Amendment Number 4 to
The Master Services Procurement Agreement

This Amendment Number 4 (this "Amendment") to the Agreement (as defined below) is entered into as of 8/8/2024 , 2024 by and between **Avangrid Management Company** ("Customer") and [redacted] ("Supplier"). Capitalized terms used and not otherwise defined herein shall have the meaning ascribed to them in the Agreement.

RECITALS:

WHEREAS, Customer and Supplier are parties to a Master Services Procurement Agreement dated June 1, 2020, as modified by Amendment 1 dated February 10, 2022, Amendment 2 dated February 22, 2023, and Amendment 3 dated February 26, 2024 (as amended to date, the "Agreement"); and

WHEREAS, the parties desire to enter into this Amendment Number to reflect changes to the Agreement as are set forth herein.

NOW THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties agree as follows:

A) **Schedule B, "Services, Warranty, Deliverables, and Vendor Requirements"** to the Agreement is hereby amended to also include Schedule B-1, attached hereto and incorporated herein solely for the purposes of Avangrid Secure Domain Information and Communication Technologies project ("ASD ICT").

B) **Schedule D," Pricing Terms"** to the Agreement is hereby amended to also include Schedule D-4 attached hereto and incorporated herein solely for the purposes of ASD ICT.

C) **Schedule H, "Data Security Rider"** to the Agreement is hereby amended to also include Schedule H-1, attached hereto and incorporated herein solely for the purposes of ASD ICT.

D) **A new schedule titled "Avangrid Contractor Safety Requirements" is hereby added to the Agreement in the form attached hereto as Schedule J.**

E) All references in the Agreement to defined terms shall be deemed to refer to such terms as such terms have or may have been amended, modified, or supplemented by this Amendment.

F) Except as expressly amended by this Amendment, the Agreement shall remain unchanged and in full force and effect and the parties hereby ratify and confirm the Agreement and each of its obligations.

G) Any conflict or inconsistency between the Agreement and this Amendment shall be resolved in favor of this Amendment.

H) This Amendment shall be governed by and construed in accordance with the laws of the State of New York without regard to its conflict of laws principles.

I) This Amendment may be signed in any number of counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

[Signature page(s) follow]

IN WITNESS WHEREOF, the parties hereto have each caused this Amendment to be executed as of the date first set forth above.

Avangrid Management Company

By:__[redacted]
Name[redacted]
Title:[redacted]
Date:__8/5/2024

Avangrid Management Company

By:__[redacted]
Name:[redacted]
Title:_[redacted]
Date:__8/8/2024

[redacted]

DocuSigned by:

By:[redacted]
Na[redacted]
Titl[redacted]
Date: 7/23/2024

[redacted]

SCHEDULE B

Services, Warranty, Deliverables, and Vendor Requirements.

Avangrid Networks

Operational Smart Grids - Cyber Assurance and Compliance

June 2024

Statement of Work for the Contract of Cyber Assurance and Compliance

Infrastructure and Communication Technology Services and Technical Resources

Contractor Skillset Based Work

- Contractor shall have the qualifications, knowledge, skill sets, industry expertise, and tools necessary to carry out all the tasks defined in this statement of work. Regarding software and infrastructure, Customer will provide the necessary systems and infrastructure to perform the requirements associated with the role.
- Contractor shall have the necessary certifications and qualifications that prove the related knowledge and experience on the different Contractor's equipment used within the Customer's ASD ICT environment.
- Contractor shall provide sufficient, competent, and qualified individuals to satisfy the staffing requirements and deliverables for the ASD ICT requirements. The work shall be performed, completed, and managed at the locations as directed by the Customer. Customer shall have the ability to directly contact Contractor without any authorization or approval from Contractor.
- Contractor shall provide staff with the following staffing competencies and qualifications associated with the specific role:
  - •Be properly trained in all aspects associated with their roles.
  - •Be properly trained and be able to determine and maintain an optimal balance of functionality, operability, reliability, interoperability, Quality of Service, and optimize field performance to minimize total cost for mobilization, technical services, and related installation materials.
  - •Maintain compliance with all current and known NERC/CIP, Legal, Security, OSHA, IBEW, and industry regulatory requirements, and licensing requirements.

Conditions for the execution of the services

- Contractor shall attend all meetings scheduled by Customer in Rochester and Binghamton NY, Augusta ME., Orange CT., and Pittsfield MA.
- Contractor shall cause its personnel and the personnel of any subcontractors to cooperate with Customer's internal teams and other technical contractors including Customer's Health and Safety department, as reasonably requested by Customer, to provide to Customer, and other service-

related contractors, reasonable access to personnel, systems, and facilities to the extent they relate to activities specifically associated with these technology services. Contractor shall not interfere with or jeopardize the safety or operation of the systems, personnel, or facilities provided Contractor receives reasonable prior written notice of such request.

- Contractor shall provide, and update Customer on any changes to its organizational chart, indicating lines of authority for personnel and their contact information, who are involved in the performance of any work in this Agreement. The chart must indicate who within the organization has the prime responsibility and final authority for the work.
- Contractor shall indicate to Customer the relationship personnel have with other programs or functions of the Contractor's organization that support Customer's work.
- Contractor must certify to Customer that the use of the proposed subcontractor is NERC CIP compliant. Customer reserves the right to recommend, approve, or reject any proposed subcontractor. Background checks will be required and available upon request.
- Contractor shall certify to Customer that personnel identified in this Statement of Work will perform the assigned work, including field documentation work and data collections as part of the Statement of Work. Where Contractor substitutes any personnel, Contractor shall notify Customer or Customer's assigned project manager.

GENERAL REQUIREMENTS FOR THE CONTRACTOR

- Contractor shall attend meetings in all operating areas identified, as scheduled by Customer's assigned project manager.
- Customer shall have the ability to directly contact Contractor. Contractor must have the ability to meet via Microsoft Teams, and onsite following required Company safety policies and guidance.

Warranty

- Contractor or Customer shall not request final system acceptance until all such items have been completed and the entire system is "turned up" for use and functioning for 30 days consistently without service interruption, or at Customer discretionary submission written approval. Customer shall verify and approve all required system acceptance items before issuing a final system acceptance and commencement, invoicing, and initiation of warranty services.

Deliverables

- The ICT Technology Services Contractor work efforts for project specific work must result in a fully deployable, tested, accepted, functional, and operational end state, complete with close-out documentation as specified for all system, and subsystem network elements combined to function as one holistic system and as defined in the Statement of Work. This includes the transfer of all related files (in Customer-required formats). Customer shall not accept or allow any partial or limited technology work packages, resulting in incomplete installations, repairs, or deployments. A "System" is defined as the primary equipment, subsystem elements, feasible and validated result-oriented installation construction packages including software, incidental hardware, and materials, that are combined into an integrated system. The System is described by means of a document, or other technical and implementation documents for deployment, installation, construction, integration, maintenance, or service by Customer, or qualified and competent Customer contractors. Customer shall approve documentation for completeness and accuracy. Parties shall

not assume that work performed, is accepted until work is fully validated resulting in full operational functionality as intended.

- Contractor shall deliver to Customer all design work and complimentary documentation for review and approval not later than 30 days after the agreed upon deadline.

Quality and Validation Testing

- Contractor shall first perform all required quality assurance activities to verify that the physical deliverable or service is complete prior to delivering any of the above-mentioned physical deliverables or technology services.
- Contractor shall certify to Customer before delivering a physical deliverable or service, that:
  - it has performed such quality assurance activities,
  - it has performed any applicable testing,
  - it has corrected all material deficiencies discovered during such quality assurance activities and testing,
  - the Deliverable or Service is in a suitable state of readiness for Customer's review and approval, and
  - the Deliverable/Service has all critical firmware, software, and security patches/updates applied, or noted for configurations to be completed.
- If a Deliverable includes installation at Customer location, then Contractor shall:
  - perform any applicable testing,
  - correct all material deficiencies discovered during such quality assurance activities and testing.
  - inform Customer that the deliverable is in a suitable state of readiness for Customer's review and approval.
- Customer may inspect the deliverable/service to confirm that all components of the deliverable/service have been delivered without material or other notable deficiencies, prior to commencement of its review or testing the deliverable/service. Contractor shall not assume acceptance without Customer's formal written approval.
- If Customer determines that, the deliverable/service has deficiencies, deficiencies identified by Customer, may be in the form of proposed cost, and implementation practicality. Customer may refuse delivery, or acceptance of the deliverable/service without performing any further inspection or testing of the deliverable/service. Customer and Contractor must agree that the deliverable/service is ready for use, is a cost-effective and efficient design to implement, and, where applicable, is certified by both Customer and Contractor for compliance related to the achievement of installation, implementation, and integration goals.
- Customer shall be entitled to observe or otherwise participate in planning, deployment, and testing activities to the extent that planning, deployment, or testing occurs at Customer locations.
- Contractor shall deliver all Test and turn-up documentation from the resulting work package implementation to Customer departments within 72 hours for review.
- Customer shall have the right to review the information and to request reasonable changes to clarify the provided information and operational functionality of the solution, including design and cost efficiencies.

- Customer shall have final approval authority of the documentation, and such approval shall be in a written form.
- Customer shall not approve any invoice until all required documentation is delivered, as well as the required design, including recommended changes, or cost analysis has been completed.
- All system(s) that reach out to remote elements must demonstrate connectivity to one or more remote target elements before final acceptance.
- Final design for System Design Acceptance and commencement of warranty services shall not begin until the Contractor has successfully completed all functional testing; delivered all required services; completed all agreed-upon efforts; and supplied all system documentation and as-built drawings; per this SOW, contract documents, and design documents, where applicable.
- All required System Acceptance items must be verified and approved by Customer shall verify and approve all required System Acceptance items prior to issuing Final System Acceptance and commencement, invoicing and initiation of warranty services.

Deliverable approvals / denials

- Customer shall approve in writing a deliverable/service upon confirming that it conforms to and, performs in accordance with, its specifications without material, performance, or cost efficiency deficiencies where applicable.
- Customer may, conditionally approve in writing a deliverable/service that contains notable deficiencies if Customer elects to permit Contractor to rectify them post-approval.
- Contractor shall work diligently to correct within 15 calendar days any deficiencies, costs and efforts will be performed at Contractor's expense, and all deficiencies noted in the deliverable/service that remain outstanding at the time of Customer's approval. Contractor will be required to remediate the problem at no cost to Customer.

Sustained Deliverable Deficiencies

- Customer may halt the testing or approval process if such process reveals deficiencies in or problems with a Deliverable/Service in a sufficient quantity or of a sufficient severity as to make the continuation of such process unproductive or unworkable.
- Customer may stop using Contractor's services or return the applicable deliverable to the Contractor for correction and re-delivery prior to resuming the testing or approval process.

Final Acceptance

- Unless otherwise stated in the Purchase Order, "Final Acceptance" of each Contractor services deliverable shall occur when each deliverable/service is approved by Customer 30 days after test and turn-up of services is completed.

Unitization Scope

- Contractor shall comply with Customer's standards and National (IEEE/ANSI/ACI) standards as well as local, state, city, and federal law requirements and guidelines for all scope of work. These include all necessary preparations for civil, environmental, aeronautical, and all required preliminary investigations and authorization.

- Contractor work must result in a fully deployable, tested, accepted, functional, and operational end state, complete with close-out documentation as specified for all system, and subsystem network elements combined to function as one holistic system, where applicable. This includes the transfer of all related files (in Customer required formats) in support of invoicing for specific efforts.
- Contractor shall deliver to Customer all ICT Technology design works and complimentary documentation for review and approval not later than 30 days after the agreed-upon deadline.

Systems/Applications

The following is a list of applications and systems that the Contractor will be required to support:

Application Name	Modules
Active Directory	Active Directory
Agent VI Innovi	Agent VI - Video Analysis
AMAG	PACS - Symmetry Connect
AMAG	PAC - AMAG Summary
Barco	Barco/VDI/Role Templates
Barco	OP Space KVM
Centrify	Centrify - PIM password vault (Session Audit & Access Restrictions)
Check Point	Firewalls - Checkpoint
Check Point	Check Point Smart Center
Ciena	Management platform: Ciena MCP
Cisco	LAN Cisco Network Switches
Cisco	Cisco ISE Network Access Control (NAC) - (Radius and TACACS included as part of Cisco ISE)
Cisco	NMS - Cisco Prime
Clearcube	Clearcube
Commend (Virtuo SIS)	VirtuoSIS - Intercom Solution
Gigamon	Gig-VUE-FM
Gigamon	Giga-VUE-VM
IT Interconnect	IT Interconnect
IT Interconnect - Meet-Me-Point	Meet-Me-Point
IronNet	IronDefense
IronNet	IronDome
Liquidware Stratusphere UX	Liquidware Stratusphere UX
LockPath (GRC)	Audit Manager
LockPath (GRC)	Compliance Manager
LockPath (GRC)	Risk Manager
LockPath (GRC)	Security Manager
LockPath (GRC)	Vendor Manager

Application Name	Modules
LogRhythm PM7400 (SEIM)	LogRhythm (Security Analytics)
Microsoft DNS Server	Microsoft DNS Server
Microsoft File Server	Microsoft File Server
Microsoft KMS	Microsoft Key Management Server
Microsoft PKI	Microsoft PKI (Certificate Authority)
Milestone - Video Surveillance	VIDEO Surveillance
Milestone - Video Surveillance	Xprotect Smart Client
MS SQL	MS SQL 2014 & 2015
Netscaler MPX	Netscaler MPX
Nokia	WAN Network Solution - NOKIA
Nokia	WAN NMS - Nokia NSP (SAM)
Nokia	WAN Network Solution - NFM - T
Owl CyberDefense	ReCon & SSUS
Owl File Transfer System	RFTS
Pivot 3	HCI Servers & Virtualization
Rational	IBM Rational Quality Manager
Rational	CCM
Red Hat	Red Hat Enterprise Linux
Repo Server	Repo Server (File Transfer Mgmt)
Shooter Detection	Shooter Detection (The Guardian Indoor Gunshot Detection System)
SolarWinds	SolarWinds - Help Desk
Solar Winds	SolarWinds - Patch Manager
Solar Winds	SolarWinds - Orion (APM)
Tenable	Security Center (Tenable Continuous View) - Vulnerability Management
Tenable	Nesus Network Monitor (NNM) - Network Passive Vulnerability Scanner
Tenable	Log Correlation Engine (LCE) - Nessus SIEM
Tenable	Nessus Scanner - Nessus Vulnerability Management
TrendMicro TP	TrendMicro Tipping Point
TrendMicro	TrendMicro SafeLock
TrendMicro	End-Point Protection
TrendMicro	Advanced Threat Protection
TrendMicro	Analyzer
TrendMicro	Deep Discovery
TrendMicro	Deep Discovery - HIPS ATP
TrendMicro	Deep OfficeScan
TrendMicro	Deep Security
TrendMicro	Vulnerability Protection for Endpoints

Application Name	Modules
Virtual Desktop Infrastructure (VDI)	Role Templates (All Zones)
Veeam	Veeam Backup Software suite
VMware	VMware - Sphere
VMware	VMware - Horizon
WSUS	WSUS
WTI	WTI - Out of Band Management

The following Development and Data Management applications are included in the ASD architecture:

Development and Data Management Applications	
Adobe flash for Chrome	Owl OV2S Screen View (Client)
ADUC Utilities	Owl OV2S Screen View (Server)
AXIS Camera Management Utility	Pivot3 CLI
Barco Wall Software	Pivot3 CLI Windows
Dell RACADM	Pivot3 Management Application
FLIR Camera Manager	Powershell Module - Active Directory
Full Shot	Powershell - Kubecti
Google Chrome	Powershell - Milestone
Libre Office	PuTTY
Microsoft Excel Viewer	RvTools
Microsoft .Net Core	SecureCRT
Microsoft Office 2016	SQL Server Management Studio
Microsoft Remote Desktop Manager	SSDT-BI
Microsoft Visio Viewer	VMware - Enhanced authentication plugin
Microsoft Visual Code	VMware - ovftool
Microsoft Visual Studio	VMware - PowerCLI
Microsoft Word Viewer	VMware - PowerCLI for Horizon
Mozilla Firefox	VMware - Remote Console
mRemoteNG	WinSCP
Notepad++	Wireshark

Physical Architecture and High-Level Equipment Summary

The list below provides a summary of the ICT equipment deployed in the Customer network:

Network and Server equipment summary for all environments:

