc.).
- **Password Reset**: If a user's AD password is expired, Duo SSO prompts them to reset it after completing MFA.
- **Inline Enrollment**: New devices can be added during login via the Universal Prompt.

Cisco Catalyst Center, Nexus Dashboard, UCSX

Deploy and configure Cisco DNA Center Assurance to enable:

- Real-time and historical visibility into network, client, and application health and DR step up
- Telemetry-based troubleshooting and analytics
- Integration with Cisco ISE

Implementation Tasks

A. Platform Readiness

- Rack Stack and Initialize the two Cisco Catalyst Center at each Data Center
- Apply latest software patch (e.g., 2.3.7.x or newer)
- Configure DNS, NTP, SNMP, Syslog, and AAA settings
- Import trusted certificates for secure telemetry

B. Network Hierarchy & Device Discovery

- Create site hierarchy (areas, buildings, floors)
- Assign devices to sites for location-based insights
- Discover and onboard switches, routers and all supported devices

C. Assurance Configuration

- Enable Assurance services and telemetry collection
- Configure SNMP, NetFlow, and streaming telemetry

D. Integration (Optional)

- Integrate Cisco ISE for identity-based insights
- Configure pxGrid and API access for external tools

E. Validation & Testing

- Verify Assurance dashboards: Network Health, Client Health, Application Health, Device backup and system backup
- Run path trace and issue detection workflows
- Document baseline performance and visibility metrics

Deliverables

- DNAC Assurance configured and operational
- Devices assigned to sites with telemetry enabled
- Integration with ISE
- Admin guide for Day 2 operations and troubleshooting and Topology

- Set up and configure templates Cisco DNA Center. All supported Cisco devices should be integrated into these platforms for consistent policy enforcement, automation, and streamlined management.

NDFC (Network Services for Data Center)

Deploy Cisco NDFC as a microservices-based application on a physical Nexus Dashboard cluster to manage:

- LAN fabrics (VXLAN EVPN, Classic Ethernet)
- SAN fabrics (Cisco MDS)
- IP Fabric for Media (IPFM)
- Optional integration with Nexus Dashboard Insights and Orchestrator

Implementation Tasks

A. Hardware Preparation

- Rack and cable **ND-NODE-L4** appliances
- Configure CIMC and BIOS settings per Cisco guidelines

- Assign IPs for:
    - **Management interface (bond1br)**
    - **Data interface (bond0br)**
- Validate Layer 2/3 adjacency and RTT requirements (≤50ms between nodes)

B. Nexus Dashboard Cluster Formation

- Bootstrap 3-node cluster in **Active-Active HA mode**
- Apply latest ND software (e.g., ND 3.2+)
- Validate cluster health and microservices orchestration

C. NDFC Application Deployment

- Install NDFC 12.1.x or newer via Cisco App Store
- Select appropriate **persona**:
    - Fabric Controller (LAN)
    - SAN Controller (with or without SAN Insights)
    - IPFM Controller
- Configure service IPs and routing tables
- Validate pod health and service reachability

D. Fabric Onboarding

- Discover and onboard Nexus/MDS switches via OOB or IB management
- Define fabric topology, roles, and policies
- Configure POAP, EPLD/SMU upgrades, and telemetry

E. Integration & Automation

- Integrate with Nexus Dashboard Insights (NDI)
- Configure SNMP, Syslog, and NetFlow forwarding
- Set up and configure templates in Cisco Nexus Dashboard. All supported Cisco devices should be integrated into these platforms for consistent policy enforcement, automation, and streamlined management.

F. Validation & Testing

- Verify fabric health, device reachability, and policy enforcement
- Run config drift detection and baseline sync

- Document fabric topology and operational workflows

Security & Compliance

- Import trusted certificates for HTTPS and telemetry
- Harden appliance per Cisco ND/NDFC security guidelines
- Configure RBAC and audit logging (if needed)

Documentation & Handoff

- Architecture diagrams and IP schema
- Fabric onboarding guide
- Day 2 operations and troubleshooting playbook

CISCO UCSX

- Upgrade Cisco UCSX environment to the latest gold version to ensure compatibility, performance, and security at each Site.