Avangrid ASD Support Network/Appliances		
Vendors Support Equipment	Total	Business Description
Cisco Data Center Switches	195 Switches	All Data Center Switches Across all Enviroments - 450 Virtual Interfaces
Cisco Prime Appliances	7 Cisco Appliances	All Cisco Prime Monitoring Appliances across all environments
Cisco ISE Appliances	7 Cisco Appliances	All Cisco ISE Authentication Appliances across all environments
Citrix Netscalers	10 MPX Appliances	All Netscaler Load Balancers across all environments
Checkpoint Firewalls	20 Physical Chassis	All Checkpoint Firewall across all environments = Total virtualized VSX FW = 16
OWL	15 Appliances	All OWL Devices across all environments
WTI	5 WTI Console	All WTI Devices across all environments
Gigamon	15 Appliances	All Gigamon Appliances across all environments
TrendMicro TPS	13 Appliances	All TrendMicro TPS Appliances across all environments
Dragos	15 Appliances	All Dragos Appliances across all environments
LogRhythm	40 Appliances	All LogRhythm Appliances across all environments
Nokia SMS Server	2 Appliances	All Nokia SMS Appliances across all environments
Stratacom NTP	4 Appliances	All Stratacom Appliances across all environments
IronNet	25 Appliances	All IronNet Appliances across all environments
Nokia VSR	5 Appliances	All Nokia VSR Appliances across all environments
NON-IP Based KVM	20 KVM	All KVM Appliances across all environments
Nokia IP/MPLS Routers	140 Routers	ALL Nokia IP/MPLS Routers across all locations
Nokia DWDM Nodes	100 DWDM Nodes	ALL Nokia DWDM across all locations
Ciena DWDM Notdes	10 DWDM Nodes	ALL Ciena DWDM across all locations
Remote Site Cisco Switches	326 Switches	All Cisco Remote Site Switches (Service Center, Substations)
TOTAL Appliances/Switches Managed = 964		

Description	Counts
Pivot3	141
Pivot3 Archiver	20
Dell R650	1
Dell VxRail E660	4
Dell R330	15
Dell R730	5

Data Center high-level requirements:

Requirement Types	Description
General	A High-Level of security, cooling and electrical availability
	High connectivity and quality of communications
Electrical	AC power: High grade inverters capable of providing clean, reliable AC power
ASD load power	Associated to the equipment for the Data Centers
Electrical UPS	2N - UPS modules for all the ASD load, times two
Electrical Generator	One generator with an external building feed for connecting a backup generator
Floor space	A server room that accommodates 9 equipment cabinets, along with 2 CRAC, a fire alarm and two power distribution modules
Cabinet Cold Aisle cooling	Must not exceed 75°F/24°C in the cold aisles
Cabinet	Power density should not exceed 7 kW per rack
	Cabinets are equipped with blanking panels so that cold and hot air does not mix
Reliability objective	TIER 3 with 99.98% availability redundant DC1 and DC2.
Mirrored data center	Mirroring at the SAN level
	Fault Tolerance at the virtualization level using VMware HA and VMware Fault Tolerance or equivalent
Replication Data center	Replication at the database level
	Replication at the Virtualization level using VMware vSphere Replication (SRM) or equivalent
Replication servers	Servers used in the mirroring, or the replication must be identical

Table of Unitized Work Request Details

Request Type - Major	Request Type - Description
Access Request	Active Directory (AD)
Access Request	AD Password Reset
Access Request	Add/Remove Security Group/Role Members
Access Request	Architecture Reference Guide Access Request
Access Request	Centrify
Access Request	Check Point/Firewall
Access Request	Cisco Prime
Access Request	Create/Modify/Delete Folder
Access Request	Create/Modify/Delete Role
Access Request	Create/Modify/Delete Security Group

Access Request	DEV with Remote Access
Access Request	Dragos
Access Request	Gigamon
Access Request	IBM Rational (RQM)
Access Request	IronNet
Access Request	LockPath (Keylight Service)
Access Request	LogRhythm
Access Request	Microsoft Applications
Access Request	MS SQL
Access Request	Nokia
Access Request	Offboarding Infra Child ticket
Access Request	Other Applications
Access Request	OWL
Access Request	PROD Access
Access Request	PROD Shared Document Access Request
Access Request	QA Access
Access Request	Red Hat
Access Request	SolarWinds Help Desk - DMZ
Access Request	SolarWinds Orion
Access Request	SolarWinds Orion - DMZ
Access Request	Tenable
Access Request	TrendMicro
Access Request	Video DNS Records Addition
Access Request	VMware
Access Request	Windows
Admin Use Only	Patch Update
Admin Use Only	Signature Update Child Ticket
Asset Management	Onboarding Infra Child ticket
Asset Management	Return Equipment/Remove User
Compliance and QA	Compliance Check
Compliance and QA	Compliance Review
Compliance and QA	Cybersecurity Compliance Check
Compliance and QA	ECR (Exceptional Circumstance Request)
Compliance and QA	Evidence Request
Compliance and QA	File Transfer Request
Compliance and QA	Product Evaluation
Compliance and QA	QAQC Testing
Cybersecurity Compliance Check Child Tickets	PROD CZ Cybersecurity Compliance Check - Anti-Malware
Cybersecurity Compliance Check Child Tickets	PROD CZ Cybersecurity Compliance Check - Listening Port Validation

Cybersecurity Compliance Check Child Tickets	PROD CZ Cybersecurity Compliance Check - SIEM
Decomm/Comm/Modify Child Tickets	Decomm/Comm/Modify - Asset Management
Decomm/Comm/Modify Child Tickets	Decomm/Comm/Modify - Cisco ISE
Decomm/Comm/Modify Child Tickets	Decomm/Comm/Modify - Cisco Prime
Decomm/Comm/Modify Child Tickets	Decomm/Comm/Modify - DNS
Decomm/Comm/Modify Child Tickets	Decomm/Comm/Modify - LogRhythm
Decomm/Comm/Modify Child Tickets	Decomm/Comm/Modify - Tenable
Decomm/Comm/Modify Child Tickets	Decomm/Comm/Modify - TrendMicro
Decomm/Comm/Modify Child Tickets	Decomm/Comm/Modify - Veeam
Decomm/Comm/Modify Child Tickets	Infra DEV
Decomm/Comm/Modify Child Tickets	Infra PROD
Decomm/Comm/Modify Child Tickets	Infra QA
Decomm/Comm/Modify Child Tickets	Network DEV
Decomm/Comm/Modify Child Tickets	Network PROD
Decomm/Comm/Modify Child Tickets	Network QA
NRI Child Tickets	Check Point/Firewall
NRI Child Tickets	Nokia Router
NRI Child Tickets	Router Configuration Validation
Password Reset	AD Password Reset
Password Reset	Default PW Reset
Security Group/Role Access	R/O Folder Access by Security Group Role
Security Group/Role Access	R/W Folder Access by Security Group Role
Site Migration Child Ticket	Check Point/Firewall
Site Migration Child Ticket	Cisco ISE
Site Migration Child Ticket	Cisco Prime
Site Migration Child Ticket	Firewall - PACS
Site Migration Child Ticket	LogRhythm
Site Migration Child Ticket	Multicast Route Engineering
Site Migration Child Ticket	Network DNS Records Addition

Site Migration Child Ticket	Network Switch Configuration
Site Migration Child Ticket	Nokia
Site Migration Child Ticket	PACS DNS Addition
Site Migration Child Ticket	Site Migration Testing
Site Migration Child Ticket	Tenable
Site Migration Child Ticket	Video DNS Records Addition
Signature Update	Check Point/Firewall
Signature Update	File Transfer Request
Signature Update	Gigamon
Signature Update	LogRhythm
Signature Update	Owl Cyber Defense
Signature Update	Tenable
Signature Update	TippingPoint
Signature Update	TrendMicro
Patch Update	Centrify
Patch Update	Cisco Data Center Nodes
Patch Update	Cisco ISE
Patch Update	Cisco Prime
Patch Update	Citrix NetScaler
Patch Update	DataCore
Patch Update	Gigamon
Patch Update	IBM Rational
Patch Update	IronNet/IronDefense
Patch Update	Liquidware
Patch Update	LockPath-Keylight
Patch Update	LogRhythm
Patch Update	MS SQL
Patch Update	Netscaler VPX
Patch Update	Owl Cyber Defense
Patch Update	Pivot3
Patch Update	Red Hat
Patch Update	Tenable
Patch Update	TrendMicro
Patch Update	Tresys
Patch Update	Veeam
Patch Update	VMware
Patch Update	Windows Systems
On Boarding	Onboarding Infra Child ticket
On Boarding	Onboarding ITSM Child ticket
On Boarding	Onboarding Request
On Boarding	Security Guard Onboarding Request

Off Boarding	Offboarding Infra Child ticket
Off Boarding	Offboarding ITSM Child Ticket
Off Boarding	Offboarding Request
Off Boarding	Security Guard Offboarding Request

ICT Labor and Technical Resources Summary and Job Descriptions

Below is a summary of the position roles and associated description of requirements associated to each of the ASD/ICT roles:

Job Title	Job ID
AD/SQL Supervisor	32
Build Analyst	57
Build Supervisor	56
Compliance Analyst	59
Compliance Manager	58
Cyber Controls Analyst	63
Cyber-Applications Analyst	65
Cyber-Applications Supervisor	64
ICT Chief Security Architect (Data)	45
Network Engineer	37
Network Supervisor	36
Quality Assurance Analyst	54
Quality Assurance Supervisor	55
SQL Database Administrator	24

ICT Role Descriptions

AD/SQL Supervisor

Job ID - 32
AD/SQL Supervisor Job Responsibilities:
Ensures the streamlined operation of the Customer Security Domain in alignment with the business objectives of the client; plans, coordinates, directs, and supports the program objectives and activities, as well as provides administrative direction and support for the daily operational activities of the Applications group.AD/SQL Supervisor, Job Duties:

- Nurture a “One Team Approach” in a multiple integrator environment.
- Supervise and mentor AD analysts and DBA’s.

- Help develop, implement and maintain department workflows and processes.
- Manage the integration of multiple Vendor schedules to meet Customer deliverables.
- Establish and maintain regular written and in-person communications with the ASD Applications Manager regarding pertinent ASD Operations activities.
- Manage software testing of changes and additions to standard security system design.
- Keep current with the latest technologies.
- Ensure all activities meet or exceed commitments to the client.
- Ensure all ASD Operations policies and procedures are followed by the team.
- Benchmark, analyze report on, and make recommendations for the improvement and growth of ASD Operations team.

AD/SQL Supervisor Skills and Qualifications:
Bachelor's degree in IT or related field or equivalent work experience. A minimum of 6 years working in MS Windows Server environment. Excellent working knowledge in PKI / Certificate enrollment and architecture design and support. Strong understanding of Windows 7 / 10 OS platform. Understanding of Computer and User authentication is needed for troubleshooting performance issues associated with logon or Host resolution for both Server and Workstation. Working Knowledge of Exchange systems and attributes in AD, with related support experience. At least 5 years of experience in managing Windows Domains using Active Directory. Thorough understanding of Domain/Forest trusts, Replication, NTFS/ACL permissions, Group Policies, etc. Excellent working knowledge of Microsoft Applications and Services (including, but not limited to WSUS, IIS, FTP, DNS, DFS, SCCM, SCOM, SQL and SharePoint) Working knowledge of DNS configuration, MS Clustering services, SAN storage configuration, Terminal services, TCP/IP protocol, LDAP Knowledge and experience applying Group Policy Objects in a Domain Environment, Extensive working knowledge around PKI, ADFS, Azure AD Connect, and O365 suite. MS Windows Server Security Configuration and Administration PowerShell, VB Scripting, VM Ware Virtualization platform History of participating in the entire lifecycle (planning, deployment, maintenance) of critical ICT services Advanced knowledge of Microsoft Office applications (including but not limited to Excel, Visio & Project) Microsoft Certified Professional in the Windows Server track Associate Degree in degree in information technology, computer science, or related field; or equivalent work experience.

SQL Database Administrator

Job ID - 24

SQL Database Administrator (DBA) Responsibilities:
Works closely with our analysts, systems administrators, and designers to support implementation, configuration, maintenance, troubleshooting, and optimization of Microsoft SQL Servers.

SQL DBA Duties:

- Responsible for creation and ongoing maintenance of functional and relational Database Diagrams for all Network Services Company SQL Databases. Keep diagrams/documentation current and establish effective vehicles to publish the documentation to Applications Staff and others for use in report development and ASD Operations Projects.
- Ability to write and troubleshoot complex Stored Procedures, ANSI and T-SQL queries and scripts, and document processes and procedures.
- Experience implementing operational automation.
- Manage SQL Server databases through multiple product lifecycle environments, from development to mission-critical production systems.
- Configure database servers and processes, including monitoring of system health and performance, to ensure high levels of performance, availability, and security.
- Update, backup, maintain & troubleshoot databases. Perform troubleshooting, resolution and root cause analysis for database and application specific incidents.
- Programing in SQL. Write and optimize SQL statements.
- Work as a subject matter expert on database technologies, reviewing changes, security & operations procedures to maximize uptime & reduce time to recover.
- Perform all common periodic Database Administration (DBA) tasks, including managing database backups and recovery, managing database users and security, Database Server Administration, Event and System Monitoring, etc.
- Design database indexing schemes and perform optimal DB tuning
- Ability to detect and troubleshoot SQL server related CPU, Memory, I/0, disk space and other resource contention.
- Periodic review of all database Maintenance, Backup, and Optimization plans. Recommend improvements to support use of database best practices, more efficient processing, improved system uptime, and to support the growth of the business.
- Periodic review of all current SQL servers from a security (Windows and SQL) standpoint. Review industry best practices and make periodic

recommendations for Database security and Windows server related security improvements.

- Ability to export and import data from/to various formats like delimited raw/text file, MS-Excel, XML, SQL Server, MS-Access, etc. Ability to transfer data between various servers and/or data sources. Ability to restore databases and individual tables upon request.
- Provide leadership, architectural recommendations and implementation plans for potential long-term database scalability, performance improvements, and support for a hybrid infrastructure.

SQL DBA Skills and Qualifications:
Bachelor's degree in IT or related field or equivalent work experience. 5+ years MS SQL Server Administration experience required. Experience with Failover Clustering and Always on Availability Groups. Experience with Performance Tuning and Optimization
Experience with backups, restores and recovery models. Experience working with Windows Server, including Active Directory. Experience writing SQL queries, analyzing query performance using query plans and tuning query performance. Experience with C#, Visual Basic or Visual Studio Preferred. Critical thinking skills and ability to adapt to rapid project changes
Provide on call support for critical production systems. Share technical expertise, providing technical mentorship and cross-training to other peers and team members. Strong organizational and communication skills.

Build Analyst

Job ID - 57
Build Analyst Responsibilities: works closely with Infrastructure Managers, designers, and QA Test Teams to oversee the ICT build and release process for the client.

Build Analyst Job Duties:

- Preparing and issuing requirements for both internal and external clients.
- Own the coordination of configuration management activities, development of build standards, and assisting the quality assurance team to a successful systems' certification process across multiple platforms and/or products.
- Build, maintain and configure the Configuration Management Database (CMDB) and configuration items.
- Acting as the liaison between external partners (Microsoft, Solarwinds, Tenable, Unlimited Technologies, G4S, CISCO, Checkpoint, etc.…) and the development team, coordinating and negotiating development plans, exceptions to quality and configuration, control build-state, as well as overall releases.

- Developing and owning the build process inside and out, interacting with external vendors to ensure formal system build standardization controls to ensure consistent application of standardized builds across all environments in accordance with design specifications.
- Working with the design team to ensure a consistent approach to systems configuration and build- documentation; produce deployment run books and provide input to release plans\implementation plans.
- Owning associated tools and databases utilized for the verification process as related to build certification and release.
- Working with both internal and external key stakeholders to determine release content plans as related to certification of final configuration specs and build standards and shepherd that content/process through external party approvals for the release.
- Owning, managing and maintaining build catalog and establishing a release plan with the PMO.
- Working closely with QA, Server Engineers, and Technical Leads on monitoring the build and integration process to ensure correct build execution and facilitate resolution of build errors/failures.
- Working with Server Engineer to understand and communicate risks as gold-build standards and release activities are developed for various systems and infrastructure components.
- Working with QA Lead to establish and maintain bug triage process, determine and prioritize must fix issues for release and work with appropriate team members to ensure bug fixes happen as planned, and all documentation and/or artifacts maintained up-to-date.
- Working closely with Dev Production, QA, and Live Ops teams on identifying and resolving risk related to releases through the monitoring and tracking of incomplete and/or uncertified builds while controlling changes to existing approved build-assets.
- Coordinating internal and external release notes, known issues, and knowledge base updates.
- Ensuring releases have passed all required checks and approvals leading up to live deployment and effectively communicate approved exceptions to all necessary key stakeholders.
- Working closely with the Program Management Office and Live Ops team to coordinate and publish frequent builds, hotfixes, and patches.
- Maintaining formal build and release records to track release content and history across the design, implementation, and QA process.
- Maintains a release repository and manages key information such as build and release procedures, dependencies, and notification lists.

Build Analyst Skills & Qualifications:
BS degree in Computer Science or IT related field with one to ten years of experience. Further education a plus. Experience working in the quality area for an organization certified to ISO 9001 or similar standard. Knowledge of Quality Assurance system development and implementation such as ANSI/ISO/ASQ 9001, SQF, ISO 14001, QS 9100, etc. Proficiency in MS Office, including Word and Excel. Excellent communication skills, both orally and written, at all levels of an organization. Strong organizational skills and motivational skills. Demonstrated ability to solve practical problems and make logical decisions. Ability to work independently, as well as within a team.

Build Supervisor

Enhance & Support all build and deployment tools through automation. Design and implement the automated code migration from development, testing, & staging through to production, Develop Process for maintaining image standards, Source Code Control Administration, Ensure the application code and or builds (VMs) is functional and maintained technical integrity, Work with QA and ITSM Manager to Support IBM Rational Database, Ensure the preservation of Confidentiality, Integrity, and Availability of Server, Network Routers, and Applications, Images/Builds, Work with outside vendors/ external interfaces including the development team and the IT group to resolve any integration endpoints (i.e. web services/ batch processes, database, file, messaging) across multiple departments including development, test, stage, UAT and production environments, Configure and prepare production releases; prepare deployment and rollback instructions; co-ordinate the refresh & reset capabilities of the database instances with the QA/Development team for each release. Support ongoing project needs in build construction, promotion, and verification while focusing on implementing build and release automation. Ensure all tickets are up-to-date with latest statuses and documentation

Build Supervisor Job Duties:

- Good technical understanding of Java/J2ee
- Experience writing SQL to configure and/or support database servers like SQL Server, Db2 or others
- Solid understanding and knowledge of relevant software development tools including version control, as well as build processes and related technologies (Maven, Ant, Jenkins, Artifactory, Sonar)
- Strong knowledge of Source Code Control Systems (i.e. Subversion, Git)
- Critical understanding of branching and merging strategies
- Experience working within Windows and Linux environments
- Experience in Java programming technologies on open source environments

- Experience with continuous integration and deployment practices.
- Ability to maintain automated builds, tests, and staging environments
- Understanding of QC & Test Automation in Agile-based Continuous Integration environment
- Automated deployment /build scripting using Shell, Python, Powershell, or Groovy
- Knowledge of IT operations, monitoring tools and ticketing systems
- Must have good written and verbal communication skills

Build Supervisor Skills & Qualifications:
Four-year college degree, preferably in Computer Science or Business, 5+ years in a technical DevOps or Build/Release Engineering position Systems level config management tools and creating automated infrastructure/ code deployment and management, Knowledge of Release Management Process, Proficient in MS Office Suite, ISS Server Management Experience, J2EE application development experience/ scripting, J2EE-stack application servers (i.e. JBoss, Tomcat, WebLogic, Websphere, etc.), and Microsoft .Net

Compliance Analyst

Job ID - 59
Compliance Analyst Responsibilities:
Promotes the reliability of the Bulk Power System through rigorous compliance with applicable NERC standards monitoring and enforcement activities and functions as a team member for internal and external audit preparation. Ensures relevant, valid, reliable, stacking, and sufficient evidence is available to demonstrate compliance. Compliance Analyst Job Duties:

- Researches regulations by reviewing regulatory bulletins and other sources of information.
- Compiles information by coordinating rate deviation filings; maintaining updated rate matrices; providing overviews of product disclosures.
- Keeps other departments abreast of requirements by researching regulatory and filing information; writing and communicating guidelines.
- Obtains approvals by revising forms and rates.
- Prepares reports by collecting, analyzing, and summarizing information.
- Maintains rapport with regulatory personnel by arranging continuing contacts; resolving concerns.
- Maintains quality service by establishing and enforcing organization standards.
- Maintains professional and technical knowledge by attending educational workshops; reviewing professional publications; establishing personal

networks; benchmarking state-of-the-art practices; participating in professional societies.

- Contributes to team effort by accomplishing related results as needed.

Compliance Analyst Skills and Qualifications:
BS/BA college degree or higher in a technical discipline, or an equivalent combination of education, training and experience. In depth knowledge of ITIL aligned Service Management principles and processes. ITIL V3 certification is preferred. At least 5 years' experience in a Service Management role, with significant exposure to IT audit and compliance; 5+ years of experience in planning, organizing and delivering impactful service improvements in complex technical environments involving multiple stakeholders. Professional certification in an audit and compliance related area, is a plus e.g. CISA, CRISC, CISM. Familiarity with industry standard compliance and security frameworks/ regulations - e.g. Data Privacy, SOX, NERC, CIP, encryption/cryptography standards and other international, federal and state regulations as applicable to the Utility industry. Knowledge of current trends within the industry and developments in legislation or regulation. Ability to drive results with people who are not direct repartees. Strong influencing and persuasive skills based on facts, data and analysis
Experience of working in a multi-vendor environment and with offshore partner resources.
Advanced interpersonal skills with demonstrable ability to build rapport and to articulate complex technical solutions in business terms. Ability to influence and build relationships and demonstrate team leadership in all interactions. Exceptional written and verbal communication skills. Communicates effectively with business clients to identify needs and evaluate alternative business solutions.

Cyber-Applications Supervisor

Job ID - 64
Cyber-Applications Supervisor Responsibilities:
Responsible for meeting with clients to determine their system needs. Oversee a secure implementation of 64 applications. Ability to work with design team to engineer complete system(s). Monitor and maintain system health which includes Database and application Servers. Test, program and troubleshoot access control and digital video systems. Follow assigned projects through to final adjustment and commissioning of installed systems. Create test plans and test systems. Install complete turnkey system (software and hardware). Customize system to tailor to customers' business model. Work off hours to support customers and technicians globally. Troubleshoot system/network related issues over the phone with Customers and Contractors. Ability to train customers and technicians on respective systems. Be available for 24-hour phone support. Document and maintain system architecture and parameters specific to customer. To work in compliance with the Company's Health and Safety standards and requirements;

with the safety of self and others in mind at all time. Provide regular updates to management on cyber security application strategies, critical projects and related risks, potential policy exceptions, and other items, as applicable.

Cyber-Applications Supervisor Job Duties:

- Ensure information security requirements are properly represented throughout ASD processes including risk assessments, new product evaluations, application development, testing, and ongoing operations.
- Engage, as necessary, in ASD sponsored application projects and advise on information security related matters. Manage the credentials, privileges and access for ASD corporate resources to ensure all information systems are functional and secure, ensuring that SLAs are met.
- Maintain IAM security policy including providing updates to CIS procedural documents to support policy.
- Represent CIS when working with BB&T business partners to understand business problems and providing solutions to those problems.
- Engage, as necessary, in ASD sponsored projects and advise on information security related matters.
- Manage the credentials, privileges and access for distributed systems to ensure all information systems are functional and secure, ensuring that SLAs are met.
- Maintain IAM security policy including providing updates to CIS procedural documents to support policy.
- Analyzes security-related technical problems and provides basic engineering and technical support in solving these problems. Effectively support the production applications within the assigned area, with a focus on quality implementations and production stability. This includes managing audit/risk profile and issues and data custodian responsibilities.
- Review technical and business processes, standards and procedures, making recommendations for continuous improvement.
- Assists in the development of testing strategies, methodologies and analyses; evaluates the adequacy and effectiveness of policies, procedures, processes, systems and internal controls; analyzes business and/or system changes to determine impact, identifies and assesses operational risk issues and assigns risk ratings consistent with established policy standards.
- Provides technical design and consulting services on (IAM) Identity and Access Management (IAM) products
- Provides customer specific though leadership and solution construction including installations of Identity and Access Management (IAM) products for User life-cycle management, Identity and Access Governance, Automated Provisioning, (SSO) Single Sign-On, Federation, and Privileged Account Management

- Enhances existing systems by analyzing business objectives, preparing an action plan and identifying areas for modification and improvement
- Creates customer level documentation specific to deployment of IAM products
- Creates knowledge articles for corporate website related to IAM
- Provide regular feedback to the Professional Services Director to guide systems integration methodology and packages service development

Cyber-Applications Supervisor Skills & Qualifications:
Bachelor's in computer science or a related field and 5 years or more of relevant experience, A current Linux certification: Red Hat Enterprise Linux (RHEL) Operating system or Linux, Professional Institute Certification (LPIC) is preferred. A current CompTIA Security+ with CE or GIAC Security Essentials Certification (GSEC) or Systems Security Certified Practitioner (SSCP) is required or must be obtained and maintained while in this role. Extensive knowledge of implementing and supporting Red Hat or similar branch of Linux. Experienced in supporting Linux in a Virtual Desktop Infrastructure. In-depth knowledge of Windows 10 and Windows Server 2016 or 2012R2, Experience with administering LogRhythm, Experienced in optimizing Linux systems for optimal performance, Experience with writing and implementing PowerShell scripts, Ability to work independently on problems and projects; and participate as part of a team. Experienced in implementing DISA Security Technical Implementation Guidelines. Experienced in managing Security Vulnerability issues, remediation, and reporting.

Cyber-Applications Analyst

Job ID – 65
Cyber-Applications Analyst Responsibilities:
Lead technical discussions and interact with our customers as the primary technical authority for an engagement. Ability to present project solutions to clients, manage client expectations, and implement and deliver solutions. Become a subject matter expert with IAM products and concepts. Participate and support Incident, problem, change and configuration management. Support application availability objectives and mitigate risks. Manage application upgrades and Lifecycle projects and tasks. Assist in the deployment of security applications; e.g. Centrify, Tenable, Lockpath, AD, LogRhythm, etc…

Cyber-Applications Analyst Job Duties:

- Ability to partner closely with key business stakeholders.
- Create code for simple changes, enhancements, and modules to ensure code works according to specifications and standards
- Analyze detailed business, functional, and high-level technical requirements—including technical recovery, security, and audit—to identify the need for, and assist with, the roll-back of units of work

- Analyze design materials and contribute solutions in design reviews to ensure designs meet requirements
- Track and resolve simple defects.
- Provide technical assistance.
- Maintain application runbooks
- Participate in on call rotation.
- Owns service level baselining, monitoring and event management for their products
- Analyze and resolve simple to moderate problems
- Analyze code to explain and identify possible issues with created code
- Prepare accurate data for test plan and modules; participate in testing reviews
- Create and execute unit code tests
- Execute change management activities

Cyber-Applications Analyst Skills & Qualifications:
Bachelors College degree or equivalent experience, 2 - 4 years of experience in a large enterprise environment. 2+ years of production support experience troubleshooting and debugging issues. Agile Development experience, Analysis skills, applying the technical solutions to problems and performance concerns. Experience in .NET Applications and Development and Scripting is a plus, Web Application security, Software Security, HTTP and related technologies, Database/Directory integration, x509 Certificates, Windows, Unix, Linux, Experience with IAM products: CA / SiteMinder, Radiant Logic, Sailpoint, Centrify, ForgeRock, Ping Identity, IBM, Okta, Oracle, RSA, Federated Identity and Single Sign-On, Access management and API Gateways, SAML, WS-Federation, OAuth, OpenID Connect, and/or SCIM standards, RADIUS and/or KERBEROS, APIs (SOAP, XML, REST, JSON), Social APIs including Facebook, Twitter, LinkedIn, etc. User Directory (Active Directory OpenLDAP, OpenDJ, etc.), Java and/or .NET development, Amazon's AWS services (i.e. VPCs, SES, RC2, R3, Route 53, Cloud Formation, etc.)

Cyber-Controls Analyst

Job ID 63
Vetting, analyzing, and implementation of various cyber security platforms within the client ASD.

Cyber-Controls Analyst Job Duties:

- Develop Information Security Plans and Policies
- Helps plan and carry out client's information security strategy for the ASD.

- Assist in the development of cyber security BMP's for the organization, and recommend security enhancements to the PMO and client management as needed.
- From a software level, help to develop strategies to respond to and recover from a security breach.
- Responsible for educating the workforce on information security through training and building awareness.
- Implement Protections
- Works with ASD Operations teams to configure, install, and commission various software platforms, such as firewalls, data encryption programs, and various best in class software platforms to protect client's sensitive information.

Cyber-Controls Skills and Qualifications:
Bachelor's degree in IT or related field or equivalent work experience; A+ and Server+ Certification or practical field experience; Scripting/Programming Skills in SQL or practical field experience; CCNA or other Cisco certifications; Direct experience with anti-virus software, intrusion detection, firewalls and content filtering; Knowledge of risk assessment tools, technologies and methods; Experience designing secure networks, systems and application architectures; Knowledge of disaster recovery, computer forensic tools, technologies and methods; Experience planning, researching and developing security policies, standards and procedures; Professional experience in a system administration role supporting multiple platforms and applications; Ability to communicate network security issues to peers and management; Ability to read and use the results of mobile code, malicious code, and anti-virus software**.**

ICT Chief Security Architect

Job ID - 45
ICT Chief Security Architect Job Responsibilities:
Responsible for providing technical leadership and strategy in the domain of physical and cyber security; Subject matter expert responsible for establishing security architectures and requirements; Architects environments, research best practices, conduct business requirement analysis, and develop forward looking security vision in line with the business needs of the organization.

Chief Security Architect Job Duties:
- Development of security architecture, specifications and identification of tools as needed to meet security policies
- Assist with architectural design and security program creation
- Support major product programs with security expertise
- Collaborate on advanced engineering projects with internal design teams

- Assist in proof-of-concepts with new features and technology related to security
- Advises others on what changes need to be made to different systems in order to comply with security policies and standards
- Conducts incident investigation and system forensic examinations
- Works on multiple projects as a team member and lead systems related security components
- Develops system testing strategies, plans, cases and conditions; monitors testing efforts
- Develops and evaluates systems security across various platforms and environments
- Performs related duties as required by project deliverables

Chief Security Architect Skills &Qualifications:
BS/BA in Computer Science, Electrical or Computer Engineering, Information Security or Mathematics required. Graduate degree preferred. 15+ years of relevant security experience. Working knowledge of international and industry standards such as NERC-CIP, NIST Technical expertise in security practices and procedures. Ability to deal collaboratively, diplomatically, and successfully with customers, co-workers and other professional colleagues, managers, and staff. Ability to work effectively in a team environment, as well as work independently with limited supervision. Excellent problem-solving skills while providing first class customer service. Outstanding oral and written communication skills.

Network Engineer

Job ID - 37

Supports Engineering Team in Network Systems Design, Installation, Programming, and Maintenance.

Network Engineer Job Duties:

- Support Customer Networking team for support of existing systems.
- Provide design, implementation, maintenance of LAN/WAN network devices and transport gear.
- Provide engineering support of Security service requests and maintenance.
- Attend deployment meetings and support deployment of network equipment ahead of security equipment.
- Support Return Material Authorization requests and testing processes to ensure material can go back to the Contractor or service repairs as necessary.
- Support designs to standards as required including NERC Compliance and documentation.

- Provide preprogramming of devices for installation as required for firmware updating and testing.
- Support system analysis with Contractor support for constant system efficiency.
- Oversee lifecycle replacements.

Network Engineer's Skills and Qualifications:
Bachelor's degree in IT or Network field or equivalent work experience with one to ten years of experience in the security environment or LAN/WAN experience with training on multiple Contractors. An acceptable and equivalent combination of education and experience will be considered. Specific system training a must. Must be proficient in Microsoft Office software programs. If required by job responsibilities, incumbent must possess a valid driver's license and pass defensive driving. Background check, NERC/CIP Compliance Training, CPR/First Aid, Bloodborne Pathogen training.

Network Supervisor

Job ID - 36
Network Supervisor Responsibilities:
Accountable for the data center, and circuit provisioning team. These teams are responsible for deployments, configurations and improvements in the of the data. Works with WAN engineering teams to complete network designs. Coordinates between domain and transport layers.

Network Supervisor Job Duties:
- Leads, coordinates and evaluates the work of network engineers to ensure function is providing all users with prompt and accurate services for data centers, WAN, and provisioning
- Leads team for the telecom drill downs for diagnostic and problem resolution, namely, downtime, performance and security incidents.
- Manages and prioritizes the work of network engineers as well as manages external intake to ensuring proper processes are followed to effectively manage demands
- Ensures network engineering solutions are clearly communicated to operations and change management
- Monitors and stays abreast of industry trends and anticipates the future direction of enterprise networks
- Acts as a backup in the rotation for the L2&3 telecom administrators.
- Accountable for seeing that business and technology standards, best practices and processes are followed

- Responsible for work flow and delivery of projects, oversees the integration and deployment of network technologies in local area networking, wide area networking, switching, routing, WAN optimization, Wireless, voice over IP, IP Telephony, video and other core network services and all application infrastructure on transport network
- An active participant for ensuring that the enterprise has the capability to support new technologies and maintain high levels of network performance and reliability
- Partners with various functional teams across the IT organization to provide direction and design principles for the network area

Network Supervisor Skills and Qualifications:
Bachelor's degree in IT or related field or equivalent work experience; 8+ years' experience in a large enterprise providing networking architecture, engineering and operations; ITIL and other IT network related certifications a plus; ability to create planning, design, and implementation documents in power point and present them to engineering and management audiences; strong business acumen, conflict resolution skills, drives project completion, and collaborates with other teams; effective verbal and written skills; knowledge and subject matter expertise in various products and services including but not limited to: Cisco data center network solutions, Cisco VPN, HP networking solutions, Juniper VPN, HP Aruba Wireless, Riverbed WAN optimization; high level knowledge in various security products and services including but not limited to: Cisco Firewalls, IDS/IPS, Palo Alto Firewalls, Sourefire IDS, Juniper VPN, Infoblox, Checkpoint Firewalls, HP Blade Servers, VMware ESX, and MS Hyper-V; demonstrated leadership, problem solving and creative thinking capabilities; ability to align business requirements into technical requirements.