Unified Communications – CUCM Hardening & Upgrade

Scope

- **Secure all Unified Communications servers (see attached inventory list) behind firewalls**
- **Apply VMware and Unified Communications security best practices**
- **Upgrade all Unified Communications servers (see attached inventory list) to the latest gold image version (version 15 as of this writing)**

Deliverables

- **Unified Communications firewall rules and segmentation**
- **VMware hardening checklist applied**
- **Unified Communications servers upgraded and validated**

PMO & Oversight

Please see section **7 (Project Management).**

6) Milestones

#	Milestone Task
1	Project Launch Workshop
2	Planning/Discovery/Design
3	Implementation Phase
4	Day 2 Support

7) Project Management

A dedicated DSI Project Manager (PM) will be assigned to oversee all aspects of this engagement. The PM will be responsible for scheduling, coordination, and support of DSI personnel assigned to the project, and will serve as the primary point of contact for all Client communications throughout the duration of the engagement.
The DSI Project Manager will provide structured reporting on a monthly basis. These reports will include:

- Hours consumed by each engineer
- Tasks completed, categorized by technology area
- Comparison of planned versus actual hours at the technology level
- Assessment of project progress, including trend analysis to determine if the project is on track, ahead, or at risk

This level of transparency will enable the Client and DSI to jointly monitor progress, manage scope, and make informed decisions as needed. Hours for this engagement are considered flexible. With appropriate coordination and approval, the customer **(CoR) may reallocate unused or remaining hours across technology areas or phases of the project based on evolving priorities.**
The project may include the following phases and activities, subject to project scope, complexity, and duration:

1. **Project Kickoff Meeting / Workshop**
    - Introductions of key stakeholders and team members
    - Overview of project objectives, scope, and deliverables
    - Review of initial project schedule and milestones
    - Documentation of action items and follow-ups
2. **Initial Project Planning**
    - Definition of escalation paths and communication protocols
    - Identification of preliminary schedule and task sequencing
    - Establishment of an estimated project completion date
3. **Ongoing Project Status Meetings** (for engagements exceeding two weeks)
    - Review of project status and key milestones
    - Discussion of issues, risks, and mitigation plans
    - Tracking of open items and follow-up actions
    - Identification of any scope or schedule deviations that may require a formal Change Order
4. **Project Closeout**
    - Final review of deliverables and milestones
    - Documentation and resolution of any outstanding issues

- Agreement on project completion and acceptance criteria

DSI is committed to ensuring successful project delivery through proactive management, clear communication, and accountability.

8) Deliverables

Some or all of the listed documentation may be included as part of the delivered services.

a. Services identified in Section (5) Scope of Work
b. Review of findings and recommendations

9) Client Responsibilities

In the delivery of the service, the Client responsibilities will be to provide where applicable:

a. Any supporting documentation such as building drawings/schematics/blueprints of Client site(s), network diagrams, configurations in electronic format;
b. Remote Access to network(s) if necessary
c. Any necessary escort personnel for DSI staff;
d. Any necessary access, passwords, and visibility to all network devices configuration and security information
e. Approval for digital photography
f. On-site access to all required areas and rooms, including secure and sensitive areas as necessary to perform the assessment
g. Access to ladders, lifts and other available equipment, when required, for wireless network assessments
h. Designation of individuals as primary Project and engineering contacts
i. Access to key knowledge personnel
j. Downtime window for upgrade
k. Provide rackspace, power for new devices
l. Provide VPN access and login to datacenter switches.

10) DSI's Responsibilities

In the delivery of the service, DSI's responsibilities will be to provide:

a. Trained and certified personnel to perform the activities identified in the Scope of Work Section of this document.
b. Provide any necessary tool(s) and related technologies essential to perform activities identified in the Scope of Work Section of this document.
c. Maintain client confidentiality and information security

11) Assumptions

Below is a list of assumptions related to the execution of the activities for this Statement of Work. Some assumptions may vary depending on whether the activities are remote or on site.

a. Access to Client systems as required as part of the scope of work
b. Client Site(s) is accessible during project hours and there are no restrictions present to entering an area necessary for the Assessment
c. DSI will be provided with necessary Client escort personnel to gain access to any necessary locations that may otherwise be inaccessible for security reasons
d. Client will respond in a timely manner to requests for access to Client site(s), device login, configuration and security information. Any delays may cause delays in the agreed to timeline
e. Work will begin on an agreed schedule between the client, DSI PMO and DSI Sales.
f. Any changes to the design and equipment presented to the Client within this proposal and BOM will require a change order to the scope of work

g. All Client systems that will interface with the solution provided as part of these services will have manufacturer support in place. Additional charges may result if DSI is required to trouble shoot unsupported systems.
h. UCS B series is under valid SmartNet contract for contacting TAC as required.

12) Out of Scope

Any services that are not specifically detailed herein are excluded from the Services to be provided under this SOW.

13) Project Completion

This project will be considered complete when expected deliverables have been received by Client, as acknowledged and agreed to by the parties through a Project Completion form, in accordance with the procedures set forth in this paragraph. At the completion of the project, DSI will provide the Client with a Project Completion form. The Client will have 7 calendar days from the date of receipt of the Project Completion form either (i) to accept it by signing and returning it to DSI, or (ii) to articulate its objections in writing to DSI. If the Client does not timely provide DSI with written acceptance or objection(s) within the Seven (7) calendar day period, the Client will be deemed to have ACCEPTED the project and all associated deliverables without any further action by either party.