Quality Assurance Supervisor

Job ID - 55
Quality Supervisor Responsibilities:
This role will have primary responsibility for development and maintenance of quality standards, processes and documentation. This includes but is not limited to; defining quality requirements and processes and preparing/maintaining necessary documentation, monitoring quality performance to identify opportunities for improvement, review and maintenance of quality files, procedures, Job Books, work instructions, etc. for relevance and adherence to company Quality System, customer and regulatory compliance.

Quality Assurance Supervisor Job Duties:
- Preparing and issuing requirements for both internal and external clients.
- Assist Architect/Developer to define and implement operational and system architectures.

- Manages the installation and, if needed, the migration of content from a legacy file management system to the new SharePoint content management system.
- Develop and execute a communications/training plan to educate the workforce as capabilities are rolled out.
- Responsible for managing the day-to-day tasks for supporting various customers in their SharePoint rollout and operations.

Quality Assurance Supervisor Skills & Qualifications:
BS degree in Computer Science or IT related field /or 7+ years in a similar quality assurance program, department, or operation is required. Further education a plus. Experience working in the quality area for an organization certified to ISO 9001 or similar standard. Knowledge of Quality Assurance system development and implementation such as ANSI/ISO/ASQ 9001, SQF, ISO 14001, QS 9100, etc. Proficiency in MS Office, including Word and Excel. Excellent communication skills, both orally and written, at all levels of an organization. Strong organizational skills and motivational skills. Demonstrated ability to solve practical problems and make logical decisions. Ability to work independently, as well as within a team.

Quality Assurance Analyst

Job ID - 54
Quality Assurance Analyst Responsibilities:
The Quality Assurance Analyst will work to monitor software quality and associated business/technical risks in support of joint functional testing with our partners. They will be dedicated to working with our partners to support joint functional test planning, developing test scenarios, monitoring and supporting execution of test scenarios, and analyzing results.
This position requires strong deductive reasoning, attention to detail, persistence, patience, and creativity. The individual will work with our modules test counterparts at our partner organizations, internal development teams, Database Administrators, Business Analysts, and support teams to analyze, maintain and execute performance testing procedures.

Quality Assurance Analyst Job Duties:
- Act as the point of contact with our partner organizations for functional testing activities through the project lifecycle
- Work with team to plan sprints and test planning for the modules
- Work with our module teams to design, develop, and execute scripts which validate, to a high degree of confidence, test cases defined within the project's test plan.
- Support the automated load/performance testing by our partners across multiple messaging protocols (including HTTP), focusing on overall

application performance - validating that application response and outputs accurately reflect business requirements.

- Track and communicate task progress, status, and key performance metrics.
- Report defects found in testing diligently, promptly, and accurately, using standard defect tracking tools.
- Communicate effectively across multiple teams/external vendors (Operations, Project Teams, Quality Service, etc.), as well as different personnel (Developers, Scrum Masters, Project Managers, etc.) when required.
- Perform data analysis when needed to analyze issues in Performance and/or Production environments.
- Conduct troubleshooting/performance test execution in support of remediation efforts as required.
- Analyze data and application changes and document their impact on the performance testing task (test cases, scripting, scenario execution, etc.).
- Ensure the test execution results fulfill the defined test objectives. - Schedule/recommends test re-execution if necessary.
- Ensure the appropriate testing and monitoring tools/technologies are configured accordingly with the test objectives/project team requirements.
- Expected to maintain technical expertise via self-education in areas governing computer sciences, performance/load testing dictums, and Quality Assurance.
- Interface directly with the DevOps and Infrastructure teams regarding Functional test environment.
- Work with our partners to establish test data in sufficient quantity to support the performance testing effort
- Active participant in the meeting(s) to verify firewall openings between performance testing software and that of the application.
- Maintain up-to-instance repository of artifacts related to performance test executions.
- Perform initial debugging procedures by reviewing configuration files, logs, or code pieces to determine breakdown source.
- Adhere to defect tracking process; document software defects, using a defect tracking tool (Quality Center), monitor the progress in a timely manner, escalate aging and priority defects.
- Timely and accurate communication of testing events, daily status, and test execution results, etc.

Quality Assurance Analyst Skills & Qualifications:
Bachelor's Degree or military experience, Minimum 3 years of experience, Applicants must be authorized to work in the US without requiring employer sponsorship currently or in the future. Specialized Knowledge & Skills, Experience with system resources measurement, Experience with relational databases (IBM Rational), Experience with SQL Query tools, Experience with Agile Scrum methodology, Experience with ALM or other Open Source Testing tools, Experience with ALM, Rally, Jira or other Open Source Testing tools.

Compliance Manager

Job ID - 58
Compliance Manager Responsibility:
Support the development, implementation, and maintenance of NERC/NIST Compliance processes. Assist with the development and implementation of architecture, programs, and procedures to maintain compliance with utilities compliance requirements. Collect, review, and insure evidence (procedures, policies, reports, data, etc.) in accordance with public utility regulatory requirements. Perform analyses of requirements, events, and evidence to assist Requirement Owners (RO) and Subject Matter Experts (SMEs) with project deliverables, milestones, and compliance documentation.

Compliance Job Duties:

- Partner with operational management to ensure consistent compliance with applicable requirements; help evaluate compliance operational performance, coordinate on issue management mitigation plans, as needed and respond to inquiries on compliance and readiness audits.
- Recognize, identify and escalate compliance or process related risks.
- Evaluate and provide recommendations for risk mitigation or enhancements to policies, controls, processes and/or procedures to meet business expectations and obligations.
- Help internal resources in the drafting of NERC RSAWs (Reliability Standard Auditor Worksheet) as needed to clearly state and explain objectives to ensure compliance.
- Assist subject matter experts and requirement owners with interpreting requirements, determining compliance to the requirement, evaluating evidence, and building controls, policies, and procedures to ensure compliance.
- Understand and apply internal control concepts to plan, perform, and report on the evaluation of various business processes/areas/ functions.
- Communicate procedures, findings, results, statuses, and recommendations up and across the organization.

- Demonstrate high-quality teamwork, interpersonal, resiliency and self-management capabilities.

Compliance Manager Skills & Qualifications:
Bachelor's degree in Engineering, Information Technology, or related field (required); at least five years of related compliance, audit, project management, and/or business partnering experience (required); working knowledge of NERC CIPv5 regulations and experience in supporting a NERC audit; working knowledge of SSAE16 SOC1 standards; strong functional knowledge of process improvement and compliance assurance methodologies; strong communication skills (oral, written, and discernment); capable of reviewing regulatory requirements, data, and evidence, and creating reports, with strong attention to detail; specific experience within highly regulated environments; capable of leading without authority and self-motivated.

SOW Appendix 4 – ICT Labor and Technical Resources Summary and Job Descriptions

Role Summary

Below is a summary of the Technical Resource roles:

Role	Job ID
Cyber Lab DevOps Engineer	TR-01
Cyber Lab Systems Engineer (platforms)	TR-02
Infrastructure Specialist (Backups, Data Protection)	TR-03
Infrastructure Specialist (Data Center Technology Engineer)	TR-04
Lead Monitoring Analyst	TR-05
Monitoring Analyst	TR-06
Senior Network Architect	TR-07
Sr. Platform Support Specialist - Network	TR-08
Systems Engineer (platforms)	TR-09
Systems Engineer Unix-Linux	TR-10
Principal Network Security Engineer/ Specialist	TR-11

Role Descriptions

Cyber Lab DevOps Engineer

Job ID: TR-01

Contractor shall provide a Cyber Lab DevOps Engineer who understands current DevOps methodologies and Hyper-Converged Infrastructure (HCI) /virtualization best practices (including automation of virtual machines).

Design lab automation techniques that support all phases of the DevOps life cycle; troubleshoots system/application issues related to the lab automation and ensure that the stakeholder security requirements necessary to protect the organization’s mission and business processes are adequately addressed in all aspects of application architecture.

The Cyber Lab DevOps Engineer shall:

- Design modeling and building use cases (e.g., unified modeling language).
- Apply best-practice methods, standards, and approaches for describing, analyzing, and documenting Customer's application architecture.

- Optimize application architecture to meet performance requirements.
- Execute application integration processes and build application architectures and frameworks.
- Apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
- Define and prioritize essential application capabilities or business functions required for partial or full system restoration after a catastrophic failure event.
- Define appropriate levels of application availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.
- Develop/integrate cybersecurity designs for applications with multilevel security requirements.
- Ensure that acquired or developed application(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines.
- Perform security reviews, identify gaps in application architecture, support risk management.
- Support activities requiring costs, design concepts/ changes to the application architecture.
- Provide input on application security requirements to be included in statements of work and other appropriate procurement documents.
- Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).
- Define and document how the implementation of a new application or new interfaces between applications impacts the security posture of the current environment.
- Analyze application architectures, allocate security services, and select security mechanisms.
- Develop an application security context, a preliminary applications security Concept of Operations (CONOPS), and define baseline applications security requirements in accordance with applicable cybersecurity requirements.
- Evaluate applications architectures to determine adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents.
- Analyze user needs and requirements to plan application architecture.
- Develop application architecture and/or components required to meet user needs.
- Document and update as necessary all application definition and architecture activities.
- Determine the protection needs (i.e., security controls) for the application architecture and document appropriately.

Skills and Qualifications:

Education Required:

- Two-year degree in Computer Science, Engineering, Business, or related field combined with 5 years of relevant experience
- BA/BS degree in Computer Science, Engineering, Business, or related field
- 3 years of DevOps experience
- 5 years of OT/IT/Enterprise architecture and program implementation experience
- Note: Will consider additional years of relevant experience and/or related technical certifications in lieu of degree requirement (in accordance with the FLSA Computer Professionals Exemption)

Experience Required:

- Knowledge of installation, integration, and optimization of applications using DevOps methodologies
- Hyper-converged Infrastructure (HCI) and automation of virtual environments
- Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
- Knowledge of lab management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.
- Knowledge of confidentiality, integrity, and availability requirements.
- Knowledge of multi-level security systems and cross domain solutions.
- Knowledge of application protection planning (e.g. OT supply chain security/risk management policies, anti-tampering techniques, and requirements).

Experience Desired:

- Knowledge of Customer's information classification program and procedures for information compromise.
- Familiarity with laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- Knowledge of key concepts in security management (e.g., Release Management, Patch Management).
- Knowledge of security system design tools, methods, and techniques.
- Knowledge of software engineering.
- Knowledge in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.
- Knowledge of system fault tolerance methodologies.
- Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression).
- Knowledge of demilitarized zones.

- Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
- Knowledge of application design processes, to include understanding of security objectives, operational objectives, and trade-offs.

Cyber Lab Systems Engineer (platforms)

Job ID: TR-02

Contractor shall provide a Cyber Lab Systems Engineer (Platforms) who understands current Hyper-Converged Infrastructure (HCI) and virtualization best practices (including automation of virtual machines).

Supports lab automation technologies and works on the capabilities needed for all phases of the testing life cycle; troubleshoots system/application issues related to the lab and ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of application architecture.

The Cyber Lab Systems Engineer shall perform the following Services:

- Design modeling and building use cases (e.g., unified modeling language).
- Apply best-practice methods, standards, and approaches for describing, analyzing, and documenting Customer's application architecture.
- Optimize application architecture to meet performance requirements.
- Execute application integration processes and build application architectures and frameworks.
- Apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
- Define and prioritize essential application capabilities or business functions required for partial or full system restoration after a catastrophic failure event.
- Define appropriate levels of application availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.
- Develop/integrate cybersecurity designs for applications with multilevel security requirements.
- Ensure that acquired or developed application(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines.
- Perform security reviews, identify gaps in application architecture, support risk management.
- Support activities requiring costs, design concepts/ changes to the application architecture.
- Provide input on application security requirements to be included in statements of work and other appropriate procurement documents.

- Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).
- Define and document how the implementation of a new application or new interfaces between applications impacts the security posture of the current environment.
- Analyze application architectures, allocate security services, and select security mechanisms.
- Develop an application security context, a preliminary applications security Concept of Operations (CONOPS), and define baseline applications security requirements in accordance with applicable cybersecurity requirements.
- Evaluate applications architectures to determine adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents.
- Analyze user needs and requirements to plan application architecture.
- Develop application architecture and/or components required to meet user needs.
- Document and update as necessary all application definition and architecture activities.
- Determine the protection needs (i.e., security controls) for the application architecture and document appropriately.

Skills and Qualifications:
Education Required:

- Two-year degree in Computer Science, Engineering, Business, or related field combined with 5 years of relevant experience
- BA/BS degree in Computer Science, Engineering, Business, or related field
- 3 years in Operational Technology Security
- 5 years of OT/IT/Enterprise architecture and program implementation experience
- Note: Will consider additional years of relevant experience and/or related technical certifications in lieu of degree requirement (in accordance with the FLSA Computer Professionals Exemption)

Experience Required:

- Knowledge of installation, integration, and optimization of OT applications and components.
- Hyper-converged Infrastructure (HCI) and automation of virtual environments
- Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
- Knowledge of technologies such as Vmware/Vcenter, Microsoft Active Directory, Reh Hat Enterprise Linux, iDRAC).
- Knowledge of lab management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.

- Knowledge of confidentiality, integrity, and availability requirements.
- Knowledge of multi-level security systems and cross domain solutions.
- Knowledge of application protection planning (e.g. OT supply chain security/risk management policies, anti-tampering techniques, and requirements).

Experience Desired

- Knowledge of Customer's information classification program and procedures for information compromise.
- Familiarity with laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- Knowledge of key concepts in security management (e.g., Release Management, Patch Management).
- Knowledge of security system design tools, methods, and techniques.
- Knowledge of software engineering.
- Knowledge in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.
- Knowledge of system fault tolerance methodologies.
- Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression).
- Knowledge of demilitarized zones.
- Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
- Knowledge of application design processes, to include understanding of security objectives, operational objectives, and trade-offs

Infrastructure Specialist (Backups, Data Protection)

Job ID: TR-03

Contractor shall provide an Infrastructure Specialist (Backups, Data Protection) who shall Define, maintain, and support Operational Smart Grids (OSG) infrastructure operational policies, standards, best practices, procedures, tools, and projects in support of efficient, resilient, and secure operations of OSG supported applications and facilities.

Work with technical teams and external vendors to provide project and/or operational support for enterprise backup/data protection. Monitor operational performance to identify opportunities for improvement.

Align the operational requirements with relevant global/corporate operational requirement(s), security framework(s) and/or associated regulatory compliance.

- Provide timely responses to all incidents, tasks and requests assigned to meet Service Level Agreements.
- Work with internal clients, suppliers/contractors, project teams and other technical staff to identify, design and support technical solutions.
- Coordination, provisioning, and installation of equipment at all data center locations
- Provide input into design of environments for improvements or project needs
- Provide maintenance of infrastructure technologies following the change management process.
- Lead the technical implementation plans in support of infrastructure technologies.
- Maintain regulatory compliance under NERC-CIP guidelines.
- Responsible for day-to-day operations and/or deployment/provisioning of data protection clients, hardware, and backup policies.
- Perform scheduled recovery tests and maintain/update recovery documentation.
- Data Center Information Management (DCIM) and automation tools.
- Perform/coordinate special assignments from OSG Infrastructure Management.
- Provide 24x7 on call support.
- Provide professional and technical mentoring for team members.
- Travel as required within the US

Skills and Qualifications:

Education: BS/BA Degree in Business, Computer Science, or other technical discipline. Will consider additional years of relevant experience (10+ years) and/or related technical certifications in lieu of degree requirement (in accordance with the FLSA Computer Professionals Exemption)

Education and Experience Requirements (Meet at least one of the following):

- AS Technical Related Degree with 8 years of technical experience
- BS Technical Related Degree with 6 years of technical experience
- MS Technical Related Degree with 4 years of technical experience

Experience Required:

- Experience with Linux/Unix system administration.
- Experience with Automation tools and scripting.
- Experience with Backup/Data Protection platforms and administration

- Working knowledge of the regulatory environment for utility companies including NERC CIP. (preferred)

Other Experience:

- Position requires a minimum of four (4) years of experience working with infrastructure solutions in an enterprise environment.
- Position requires professional experience with Veritas NetBackup, Unix and Linux OS, Windows OS, Storage, and Technical Project Coordination.
- Fundamental understanding of Networking, Active Directory, and VMware.

Key Technical Working Skills:

- In-depth knowledge of Data Protection Platforms (esp. Veritas NetBackup)
- In-depth knowledge of Unix and Linux operating systems (esp. Oracle Solaris 10/11, Red Hat 6, 7, and 8)
- In-depth knowledge of professional standards and trends within areas of expertise.
- researching and developing policies, standards, and procedures
- automation tools\scripting at an intermediate to expert level
- Must possess ability to deal collaboratively, diplomatically, and successfully with customers, co-workers and other professional colleagues, managers, and staff.
- Must be able to work effectively in a team environment, as well as work independently with limited supervision.
- Must have excellent problem-solving skills while providing first class customer service. Requires outstanding oral and written communication skills.
- Each employee must accept responsibility for their own safety and health as well as the safety and health of their fellow employees.

Infrastructure Specialist (Data Center Technology Engineer)

Job ID: TR-04

Contractor shall provide an Infrastructure Specialist (Data Center Technology Engineer) who shall Define, maintain, and support of Operational Smart Grids (OSG) infrastructure operational policies, standards, best practices, procedures, tools, and projects in support of efficient, resilient, and secure operations of OSG supported applications and facilities.

Work with technical teams and external vendors to provide operational support for a diverse set of operational enterprise services. Monitor operational performance to identify opportunities for improvement.

Align the operational requirements with relevant global/corporate operational requirement(s), security framework(s) and/or associated regulatory compliance.

Duties:

- Provide timely responses to all incidents, tasks and requests assigned to meet Service Level Agreements.
- Work with internal clients, suppliers/contractors, project teams and other technical staff to identify, design and support technical solutions.
- Installation of server racks, PDUs, servers, switches, storage, appliances, etc. including racking, stacking, labeling, cabling, initial config, and documentation
- Maintain spare parts, cables, and equipment inventories
- Maintain organized and clean inventory, storage, and datacenter spaces
- Supervise on-site vendor support and contractors doing work in datacenter spaces
- Provide maintenance and break-fix of infrastructure technologies following the change management process.
- Coordinate maintenance and break-fix of facility items with General Services
- Participates in the technical implementation plans in support of infrastructure technologies.
- Support physical and virtual infrastructure, including all existing physical and virtual systems, installation of additional systems, patching, maintenance, upgrades, and support.
- Participates in the evaluation, selection, and testing of hardware and software products.
- Maintain regulatory compliance under NERC/CIP guidelines.
- Maintain high quality security controls surrounding the critical SCADA systems.
- Perform special assignments form OSG Infrastructure Manager.
- Provide first shift weekday on-site support including for Outage Management applications and storm room.
- Available 24x7 for on call support including for Outage Management applications and storm room.
- Must be able to lift a weight of 50 pounds

Skills and Qualifications:

Education: BS/BA Degree in Business, Computer Science, or other technical discipline. MA/MS Degree preferred. Will consider additional years of relevant experience and/or related technical certifications in lieu of degree requirement (in accordance with the FLSA Computer Professionals Exemption)

Education and Experience Requirements (Meet at least one of the following):

- 12 years of technical experience
- AS Technical Related Degree with 8 years of technical experience.

- BS Technical related Degree with 5 years of technical experience
- MS Technical related Degree with 2 years of technical experience

Experience Required:

Position requires a minimum of (2) years' experience working with infrastructure solutions in an enterprise environment. Position requires professional experience with more than one of the following areas: Data Center Operations, Data Protection Platforms, Infrastructure Operational Policies & Procedures, and/or Technical Project Coordination. Fundamental understanding of UNIX Operating Systems (OS), Linux OS, Microsoft OS, Active Directory, VMware, Citrix, Networking, Routing, Firewalls, Security tools and/or scripting. (Associated certifications are preferred.)

Other Experience:

- Must possess ability to deal collaboratively, diplomatically, and successfully with customers, co-workers and other professional colleagues, managers, and staff.
- Must be able to work effectively in a team environment, as well as work independently with limited supervision.
- Must have excellent problem-solving skills while providing first class customer service. Requires outstanding oral and written communication skills.
- Each employee must accept responsibility for their own safety and health as well as the safety and health of their fellow employees.

Key Technical Working Skills:

- Knowledge Data Center terminology and standards including ability to recognize different kinds of cables, connectors, SFPs etc.
- Perform daily site inspections of all Mechanical & Engineering (M&E) systems and technical equipment, including servicing and maintenance.
- Under close supervision, complete assigned work according to established processes and procedures in accordance with Avangrid's, Health and Safety Policy - ensuring all safety processes and PPE requirements are followed. Also, ensure all regulatory requirements and quality standards are met.
- Oversee third-party vendors, ensuring compliance with Customer's developed processes, procedures, and all applicable laws/regulations. Accompany vendors on site visits on an as needed basis and ensure site standards are met.
- Help create and develop work processes, Job Hazard Analysis reports, and SOPs for critical work with risk assessment. Ensure that documents and logbooks are updated.
- Complete all required training to ensure successful completion of all job-related responsibilities
- May provide informal assistance such as technical guidance and/or training to coworkers.

- Understanding of Security, computer hardware, software applications and data communication equipment.
- Network diagrams, firewall rules, ports, and services
- Understanding of relevant Compliance Regulations and Policies. (NERC-CIP, Etc.)
- The ability to demonstrate good communication skills both written and orally. This communication would be with team members, other departments, regulating authorities and leadership local and abroad.
- Experience to make sound decisions while working in a high-pressure environment outside normal hours.
- Working in storm or other emergency conditions for 24x7x365 system support
- Must be able to work independently and contribute proactively to drive results
- Ensures quality even on the most complex tasks or projects

Lead Monitoring Analyst
Job ID: TR-05

Contractor shall provide a Lead Monitoring Analyst who shall be in either Rochester (NY) or Orange (CT), shall be responsible for the day-to-day activities involved in both reactive Network Monitoring and Incident Management. The Lead Monitoring Analyst shall demonstrate proficiency in log analysis, discovery tools and network monitoring and detection tools and take initiative on projects, proactively identify process deficiencies, and make recommendations to resolve them, and work effectively both autonomously and within a team.

The Lead Monitoring Analyst shall perform the following Services:

- Identify and implement improvements to services and tools (SIEM, and other tools)
- Provide support to develop and continuously improvement to SIEM through (creating play books, run books, monitoring)
- Develop dashboard and views for team and Management
- Work with team to Implement efficient event monitoring, processes improvement and automation
- Perform daily health checks through suite of tools
- Develop and drive new automation to reduce failures and improve overall performance of SIEM and networking tools
- Mentor and lead others through tasks, obstacles and problem solving
- Participate in the governance of application and infrastructure monitoring design, implementation, customization, and support
- Detect, analyze, and remediate malicious network traffic, Identify, and contain threats
- Review suspicious patterns and signatures within network traffic
- Strong understanding of SIEM, Network Monitoring, IDS, IPS and associated technologies

- Assist in the investigation of equipment failures, network anomalies
- Analyze system data and reports to identify compliance gaps and issues related to operational processes
- Understands Incident Management processes and escalation processes
- Grow the technical skillset through online training and self-motivated personal improvement
- Willing to work 1st, 2nd or 3rd shift and weekends

Skills and Qualifications:

- Prior eexperience in Networking, Network Monitoring, or Incident Response
- Experience in well-known and/or open-source Network and Host forensic tools
- Able to manage self and others under stress
- General networking knowledge – TCP/IP protocols, OSI model, Firewalls, other networking devices
- Mentor
- Previous experience with ticketing systems
- Preferred experience with case management tools
- Proven track record of leadership skills, mentoring others along with meeting standards and meeting leadership goals
- Strong customer service skills and decision-making skills
- Good analytical skills – ability to analyze and think out of the box when working a security event
- Self-motivated, methodical and detail oriented
- Familiarity with regulatory requirements such as NERC/CIP, SOX etc. (preferred)
- Utility Industry experience (preferred)

Education and Experience Requirements (Meet at least one of the following):

- 10+ years prior experience in networking, network monitoring and incident response and familiarity with NIST standards
- Associate degree in Computer Science or related program with 6+ years relevant work experience in security information technology or incident response
- Bachelor's degree in computer science or related program with 2+ years relevant work experience in security information technology or incident response

Qualifications for SIEM monitoring role:

- 4+ years' experience with monitoring tools

- Experience with SIEM (creating playbooks, Run books and monitoring)
- Strong relationship management abilities, analytical and problem-solving skills
- Experience with Incident management process and procedures
- A strong team player, can work under pressure and ability to multi-task

Monitoring Analyst

Job ID:TR-06

Responsibilities:

Located in either Rochester (NY) or Orange (CT), this position will be responsible for the day-to-day activities involved in both reactive Network Monitoring and Incident Management. A candidate for this role should demonstrate proficiency in log analysis, discovery tools and network monitoring and detection tools. Furthermore, they should be able to take initiative on projects, proactively identify process deficiencies and make recommendations to resolve them and work effectively both autonomously and within a team.

Duties:

- Ability to identify and implement improvements to services and tools (SIEM, and other tools)
- Provide support to develop and continuously improvement to SIEM through (creating play books, run books, monitoring)
- Development of dashboard and views for team and Management
- Work with team to Implement efficient event monitoring, processes improvement and automation
- Perform daily health checks through suite of tools
- Develop and drive new automation to reduce failures and improve overall performance of SIEM and networking tools
- Participate in the governance of application and infrastructure monitoring design, implementation, customization, and support
- Detect, analyze, and remediate malicious network traffic, Identify, and contain threats
- Review suspicious patterns and signatures within network traffic
- Strong understanding of SIEM, Network Monitoring, IDS, IPS and associated technologies
- Assist in the investigation of equipment failures, network anomalies
- Analyze system data and reports to identify compliance gaps and issues related to operational processes
- Understands Incident Management processes and escalation processes
- Grow the technical skillset through online training and self-motivated personal improvement

- Willing to work 1st, 2nd or 3rd shift and weekends

Skills and Qualifications:

- Experience in well-known and/or open-source Network and Host forensic tools
- Able to manage self and others under stress
- General networking knowledge – TCP/IP protocols, OSI model, Firewalls, other networking devices
- Strong customer service skills and decision-making skills
- Good analytical skills – ability to analyze and think out of the box when working a security event
- Self-motivated, methodical and detail oriented
- Familiarity with regulatory requirements such as NERC/CIP, SOX etc. (preferred)
- Utility Industry experience (preferred)

Education and Experience Requirements (Meet at least one of the following):

- 4 years prior experience in networking, network monitoring and incident response and familiarity with NIST standards
- Associate degree in computer science or related program with 2+ years relevant work experience in security information technology or incident response
- Prior experience in Networking, Network Monitoring, or Incident Response

Qualifications for SIEM monitoring role:

- 1-3 years' experience with monitoring tools
- Experience with SIEM (creating playbooks, Run books and monitoring)
- Strong relationship management abilities, analytical and problem-solving skills
- Experience with Incident management process and procedures
- A strong team player, can work under pressure and ability to multi-task

Senior Network Architect

Job ID: TR-07

Contractor Shall provide a Senior Network Architect who shall perform enterprise planning, engineering, and diagnostics for Point to Multipoint Radio, Microwave, Fiber Optic, IP networks and provide level 3 engineering support on an after- hours on-call basis.

The Senior Network Architect shall perform the following Services:

- Support, analysis, scheduling, acquisition, implementation, and documentation of microwave, fiber and IP communications hardware, software, and facilities for assigned projects.
- Resolves complex technical facility, hardware, and software problems utilizing a variety of hardware and software testing tools.
- Manages and maintains up-to-date documentation and procedures that define the operability of the microwave, fiber an IP networking system.
- Identifies and evaluates new Microwave, Fiber and IP technologies and products.
- Monitors system performance and ensures capacity planning is performed by assessing and making recommendations for improvement.
- Interfaces with field technicians and Network Operations Center (NOC) to ensure proper escalation during outrages or periods of degraded system performance.
- Lead Telecom Request for Proposal (RFP) development efforts.
- Direct engineering/construction contracting firms and ensure successful achievement of project goals.
- May function as a lead position providing guidance, coordination, and training for field technicians.

Skills and Qualifications:

BS/BA Degree in a technical field

5 - 7 years' experience in a network engineering/planning role

Demonstrated knowledge of Microwave and SONET network systems, i.e. system installation and configuration.

Demonstrated project management experience.

Proficiency in the design, configuration, and implementation of SONET and Microwave Systems.

Project management skills including scheduling, cost tracking, development of task plans, and progress/status reporting.

Competencies:

- Good oral and written communication skills.
- Problem solving and analytical skills.
- Ability to multitask.
- Interpersonal and Communication Skills.
- Must be a proven team player to work, promote and consolidate efficient team working relationships.

Senior Platform Support Specialist - Network

Job ID: TR-08

Contractor shall provide a Senior Platform Support Specialist – Network, who shall maintain and support of OSG infrastructure and applications. Direct works with other technical teams and external vendors to provide operational support for routers, switches, firewalls, load balancers, and other enterprise network or security services.

The Senior Platform Support Specialist shall:

- Provide timely responses to all incidents, tasks and requests assigned to meet Service Level Agreements.
- Work with internal clients, suppliers/contractors, project teams and other technical staff to support technical solutions.
- Provide maintenance of infrastructure technologies following the change management process.
- Participate in or lead the technical implementation plans in support of infrastructure technologies.
- Support physical and virtual infrastructure, including all existing physical and virtual systems, installation of additional systems, patching, maintenance, upgrades and support.
- Create and maintain secure access on various systems.
- Assist in the evaluation, selection, and testing of hardware and software products.
- Maintain regulatory compliance under NERC/CIP guidelines.
- Maintain high quality security controls surrounding the critical SCADA systems.
- Provide 24x7 on call support.

Skills and Qualifications:

Education: BS/BA Degree in Business, Computer Science or other technical discipline. Requires a minimum of seven (7) years of experience working with infrastructure solutions in an enterprise environment. Requires professional experience with one or more of the following: Network Operating Systems, Firewall Operating systems, Networking Protocols, Security Practices and scripting; Some experience with Linux Operating Systems (OS), Microsoft OS, Active Directory, VMware, Citrix, and Monitoring/Trending solutions preferred. Certifications in Cisco, Checkpoint, Palo Alto, Citrix, F5 and/or other network/security technologies are preferred.

Systems Engineer (platforms)

Job ID:TR-09

Contractor shall provide a Systems Engineer (platforms) who shall analyze, integrate and build upon the shared platform aggregating the tools, services and workflows that encompass the platform's infrastructure, applications, and strategic security in support the changing needs of our customers across the organization with a focus on cyber security.

The System Engineer shall:

- Perform functional analysis and complex system decomposition into manageable sub-systems

- Translate technology and environmental conditions (e.g., law and regulation) into system and security designs and processes
- Communicate with stakeholders to identify what they want to accomplish within a system
- Develop system concepts, requirements documents, statements of work (SOW), block diagrams, data-flow diagrams, UML type diagrams, and other documentation to support the Cyber Architecture team
- Prepare bills of material (BOM) and/or other forms of documentation conforming to accepted standards and practices
- Design and implement scalable and reliable system in coordination with appropriate personnel including architects, engineers, etc. to ensure that the solutions developed meet the needs of the respective project
- Assist in the coordination of various teams testing and evaluating for the development of design and its implementation of the best output
- Develop/integrate cybersecurity designs for systems with multilevel security requirements
- When applicable, install, configure, and test operating systems, applications, software, hardware and system management tools and leverage IT staff for routine tasks by clearly documenting design, maintenance, and support procedures
- Provide work status updates to team members and to management
- Perform department tasks related to configuration management
- Respond to requests for information from both internal and external teams
- Participate in design review meetings as required
- Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.
- Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.
- Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle.
- Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines.
- Identify and prioritize critical business functions in collaboration with organizational stakeholders
- Provide advice on project costs, design concepts, or design changes
- Provide input on security requirements to be included in statements of work and other appropriate procurement documents
- Test software routinely for bugs, redundancies, and security issues

- Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).
- Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.
- Analyze candidate architectures, allocate security services, and select security mechanisms.
- Develop a system security context, a preliminary system security Concept of Operations (CONOPS) and define baseline system security requirements in accordance with applicable cybersecurity requirements.
- Write detailed functional specifications that document the architecture development process.
- Analyze user needs and requirements to plan architecture.
- Develop operational technology architecture or system components required to meet user needs.
- Document and update as necessary all definition and architecture activities.
- Determine the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately.
- Translate proposed capabilities into technical requirements.
- Assess and design security management functions as related to cyberspace
- Standardize and automate processes using scripting technology
- Conduct high-level root-cause analysis of service interruptions and establish preventive measures

Skills and Qualifications:

- Experience in Systems Engineering or related systems development including requirement development, functional analysis & decomposition, and concept design.
- Proficient in Cybersecurity Solution Architecture discipline, concepts, and best practices
- Multi-level security systems and cross domain solutions
- Installation, integration, and optimization of system components
- Industry-standard and organizationally accepted principles and methods
- Cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
- Operating systems & common platform applications
- Security system and software design tools, methods, and techniques
- Systems testing and evaluation methods
- Cyber threats and vulnerabilities.