14) Pricing

Below is included in a separate quote.

15) Billing

Client will be invoiced monthly for services to date. If the project is completed prior to the end of the month, the final invoice will be submitted as soon as the project effort is complete. If billing milestones are established as part of the project, it will supersede monthly invoicing.

16) Change Order to Statement of Work

Requests by Client, which are outside the scope of this SOW are subject to a change order using the form in Appendix C.

17) SOW Acceptance

As a duly authorized representative, I hereby acknowledge, accept and authorize this statement of work.

Client

(SIGNED)	***(DATE)***
(PRINT NAME)	***(TITLE)***

This SOW will not be considered valid for execution unless signed by autorized agent of Client.

Appendix A

PROJECT COMPLETION CERTIFICATE

When the project is complete, DSI will request final acceptance of all services and deliverables from Client via the following project completion form:

PROJECT COMPLETION FORM
This document serves to confirm that the project has been completed and all of its deliverables have been met per the Statement of Work.

1. Project Name:
2. Client:
   - Client
   - Client Contact
   - Title
   - Address1
   - Address2
   - City, State, Zip
   - Phone number
   - Email Address

3. Project Number: DSI Internal Use	4. Phase(s) to be Billed: Specific phase(s) billed

Summary of Deliverables:

☐ First Deliverable
☐ Second Deliverable
☐ Third Deliverable
☐ Additional Deliverables…
Note: Please provide total project hours

5. Acceptance

PROJECT COMPLETION DELARATION:

The Client project team has received and reviewed all expected deliverables of the project, accepts all the services provided, and considers the terms of the SOW fulfilled. Client authorizes DSI to invoice any outstanding balance for services rendered.

Signature: SAMPLE – DO NOT SIGN

Title: SAMPLE – DO NOT SIGN

Date: SAMPLE – DO NOT SIGN

Appendix B

Satisfaction Survey

To ensure we are providing service excellence please take a moment to fill out the survey below and return it to the DSI Project Manager assigned to the project.

Overall, I am very satisfied with the way DSI performed this project.
☐ Strongly agree ☐ Agree ☐ Neutral Disagree ☐ Strongly Disagree

Overall, I am very satisfied with the scheduling of this project.
☐ Strongly agree ☐ Agree ☐ Neutral Disagree ☐ Strongly Disagree

Overall, I am very satisfied with the level of communication during this project.
☐ Strongly agree ☐ Agree ☐ Neutral Disagree ☐ Strongly Disagree

Overall, I am very satisfied with the Project Management on this project.
☐ Strongly agree ☐ Agree ☐ Neutral Disagree ☐ Strongly Disagree

Overall, I am very satisfied with the Engineering effort on this project.
☐ Strongly agree ☐ Agree ☐ Neutral Disagree ☐ Strongly Disagree

Overall, I am satisfied with the DSI account manager.
☐ Strongly agree ☐ Agree ☐ Neutral Disagree ☐ Strongly Disagree

Compared to how you felt about DSI before this project, what is the likelihood of completing another project with DSI?
☐ Better, based on Performance ☐ About the same ☐ Worse, based on performance

Based on your experience, how likely would you be to recommend DSI?
☐ Definitely will ☐ Probably will ☐ About the same ☐ Probably will not ☐ Definitely will not

Additional comments:

Appendix C

PROJECT CHANGE ORDER

Throughout the project it may be necessary to amend this scope of work or request approval for additional project related costs. Such requests will be submitted to Client via the following project change order.

PROJECT CHANGE ORDER

1. Project Information

1. **Project Name:**
2. **Account Manager:**
3. **Project Manager:**
4. **Client Sponsor:**
5. ***Governing SOW:*** This change request shall serve as an extension of service SOW 'Statement of Work for Storage Assessment executed between DSI and Client on [DATE].

2. Change Request

2.1. Change Description

Details of changes requested

2.2. Change Description:

2.3. Change Justification:

2.4. Change Impact

2.4.1. Effective Date:

2.4.2. Estimated Duration:

2.4.3. Estimated Cost:

3. Acceptance

Client ACCEPTANCE OF PROPOSED CHANGE:

The Client project team has reviewed and accepts the proposed change to the project scope and modification of the terms of the governing SOW.

Signature:	SAMPLE – DO NOT SIGN
Title:	SAMPLE – DO NOT SIGN
Date:	SAMPLE – DO NOT SIGN

Appendix D

Additional Supporting Information