Education Required:

- Two-year degree in Computer Science, Engineering, Business, or related field combined with 15 years of relevant experience
- BA/BS degree in Computer Science, Engineering, Business, or related field
- 5 years in Operational Technology Security
- 10 years of OT/IT/Enterprise architecture and program implementation experience
- Note: Will consider additional years of relevant experience and/or related technical certifications in lieu of degree requirement (in accordance with the FLSA Computer Professionals Exemption)

Experience Desired:

- Analysis and augmentation of critical infrastructure systems with information communication technology that were designed without system security considerations
- Operational Technology (OT) architectural concepts and patterns (e.g., baseline, validated design, and target architectures.)
- Familiarity with laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- Network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- Computer networking concepts, protocols, and network security methodologies.
- Physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.
- Demilitarized zones (DMZ)
- Organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions)
- Network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools
- Network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services and network security (e.g., encryption, firewalls, authentication, honeypots, perimeter protection)
- Programming languages, operating systems, current equipment and technologies, enterprise backup and recovery procedures, system performance-monitoring tools, active directories, virtualization, HTTP traffic, content delivery, and caching
- Project management, application design and integration, and cloud computing (specifically AWS and Microsoft Azure)
- Familiarity with cybersecurity concepts and implementations
- Familiarity with SCADA and ICS systems in the Energy Sector
- Familiarity with UML type diagrams

Systems Engineer Unix-Linux

Job ID: TR-10

Contractor shall provide a Systems Engineer Unix-Linux, who shall define, maintain, and support of Operational Smart Grids (OSG) infrastructure operational policies, standards, best practices, procedures, tools, and projects in support of efficient, resilient, and secure operations of OSG supported applications and facilities.

Works with technical teams and external vendors to provide project and/or operational support for a diverse set of enterprise services. Monitor operational performance to identify opportunities for improvement. Align the operational requirements with relevant global/corporate operational requirement(s), security framework(s) and/or associated regulatory compliance.

The System Engineer shall:

- Provide timely responses to all incidents, tasks and requests assigned to meet Service Level Agreements.
- Work with internal clients, suppliers/contractors, project teams and other technical staff to identify, design and support technical solutions.
- Coordinate, provision, and install equipment at all data center locations
- Provide input into design of environments for improvements or project needs
- Provide maintenance of infrastructure technologies following the change management process.
- Lead the technical implementation plans in support of infrastructure technologies.
- Maintain regulatory compliance under NERC-CIP guidelines.
- Provide day-to-day operations and/or deployment/provisioning of Unix/Linux, storage, and data protection servers and appliances.
- Data Center Information Management (DCIM) and automation tools.
- Perform/coordinate special assignments from OSG Infrastructure Management.
- Provide 24x7 on call support.
- Provide professional and technical mentoring for team members.
- Travel as required within the US

Skills and Qualifications:

Education: BS/BA Degree in Business, Computer Science or other technical discipline. Will consider additional years of relevant experience (10+ years) and/or related technical certifications in lieu of degree requirement (in accordance with the FLSA Computer Professionals Exemption)

Education and Experience Requirements (Meet at least one of the following):

- AS Technical Related Degree with 8 years of technical experience
- BS Technical Related Degree with 6 years of technical experience
- MS Technical Related Degree with 4 years of technical experience

Experience Required:

- Experience with Linux/Unix system administration.
- Experience with Automation tools and scripting.
- Experience with backup and storage platforms
- Working knowledge of the regulatory environment for utility companies including NERC CIP. (preferred)

Other Experience:

- Position requires a minimum of four (4) years of experience working with infrastructure solutions in an enterprise environment.
- Position requires professional experience with Unix and Linux OS, Data Protection Platforms, Storage, and Technical Project Coordination.
- Fundamental understanding of Networking, Active Directory, and VMware.

Key Technical Working Skills:

- In-depth knowledge of Unix and Linux operating systems (esp. Oracle Solaris 10/11, Red Hat 6, 7, and 8)
- In-depth knowledge of professional standards and trends within areas of expertise.
- Veritas data protection platform
- Oracle X86 Servers, ZFS, Exadata
- researching and developing policies, standards, and procedures
- automation tools\scripting at an intermediate to expert level
- Must possess ability to deal collaboratively, diplomatically, and successfully with customers, co-workers and other professional colleagues, managers, and staff.
- Must be able to work effectively in a team environment, as well as work independently with limited supervision.
- Must have excellent problem-solving skills while providing first class customer service. Requires outstanding oral and written communication skills.
- Each employee must accept responsibility for their own safety and health as well as the safety and health of their fellow employees.

Principal Network Security Engineer/Specialist

Job ID: TR-11

Position Responsibilities:

- Provide timely responses to all incidents, tasks and requests assigned to meet Service Level Agreements.
- Work with internal clients, suppliers/contractors, project teams and other technical staff to identify, design and support technical solutions.
- Design, plan and implement changes to the environment for improvements or projects
- Provide maintenance of infrastructure technologies following the change management process
- Lead the technical implementation plans in support of infrastructure technologies
- Leads others to solve problems
- Leads contractors to deliver services to projects and or operational duties as needed
- Leads functional teams or projects as assigned
- Lead the evaluation, selection, and testing of hardware and software products
- Maintain regulatory compliance under NERC/CIP guidelines
- Maintain high quality security controls surrounding the critical SCADA systems
- Perform/coordinate special assignments from OSG Infrastructure Management
- Provide 24x7 on call support
- Provide professional and technical mentoring for team members

Skills and Requirements

JOB REQUIREMENTS:
Education and Experience Required:

- BS Technical Related Degree with 15+ years' technical experience
- Position requires a minimum of twelve (12) years' experience working with infrastructure solutions in an enterprise environment
- Position requires professional experience with more than one of the following areas:
    - Data Center Operations, Disaster Recover/Business Continuity Planning & Execution, Security & Compliance Management, Infrastructure Operational Policies & Procedures, and/or Technical Project Coordination
- Position requires Operational experience in an Enterprise Environment configuring and maintaining Cisco Routers/Switches/Firewalls such as Cisco Nexus 9K, Cisco Catalyst, Cisco ASR Routers, Cisco 4K Routers, Cisco ISE, Cisco Firepower, Cisco ASA
- Position requires Operational experience in an Enterprise Environment configuring and maintaining Next generation firewalls such as Checkpoint and Palo Alto

Skills/ Abilities:

- Expert within network infrastructure, operations & network security
- Proficient in professional standards and trends within area of expertise
- Proficient in deploying Checkpoint, Palo Alto, Cisco ASA firewalls along with implementing VPN's
- Knowledge of multiple security technologies, to include network security, NAC, Micro segmentation, network security architecture

- Implementing security technologies such as SAML and PKI Infrastructure
- Network Access Control systems in a large enterprise
- Experience with authentication systems such as RADIUS, TACACS+, SSO, LDAP Experience planning, researching, and developing security policies, standards, and procedures
- Experience with architecting in cloud environments (AWS, Azure, and GCP)
- SD-WAN and other tunneling\encryption transport technologies
- Network Security Automation and DevOps
- Strong Routing and Switching experience (BGP, OSPF, VPC, VXLAN, vain traffic engineering, Multicast, etc.

Desired Skills/ Abilities:

- Experience with packet capture software such as Wireshark, WinDump, tcpdump, etc.
- Experience with installing and configuring Citrix Netscalers in an Enterprise High Availability environment
- Experience with installing and configuring Cisco ISE in a distributed deployment with multiple personas
- Experience with Zero Trust Architecture
- Experience working in a regulated environment
- NERC/CIP experience a plus
- Experience with Cisco Nexus Dashboard Fabric Controller (Formerly DCNM)
- Experience using Solarwinds Orion platform suite of tools

*Note: Will consider additional years of relevant experience and/or related technical certifications in lieu of degree requirement (in accordance with the FLSA Computer Professionals Exemption)

SCHEDULE D-4
PRICING TERMS

Solely for the purposes of ASD ICT

1. Prices shall remain firm for orders placed during the term of this Agreement.
2. Payment Terms are Net 60 days from the date of the invoice.
3. Customer does not commit to the ordering of any of the positions below, the fulfillment of the positions will be based on Customer's actual need.

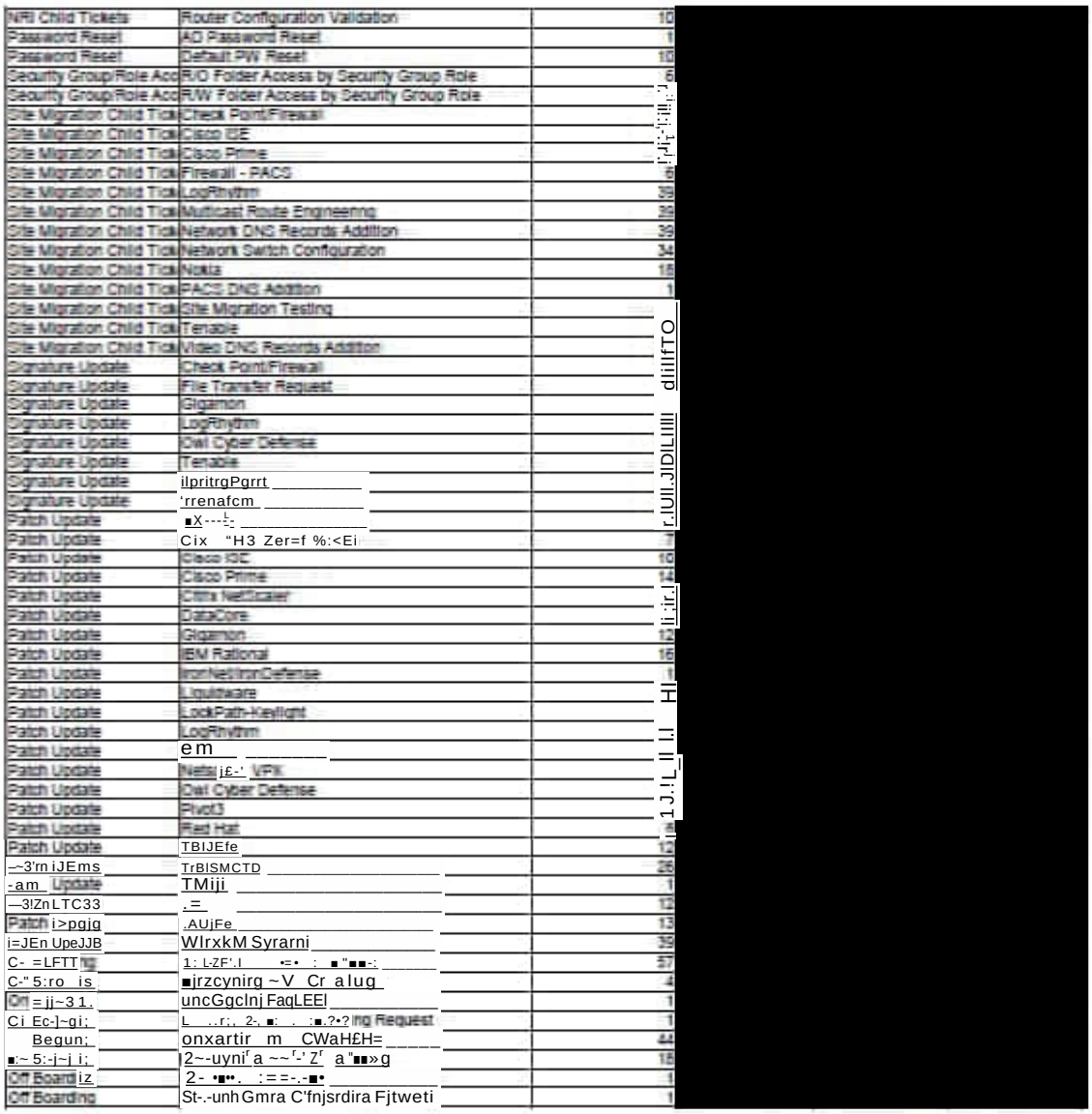
ICT Labor

Role	Job ID	2024 Standard Hourly Rate	2025 Standard Hourly Rate	2026-April 2027 Standard Hourly Rate	2024 Overtime/On Call Hourly Rate	2025 Overtime/On Call Hourly Rate	2026-April 2027 Overtime/On Call Hourly Rate	2024 After Hours Call Out Rate per Call Out	2025 After Hours Call Out Rate per Call Out	2026-April 2027 After Hours Call Out Rate per Call Out
AD/SOL Supervisor	32	[redacted]								
Build Analyst	57									
Build Supervisor	56									
Compliance Analyst	59									
Compliance Manager	58									
Cyber Controls Analyst	63									
Cyber-Applications Analyst	65									
Cyber-Applications Supervisor	64									
ICT cruel Security Architect (Data)	45									
Network Engineer	37									
Network Supervisor	36									
Quality Assurance Analyst	54									
Quality Assurance Supervisor	55									
SQL Database Administrator	24									
Total										

Unitized Work

intio'ji on Fllur Tool

Raquest Typ* - Major	FUqUM4 T,pi - DMcHptlon	PrapMm NumMi or UnrU Annually	2024 Unrl Prlti	MM Unit Prte»	202fi-AprU 2027 Lrnir Prlci
Access Request	Active Directory (AD)	1			
Access Request	AD Password Reset	1			
Access Request	Add/Remove Security Group/Role Members	45			
Access Request	Architecture Reference Guide Access Request	1			
Access Request	Centrify	1			
Access Request	Check Point/Firewall	1			
Access Request	Cisco Prime	1			
Access Request	Create/Modify/Delete Folder	4			
Access Request	Create/Modify/Delete Role	8			
Access Request	Create/Modify/Delete Security Group	7			
Access Request	DEV with Remote Access	4			
Access Request	Dragos	1			
Access Request	Gigamon	2			
Access Request	IBM Rational (RQM)	3			
Access Request	IronNet	1			
Access Request	LockPath (Keylight Service)	14			
Access Request	LogRhythm	4			
Access Request	Microsoft Applications	1			
Access Request	MS SQL	12			
Access Request	Nokia	4			
Access Request	Offboarding infra Child ticket	1			
Access Request	Other Applications	2			
Access Request	OWL	3			
Access Request	PROD Access	11			
Access Request	PROD Shared Document Access Request	1			
Access Request	QA Access	8			
Access Request	Red Hat	2			
Access Request	SolarWinds Help Desk - DMZ	20			
Access Request	SolarWinds Orion	2			
Access Request	SolarWinds Orion - DMZ	4			
Access Request	Tenable	4			
Axes Request	TrendMicro	1			
Access Request	Video DNS Records Addition	1			
Access Request	VMware	1			
Access Request	Windows	3			
>j.- ~ -=e 1- i	Patch Update	1			
Admin Use Only	Signature Update Child Ticket	1			
Asset Management	Onboarding infra Child ticket	1			
Asset Management	Return Equipment/Remove User	1			
;r~: F.i -[x]	Compliance Check	1			
Compliance and QA	Compliance Review	26			
Compliance and QA	Cybersecurity Compliance Check	5			
Compliance and QA	ECR (Exceptional Circumstance Request)	1			
Compliance and QA	Evidence Request	20			
Compliance and QA	File Transfer Request	1054			
Compliance and I-[1]	Product Evaluation	1			
Compliance and QA	QAQC Testing	1			
Cybersecurity Compliand	PROD CZ Cybersecurity Compliance Check - Anti-	8			
Cybersecurity Compliand	PROD CZ Cybersecurity Compliance Check - Liste	3			
Cybersecurity Compliand	PROD CZ Cybersecurity Compliance Check - SIEM	8			
Decomm/Comm/Modify	Decomm/Comm/Modify - Asset Management	1			
Decomm/Comm/Modify	Decomm/Comm/Modify - Cisco ISE	4			
Decomm/Comm/Modify	Decomm/Comm/Modify - Cisco Prime	3			
Decomm/Comm/Modify	Decomm/Comm/Modify - DNS	16			
Decomm/Comm/Modify	Decomm/Comm/Modify - LogRhythm	17			
Decomm/Comm/Modify	Decomm/Comm/Modify - Tenable	17			
Decomm/Comm/Modify	Decomm/Comm/Modify - TrendMicro	14			
Decomm/Comm/Modify	Decomm/Comm/Modify - Veeam	14			
Decomm/Comm/Modify	Infra DEV	9			
,~7.: : . •m/Modify	r*j =~?j	10			
Decomm/Comm/Modify	Infra QA	9			
Decomm/Comm/Modify	Network DEV	2			
Decomm/ 2: -i~i Modify	Network PROD	2			
I-e-xnr 2. 'm/Modify	I -er.'.yi -*	3			
M i ct'iia'niiEi	Check Point/Firewall	10			
N'I CrJldnaxs*	tiaira'tuer	8			



NRI Child Tickets	Router Configuration Validation	10
Password Reset	AD Password Reset	1
Password Reset	Default PW Reset	10
Security Group/Role Acc	R/O Folder Access by Security Group Role	6
Security Group/Role Acc	R/W Folder Access by Security Group Role	
Site Migration Child Tick	Check Point/Firewall	
Site Migration Child Tick	Cisco ISE	
Site Migration Child Tick	Cisco Prime	
Site Migration Child Tick	Firewall - PACS	6
Site Migration Child Tick	LogRhythm	39
Site Migration Child Tick	Multicast Route Engineering	39
Site Migration Child Tick	Network DNS Records Addition	39
Site Migration Child Tick	Network Switch Configuration	34
Site Migration Child Tick	Nokia	16
Site Migration Child Tick	PACS DNS Addition	1
Site Migration Child Tick	Site Migration Testing	
Site Migration Child Tick	Tenable	
Site Migration Child Tick	Video DNS Records Addition	
Signature Update	Check Point/Firewall	
Signature Update	File Transfer Request	
Signature Update	Gigamon	
Signature Update	LogRhythm	
Signature Update	Owl Cyber Defense	
Signature Update	Tenable	
Signature Update	ilpritrgPgrrt	
Signature Update	'rrenafcm	
Patch Update	■X---⊥-	
Patch Update	Cix "H3 Zer=f %:<Ei	1
Patch Update	Cisco ISE	10
Patch Update	Cisco Prime	14
Patch Update	Citrix NetScaler	
Patch Update	DataCore	
Patch Update	Gigamon	12
Patch Update	IBM Rational	16
Patch Update	IronNet/IronDefense	1
Patch Update	Liquitware	
Patch Update	LockPath-Keylight	
Patch Update	LogRhythm	
Patch Update	em	
Patch Update	Netsj j£-' VPX	
Patch Update	Owl Cyber Defense	
Patch Update	Pivot3	
Patch Update	Red Hat	8
Patch Update	TBIJEfe	12
—3'rn iJEms	TrBISMCTD	25
-am Update	TMiji	1
—3!ZnLTC33	.=	12
Patch i>pgjg	.AUjFe	13
i=JEn UpeJJB	WIrxkM Syrarni	35
C- =LFTT'g	1: L-ZF'.I •=• : ■"■■-:	57
C-" 5:ro is	■jrzcynirg ~V Cr alug	4
Ort = jj~31.	uncGgclnj FaqLEEl	1
Ci Ec-]~gi;	L ..r;. 2-. ■: . :■.?•? ing Request	1
Begun;	onxartir m CWaH£H=	44
■:~ 5:-j~j i;	2~-uyni' a ~~'-' Z' a"■■»g	18
Off Board iz	2- •■•. :==-.-■•	1
Off Boarding	St-.-unh Gmra C'fnjsrdira Fjtweti	1

Technical Resources

Role	Job ID	2024 Standard Hourly Rate	2025 Standard Hourly Rate	2026-April 2027 Standard Hourly Rate	2024 Overtime On Call Hourly Rate	2025 Overtime On Call Hourly Rate	2026-April 2027 Overtime.'On Call Hourly Rate	2024 After Hours Call Out Rate per Call Out	2025 After Hours Call Out Rate per Call Out	2026-Aprll 2027 After Hours Call Out Rate per Call Out
Cyber Lab DevOps Engineer	TR-01	[redacted]								
Cyber Lab Systems Engineer (platforms)	TR-02									
Infrastructure Specialist (Backups. Ltata Protection)	TR-03									
Infrastructure Specialist (Data Center Technology Engineer)	TR-Q4									
! '•! • <■"• , Tvst	TR-Q5									
Mr - lj.jrir- j	TR-06									
Senior Network Architect	TR-07									
Sr Platform Supl >rt_Speci ' st - Network	TR-Q8									
Systen r Engineer ijpl.itf r-j	TR-Q9									
Systen t: Engineer I »ri - L l . l . '	TR-10									
Pnndpal Network Security Engineer/ Specialist	TR-11									
Total										

SCHEDULE H-1
DATA SECURITY RIDER

Solely for the purposes of ASD ICT

For the purposes of this Privacy and Data Security Rider (the "Rider") **Avangrid Service Company** and any of its affiliates procuring or receiving services, works, equipment or materials under the Agreement (as defined below) shall be hereinafter referred to as the "CUSTOMER". [redacted] shall be hereinafter referred to as the "VENDOR."

(a) Among other, the purpose of this Rider is to enable the VENDOR to Process on behalf of the CUSTOMER the Personal Data and Company Data necessary to comply with the purpose of the Agreement (as defined below), define the conditions under which the VENDOR will Process the Personal Data and Company Data to which it has access during the performance of the Agreement, and establish the obligations and responsibilities of the VENDOR derived from such Processing. Personal Data disclosed by CUSTOMER to VENDOR is provided only for limited and specified purposes as set forth in the Agreement and this Rider.

(b) The following definitions are relevant to this Rider:

(i) "Personal Data" means any information about an individual, including an employee, vendor, customer, or potential customer of CUSTOMER or its affiliates, including, without limitation: (A) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, biometric records, personal electronic mail address, internet identification name, network password or internet password; (B) information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household, or (C) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information, as well as cookie information and usage and traffic data or profiles, that is combined with any of the foregoing.

(ii) "Company Data" means any and all information concerning CUSTOMER and its affiliates and their respective business in any form, or to which the CUSTOMER or its affiliates have access, that requires reinforced protection measures, including but not limited to CUSTOMER sensitive information (confidential or restricted), internal use information, Personal Data, Cardholder Data, commercially sensitive information, Critical Infrastructure Information, other information that relates to critical infrastructure, information that relates to the operation or functionality of facilities, networks, or grids, commercially sensitive information, strategic business information, credentials, encryption data, system and application access logs, or any other information that may be subject to legal or regulatory requirements.

(iii) "Critical Infrastructure Information" means engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure (physical or virtual) that (A) relates details about the production, generation, transmission, or distribution of energy; (B) could be useful to a person planning an attack on critical infrastructure; (C) is exempt from mandatory disclosure under the

Freedom of Information Act; and (D) gives strategic information beyond the location of the critical infrastructure.

(iv) "Processing" (including its cognate, "process") means any operation, action, error, omission, negligent act, or set of operations, actions, errors, omissions, or negligent acts that is performed upon Personal Data or Company Data, whether or not by automatic means, including, without limitation, collection, recording, organization, storage, access, adaptation, alteration, retrieval, consultation, retention, use, disclosure, dissemination, exfiltration, taking, removing, copying, making available, alignment, combination, blocking, deletion, erasure, or destruction.

(v) "Data Security Incident" means: (A) the loss or misuse (by any means) of Personal Data or Company Data; (B) the inadvertent, unauthorized and/or unlawful Processing, corruption, modification, transfer, sale or rental of Personal Data or Company Data; (C) any other act, omission or circumstance that compromises or may reasonably compromise the security, confidentiality, or integrity of Personal Data or Company Data, including but not limited to incidents where Personal Data or Company Data has been damaged, lost, corrupted, destroyed, or accessed, acquired, modified, used, or disclosed by any unauthorized person, by any person in an unauthorized manner, or for an unauthorized purpose; (D) any act, omission or circumstance that compromises or may reasonably compromise the cybersecurity of the products and services provided to CUSTOMER by VENDOR or the physical, technical, administrative, or organizational safeguards protecting VENDOR's systems or, if VENDOR knows or reasonably believes, CUSTOMER's systems storing or hosting Personal Data or Company Data, or (F) VENDOR receives any complaint, notice, or communication which relates directly or indirectly to (x) VENDOR's Processing of Personal Data or Company Data or VENDOR's compliance with Technical and Organizational Measures or applicable law in connection with Personal Data or Company Data or (y) the cybersecurity of products and services provided to CUSTOMER by VENDOR.

(vi) "Technical and Organizational Measures" means security measures, consistent with the type of Personal Data or Company Data being Processed and the services being provided by VENDOR, to protect Personal Data or Company Data, which measures shall implement industry accepted protections which may include physical, electronic and procedural safeguards to protect the Personal Data or Company Data supplied to VENDOR against any Data Security Incident, and any security requirements, obligations, specifications or event reporting procedures set forth in this Rider or in any Schedule to this Rider. As part of such security measures, VENDOR shall provide a reasonably secure environment for all Personal Data and Company Data and any hardware and software (including servers, network, and data components) to be provided or used by VENDOR as part of its performance under the Agreement.

(vii) "Losses" shall mean all losses, liabilities, damages, and claims and all related or resulting costs and expenses (including, without limitation, reasonable attorneys' fees and disbursements and costs of investigation, litigation, settlement, judgment, interest and penalties).

(viii) "Agreement" shall mean the effective date of the corresponding MSA, MMA, CSA, and/or any associated purchase orders, statements of work, notices to proceed and related documents issued in connection therewith.

(c) Personal Data and Company Data shall at all times remain the sole property of CUSTOMER, and nothing in this Rider or the Agreement will be interpreted or construed as granting VENDOR any license or other right under any patent, copyright, trademark, trade secret, or other

proprietary right to Personal Data or Company Data. VENDOR shall not create or maintain data which are derivative of Personal Data or Company Data except for the purpose of performing its obligations under the Agreement and this Rider and as authorized by CUSTOMER.

(d) Regarding the Processing of Personal Data and Company Data, the parties agree that:

(i) VENDOR shall Process Personal Data and Company Data only on behalf of CUSTOMER, on the instruction of CUSTOMER and in accordance with the Agreement, this Rider and privacy and security laws applicable to VENDOR's services or VENDOR's possession or Processing of Personal Data and Company Data. CUSTOMER hereby instructs VENDOR, and VENDOR hereby agrees, to Process Personal Data and Company Data only as necessary to perform VENDOR's obligations under the Agreement and as further described below and for no other purpose. For the avoidance of doubt and without limitation, (i) VENDOR shall not Process Personal Data or Company Data for any purpose other than providing the services specified in the Agreement nor for any purpose outside the scope of the Agreement; and (ii) VENDOR is prohibited from (w) selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Data and Company Data to any business or third party (x) retaining, using, or disclosing Personal Data or Company Data for any purpose other than for the purposes specified in the Agreement and this Rider, (y) retaining, using or disclosing Personal Data and Company Data outside of the direct business relationship between CUSTOMER and VENDOR pursuant to the Agreement, and (z) combining Personal Data or Company Data received from CUSTOMER with Personal Data or Company Data received from or on behalf of another person or persons or collected by VENDOR.

(ii) The parties agree that:

The Processing activities that will be carried out by VENDOR are: VENDOR services, including without limitation support services. VENDOR may also use CUSTOMER's employee contact information to communicate and provide the services.

- The categories of Personal Data or Company Data that will be Processed by VENDOR are: Internal Emails or Memo, Business Plans, Training Materials, Organizational Charts, Generic Maps/Diagrams, Incident Response Plans, Operating Procedures, Transaction Data, Service Level Agreements (SLA), IP Address, Password Databases, Security Configuration (BES Cyber Systems, and ESP or PSP Equipment), and CIP Assets (IP Addresses and Hostnames) for both CIP and Non CIP environments.

- The categories of Personal Data subjects whose information will be processed by VENDOR are: employee contact information.

- The instructions for the Processing of Personal Data or Company Data are : VENDOR may Process Personal or Company Data (a) in order to provide the services including without limitation support services; and (b) as directed by CUSTOMER personnel.

(iii) The duration of the Processing shall be: for approximately three years with an option of a two-year extension.

(i) VENDOR shall immediately inform the CUSTOMER if in VENDOR's

(i) opinion a Processing instruction given by CUSTOMER may infringe the privacy and security laws VENDOR shall immediately inform the CUSTOMER if in VENDOR's opinion a Processing instruction given by CUSTOMER may infringe the privacy and security laws applicable to VENDOR's services or VENDOR's possession or Processing of Personal Data or Company Data.

(ii) In the event that the activities to be carried out by VENDOR under the Agreement do not require access to Personal Data, VENDOR, its employees and representatives shall be prohibited from accessing and Processing Personal Data. If they gain access to Personal Data, VENDOR shall immediately inform CUSTOMER. Notwithstanding the foregoing, any Processing of Personal Data by VENDOR shall be subject to the terms and conditions set forth in this Rider.

(e) As a condition to starting work, VENDOR's employees and other persons authorized, pursuant to the terms of this Rider, to Process Personal Data or Company Data shall acknowledge in writing their agreement to [(i) comply with the terms of CUSTOMER's Acceptable Use Requirements set forth in Schedule C hereto, as such Acceptable Use Requirements may be modified or supplemented from time-to-time upon notice from the CUSTOMER, (ii) maintain the confidentiality of Personal Data and Company Data, and (iii) comply with any applicable Technical and Organizational Measures. In addition, VENDOR's employees and other authorized persons that access CUSTOMER's premises shall abide by CUSTOMER's physical security policies, rules and procedures.

(f) At any and all times during which VENDOR is Processing Personal Data or Company Data, VENDOR shall:

(i) Comply with all applicable privacy and security laws to which it is subject, or that are applicable to VENDOR's services or VENDOR's possession or Processing of Personal Data and\or Company Data, and not, by act or omission, place CUSTOMER or its affiliates in violation of any privacy or security law known by VENDOR to be applicable to them;

(ii) With regards to the Processing of Personal Data, maintain a record of Personal Data Processing activities carried out on behalf of CUSTOMER, which shall include at least:

(A) The name and contact details of the VENDOR, any subcontractor, where applicable and as previously authorized by CUSTOMER, the CUSTOMER on whose behalf the VENDOR is Processing Personal Data, their respective representatives and, where applicable, the data protection officer;

(B) The categories of Processing activities carried out on behalf of CUSTOMER;

(C) Where applicable, international transfers of Personal Data to a third country or international organization, identifying the third country or international organization, and identification of appropriate safeguards;

(D) A general description of the appropriate Technical and Organizational Measures that VENDOR is implementing relating to:

- The ability to ensure the continued confidentiality, integrity, availability and resilience of Personal Data Processing systems and services;

- The ability to quickly restore availability and access to Personal Data in the event of a physical or technical incident; and

- A process of regular verification, evaluation and assessment of the effectiveness of Technical and Organizational Measures to ensure the security of the Personal Data Processing;

- Pseudonymization and encryption of Personal Data;

(iii) Have in place appropriate and reasonable Technical and Organizational Measures to protect the security of Personal Data and Company Data and prevent a Data Security Incident, including, without limitation, a Data Security Incident resulting from or arising out of VENDOR's internal use, Processing or other transmission of Personal Data and Company Data, whether between or among VENDOR's subsidiaries and affiliates or any other person or entity acting on behalf of VENDOR. Taking into account the state-of-the-art, the costs of implementation, and the nature, scope, context and purposes of the Processing as well as the risks of varying likelihood and severity for, among other, the rights and freedoms of the data subjects, VENDOR shall implement Technical and Organizational Measures to ensure a level of security appropriate to the risk. Without limiting the generality of the foregoing, the VENDOR will implement measures to:

(A) Ensure the continued confidentiality, integrity, availability and resilience of Processing systems and services;

(B) Quickly restore availability and access to Personal Data and Company Data in the event of a physical or technical incident;

(C) Verify and evaluate, on a regular basis, the effectiveness of the Technical and Organizational Measures implemented;

(D) Pseudonymize and encrypt Personal Data, where applicable; and

(E) Safely secure or encrypt all Personal Data and Company Data, during storage or transmission;

(iv) Except as may be necessary in connection with providing services to CUSTOMER (and provided that immediately upon the need for such Personal Data and Company Data ceasing, such Personal Data or Company Data is immediately destroyed or erased), not use or maintain any Personal Data or Company Data on a laptop, hard drive, USB key, flash drive, removable memory card, smartphone, or other portable device or unit; and ensure that any such portable device or unit is encrypted.

(v) Notify CUSTOMER at asoc@avangrid.com or (855)548-7276no later than one (1) day from the date of obtaining actual knowledge of any Data Security Incident, or from the date the VENDOR

reasonable believes that a Data Security Incident has taken place, whatever is earlier, and at VENDOR's cost and expense, assist and cooperate with CUSTOMER concerning any disclosures to affected parties and other remedial measures as requested by CUSTOMER or required under applicable law. If the Data Security Incident involves Personal Data, the following information shall be provided as a minimum:

(A) Description of the nature of the Data Security Incident, including, where possible, the categories and approximate number of data subjects affected, and the categories and approximate number of Personal Data records affected;

(B) Contact details of the data protection officer of the VENDOR, where applicable, or other contact person for further information;

(C) Description of the possible consequences of the Data Security Incident or violations; and

(D) Description of the measures taken or proposed to remedy the Data Security Incident, including, where appropriate, the measures taken to mitigate possible negative effects;

(vi) VENDOR designates the following contacts for the purposes of communications related to a Data Security Incident: [redacted]

(vii) Assist and cooperate with CUSTOMER to enable CUSTOMER to comply with its obligations under any applicable privacy or security law, including but not limited to maintaining Personal Data and Company Data secured, responding to Data Security Incidents, and, where applicable, ensuring the rights of data subjects and carrying out Personal Data impact assessments;

(viii) Inform the CUSTOMER, if, where applicable, data subjects exercise their rights of access, rectification, erasure or objection, restriction of processing, data portability and not to be the subject to automated decisions by the VENDOR. The communication must be made immediately and in no case later than one (1) business day following the receipt of the request by VENDOR. VENDOR shall assist CUSTOMER, taking into account the nature of the Personal Data Processing, through appropriate Technical and Organizational Measures, and with any information that may be relevant to the resolution of the request;

(ix) Not use independent contractors or provide Personal Data or Company Data to independent contractors or other personnel that are not full-time employees of VENDOR without CUSTOMER's prior written approval;

(x) Not disclose Personal Data or Company Data to any third party (including, without limitation, VENDOR's subsidiaries and affiliates and any person or entity acting on behalf of VENDOR) unless with respect to each such disclosure: (A) the disclosure is necessary in order to carry out VENDOR's obligations under the Agreement and this Rider; (B) VENDOR executes a written agreement with such third party whereby such third party expressly assumes the same obligations set forth in this Rider; (C) VENDOR has received CUSTOMER's prior written consent; (D) the Processing is carried out in accordance with the instructions of CUSTOMER, and (D) VENDOR shall remain responsible for any breach of the obligations set forth in this Rider to the same extent as if VENDOR caused such breach;

(xi) Not permit any officer, director, employee, agent, other representative, subsidiary, affiliate, independent contractor, or any other person or entity acting on behalf of VENDOR to Process Personal Data or Company Data unless such Processing is in compliance with this Rider and is necessary to carry out VENDOR's obligations under the Agreement and this Rider. Personal Data and Company Data shall only be accessed by persons who need access to carry out VENDOR's obligations under the Agreement and this Rider and in accordance with the instructions of CUSTOMER; VENDOR shall provide appropriate privacy and security training to its employees and those persons authorized to Process Personal Data or Company Data.

(xii) Establish policies and procedures to provide all reasonable and prompt assistance to CUSTOMER in responding to any and all requests, complaints, or other communications received from any individual who is or may be the subject of any Personal Data Processed by VENDOR to the extent such request, complaint or other communication relates to VENDOR's Processing of such Personal Data;

(xiii) Establish policies and procedures to provide all reasonable and prompt assistance to CUSTOMER in responding to any and all requests, complaints, or other communications received from any individual, government, government agency, regulatory authority, or other entity that is or may have an interest in the Personal Data or Company Data, exfiltration of Personal Data or Company Data, disclosure of Personal Data or Company Data, or misuse of Personal Data or Company Data to the extent such request, complaint or other communication relates to VENDOR's Processing of such Personal Data or Company Data;

(xiv) Not transfer any Personal Data or Company Data across a country border, unless directed to do so in writing by CUSTOMER, and VENDOR agrees that CUSTOMER is solely responsible for determining that any transfer of Personal Data or Company Data across a country border complies with the applicable laws and this Rider;

(xv) Keep Personal Data and Company Data in strict confidence;

(g) At the time of the execution of this Rider, and at any time, upon CUSTOMER's request, VENDOR shall provide evidence that it has established and maintains Technical and Organizational Measures governing the Processing of Personal Data and Company Data appropriate to the Processing and to the nature of the Personal Data and Company Data;

(h) To the extent VENDOR maintains Personal Data and Company Data at its location, CUSTOMER shall have the right to conduct onsite inspections and/or audits (with no advance notice to VENDOR) of VENDOR's information security protocols, and VENDOR agrees to cooperate with CUSTOMER regarding such inspections or audits; provided, any such inspections or audits shall be conducted during normal business hours and in a manner so as to minimize any disruptions to VENDOR's operations. VENDOR will promptly correct any deficiencies in the Technical and Organizational Measures identified by CUSTOMER to VENDOR;

(i) VENDOR shall keep and make accessible to CUSTOMER, at any time, upon CUSTOMER's request, documentation that evidences compliance with the terms of this Rider. CUSTOMER may conduct audits and inspections, either directly or through a third party, and VENDOR agrees to cooperate with CUSTOMER regarding such audits;

(j) VENDOR shall cease Processing Personal Data and Company Data and return, or securely delete or destroy, or cause or arrange for the return, or secure deletion or destruction of, all Personal Data and Company Data subject to the Agreement and this Rider, including all originals and copies of such Personal Data and Company Data in any medium and any materials derived from or incorporating such Personal Data and Company Data, upon the expiration or earlier termination of the Agreement, or when there is no longer any legitimate business need (as determined by CUSTOMER) to retain such Personal Data and Company Data, or otherwise on the instruction of CUSTOMER, but in no event later than ten (10) days from the date of such expiration, earlier termination, expiration of the legitimate business need, or instruction. If applicable law prevents or precludes the return or destruction of any Personal Data or Company Data, VENDOR shall notify CUSTOMER of such reason for not returning or destroying such Personal Data and Company Data and shall not Process such Personal Data and Company Data thereafter without CUSTOMER's express prior written consent. VENDOR's obligations under this Rider to protect the security of Personal Data and Company Data shall survive termination of the Agreement.

(k) To the extent that VENDOR is afforded regular access in any way to "Cardholder Data" as defined below and for so long as it has such access, the following requirements shall apply with respect to the Cardholder Data; provided, that the parties do anticipate that VENDOR will have access to any Cardholder Data:

(i) VENDOR represents that it is presently in compliance and will remain in compliance with the Payment Card Industry Data Security Standard ("PCI Standard"), and all updates to PCI Standard, developed and published jointly by American Express, Discover, MasterCard and Visa ("Payment Card Brands") for protecting individual credit and debit card account numbers ("Cardholder Data").

(ii) VENDOR acknowledges that Cardholder Data is owned exclusively by CUSTOMER, credit card issuers, the relevant Payment Card Brand, and entities licensed to process credit and debit card transactions on behalf of CUSTOMER, and further acknowledges that such Cardholder Data may be used solely to assist the foregoing parties in completing a transaction, supporting a loyalty program, providing fraud control services, or for other uses specifically required by law, the operating regulations of the Payment Card Brands, or this Agreement.

(iii) To the extent Cardholder Data is regularly maintained on the premises or property of VENDOR, VENDOR shall maintain a business continuity plan addressing the possibility of a potential disruption of service, disaster, failure or interruption of its ordinary business process, which business continuity plan provides for appropriate back-up facilities to ensure VENDOR can continue to fulfill its obligations under the Agreement.

(iv) VENDOR agrees that, in the event of a Data Security Incident arising out of or relating to VENDOR's premises or equipment contained thereon, VENDOR shall afford full cooperation and access to VENDOR's premises, books, logs and records by a designee of the Payment Card Brands to the extent necessary to perform a thorough security review and to validate VENDOR's compliance with the PCI Standards; provided, that such access that be provided during regular business hours and in such a manner so as to minimize the disruption of VENDOR's operations.

(l) To the extent that the VENDOR processes personal information of California residents as such terms are defined in the California Consumer Privacy Act of 2018, as amended (Cal. Civ. Code §§ 1798.100 to 1798.199.95), the terms and conditions set forth in Schedule D of this Rider shall apply.

(m) To the extent that VENDOR processes personal data of Connecticut consumers as such terms are defined in An Act Concerning Personal Data Privacy and Online Monitoring (Public Act No. 22-15), the terms and conditions of Schedule E shall apply.

(n) VENDOR represents that the security measures it takes in performance of its obligations under the Agreement and this Rider are, and will at all times remain, at the highest of the following: (a) Privacy & IT Security Best Practices (including, but not limited to, National Institute of Standards and Technology ("NIST") SP 800-53, International Organization for Standardization ("ISO") 27001/27002, Control Objectives for ("COBIT") framework, Center for Internet Security ("CIS") Security Benchmarks, and Top 20 Critical Controls) and (b) any security requirements, obligations, specifications, or event reporting procedures set forth in Schedule A.

(o) In addition to any other insurance required to be provided by VENDOR hereunder, VENDOR shall also provide the Cyber-Insurance coverage meeting the requirements specified in Schedule B, attached hereto and made part hereof. VENDOR shall also comply with the terms and conditions in Schedule B as they relate to any insurance required to be provided by VENDOR pursuant to this Agreement.

(p) Notwithstanding anything in the Agreement or this Rider to the contrary, VENDOR shall indemnify, defend and hold CUSTOMER, its affiliates, and their respective employees, officers, representatives and contractors, harmless from and against all Losses caused by, resulting from, or attributable to VENDOR's breach or violation of applicable laws, regulations or any of the terms and conditions of this Rider. VENDOR's obligation to indemnify, defend, and hold harmless shall survive termination or expiration of the Agreement and this Rider.

(q) Failure by VENDOR to comply with any requirement of this Rider shall constitute a material breach of the Agreement and a VENDOR default thereunder. CUSTOMER shall be allowed to terminate the Agreement, and CUSTOMER shall have all rights and remedies provided by law or equity under the Agreement and this Rider.

Schedule A

General Security Requirements

(a) The following definitions are relevant to this General Security Requirements Schedule:

(i) "Cyber-infrastructure" means electronic information and communication systems and services, as well as the information contained therein. These systems, both those housed within facilities as well as those that are cloud-based, be they proprietary or third-party, in any manner, are comprised of hardware and software for processing (creating, accessing, modifying and destroying), storing (on magnetic, electronic or other formats) and sending (shared use and distribution) information, or any combination of said elements that include any type of electronic device such as, without limitation, standard computers (desktop/laptop) with internet connections, digital storage methods used on computers

(e.g. hard drives), mobiles, smartphones, personal digital assistants, data storage media, digital and video cameras (including CCTV), GPS systems, etc.

(ii) "Protected Information" means Personal Data and Company Data as defined in the Rider.

(iii) Capitalized terms not otherwise defined in this Schedule shall have the meaning set forth in the Rider.

(b) VENDOR must, always, know the level of information protection that should be afforded to the Protected Information as well as the corresponding standards and applicable laws and regulations, and it shall adopt the Technical and Organizational Measures adequate thereto. VENDOR shall, at least, maintain Technical and Organizational Measures consistent with the type of Protected Information being processed and the services being provided by VENDOR, to secure Protected Information, which measures shall implement industry accepted protections which include physical, electronic and procedural safeguards to protect the Protected Information supplied to VENDOR against any Data Security Incident or other security incident, and any security requirements, obligations, specifications or event reporting procedures set forth in the Agreement, the Rider or this Schedule. As part of such security measures, VENDOR shall provide a secure environment for all Protected Information and any hardware and software (including servers, network, and data components) to be provided or used by VENDOR as part of its performance under the Agreement on which Protected Information is contained.

(c) When the scope of the Agreement implies the use or connection of VENDOR's Cyber-infrastructure to that of CUSTOMER, the VENDOR shall have reasonable Technical and Organizational Measures for its protection and for the prevention of any Data Security Incident.

(i) The connection between the CUSTOMER's and the VENDOR's network is not permitted, unless expressly agreed to in writing, in which case it must be done by establishing encrypted and authenticated virtual private networks, and the number of interconnection points between the two networks must be the minimum that is compatible with the required level of availability. The connection to the VENDOR's network shall be removed as soon as there is no need for it.

(ii) Direct user connections from the VENDOR to CUSTOMER's network are not permitted, unless authorized in writing by CUSTOMER and only for a limited period of time.

(iii) If the Agreement is fully or partially performed at the VENDOR's premises or property, the VENDOR must establish mechanisms and procedures for physical access to said premises or property to prevent unauthorised persons from accessing Cyber-infrastructure or Protected Information.

(d) VENDOR shall establish mechanisms and procedures for identifying, authenticating and controlling logical access necessary to prevent unauthorised persons from accessing its Cyber-infrastructure elements and CUSTOMER's Protected Information, and, in particular:

(i) VENDOR will have procedures based on the principle of least privilege when granting, assigning and withdrawing authorized access and permissions to its personnel or the personnel of its subcontractors, where applicable, including privileged users or administration taking into account the need for the use, the confidentiality of the Protected Information and the resources for the performance of their tasks;

(ii) VENDOR will maintain an updated inventory of the access granted and will withdraw access from personnel who cease working in connection with the Agreement within a period of less than twenty-four (24) hours. Credentials must always be encrypted when stored and transmitted; and

(iii) VENDOR shall have policies and procedures that ensure the strength of the passwords and that they are updated regularly. Passwords shall be changed during the installation processes of new hardware or software. VENDOR's default passwords shall be changed.

(e) VENDOR shall implement Technical and Organisational Measures necessary to ensure operational continuity under applicable service level agreements (including but not limited to contingency plans, backup and recovery procedures). In particular:

(i) VENDOR shall make backup copies of the Protected Information as frequently as is required for the services being provided by VENDOR and according to the nature of the data, establishing the appropriate procedures and mechanisms to ensure that the data can be retrieved, that only authorised VENDOR personnel can access it and that they are transferred and stored in such a way as to prevent access or manipulation by unauthorised persons; and

(ii) The same security measures shall apply to backups as to the original Protected Information.

(f) In the event that CUSTOMER has expressly authorized VENDOR to use its own IT equipment for accessing CUSTOMER's Cyber-infrastructure, the VENDOR shall guarantee and undertake that there are adequate security measures to protect the stationary or portable IT equipment and mobile devices used to access such Cyber-infrastructure or for storing, processing or transmitting the Protected Information, including but not limited to:

(i) Automatic locking if the device is left unattended for a certain period of time. User authentication will be required for unlocking.

(ii) Protection against malicious software and known vulnerabilities.

(iii) Updating the operating system as often as the vendor requires.

The VENDOR shall maintain an action procedure should the equipment or device be lost or stolen, ensuring, to the maximum extent possible that the event be communicated promptly, Protected Information be deleted safely in accordance with recognised standards, and access to CUSTOMER's systems or systems containing CUSTOMER's Protected Information be suspended.

Before equipment is reused or replaced, the VENDOR must protect, or if applicable remove, all the Protected Information stored on it, ensuring that unauthorised personnel or third parties cannot access or recover it.

(g) The VENDOR shall establish adequate procedures to guarantee protection against loss or unauthorised processing of files, computer media and paper documents containing Protected Information and guarantee that they are destroyed when the reasons for their creation no longer apply. Extracting data from a file and downloading it to a server or delivering it electronically is considered equivalent to computer media for the purposes of complying with these measures.

AVANGRID may request information concerning any Processing of Protected Information by the VENDOR.

(h) The VENDOR shall include security measures appropriate to the nature of the Protected Information Processed in developing, maintaining and testing the equipment that will be used to perform the services being provided by VENDOR. The VENDOR will adopt secure code development standards and ensure that no real data is used in test environments. If necessary, CUSTOMER's express written authorisation will be required, and the same security measures required for the work environment will be applied to these test environments.

(i) When the scope of the Agreement includes the supply of equipment and/or materials, the VENDOR shall prove that best security practices and standards have been applied for the design, fabrication, maintenance, and, where applicable, installation of the supplied equipment and/or materials, including its components.

For any such equipment and/or materials with information processing capacity or network connectivity options:

(i) The VENDOR shall provide evidence or certificates that guarantee design security, firmware/software updates and malware protection.

(ii) The VENDOR shall conduct periodic analyses of vulnerabilities and inform CUSTOMER about any necessary updates, especially those that affect security.

(iii) All internet connected devices shall be protected with adequately complex passwords that can be changed by CUSTOMER.

(iv) The configuration of devices, equipment and materials shall be adjustable exclusively according to AVANGRID's needs, and any unnecessary functionality deactivated. Should the VENDOR conduct any configuration, documentation to that effect shall be provided.

(j) VENDOR should fully implement the mitigation actions available on the APTs Targeting IT Service Provider CUSTOMERS site page to protect against this malicious activity. VENDOR should implement the following specific actions:

(i) Apply the principle of least privilege to their environment, which means customer data sets are separated logically, and access to client networks is not shared;

(ii) Implement robust network and host-based monitoring solutions that looks for known malicious activity and anomalous behaviour on the infrastructure and systems providing client services;

(iii) Ensure that log information is aggregated and correlated to enable maximum detection capabilities, with a focus on monitoring for account misuse; and

(iv) Work with CUSTOMER to ensure hosted infrastructure is monitored and maintained, either by the service provider or the client.

Schedule B

Cyber-Insurance Requirements

(a) VENDOR shall during the term of the Agreement have and maintain the following insurance coverage:

(i) Cyber Errors and Omissions Policy providing coverage, on a per occurrence basis, for acts, errors, omissions, and negligence of employees and contractors giving rise to potential liability, financial and other losses relating to data security and privacy, including cost of defense and settlement, in an amount of at least $10 million dollars, which policy shall include coverage for all costs or risks associated with:

1) violations of data privacy or data security laws and regulations; and

2) cyber risks, including denial-of-service attacks, risks associated with malware and malicious code, whether designed to interrupt a network or provide access to private or confidential information; and

3) other risks specific to the work performed by VENDOR as shall be identified by CUSTOMER.

(ii) Such coverage shall be furnished by an insurance company with an A.M. Best Financial Strength Rating of A- or better, and which is otherwise reasonably acceptable to CUSTOMER.

(b) VENDOR warrants that the scope of all coverage evidenced to the CUSTOMER pursuant to this Agreement shall be the sole responsibility of the VENDOR to maintain at committed to levels required by this document and VENDOR, in any event of a loss, will take full responsibility for the payment of any policy deductible, self-insured retention, premium or retrospective premium obligation necessary to maintain coverage, and shall include coverage for any indemnification and hold harmless agreements made by the VENDOR pursuant to the Data Security Rider. VENDOR's failure to pay the applicable deductible, self-insured retention, or retrospective premium shall constitute a material breach of this Agreement, with damages equal to at least the amount of insurance lost or not provided due to such breach.

(c) All insurance coverage(s) provided by VENDOR pursuant to this Agreement shall be primary and non-contributing with respect to any other insurance or self-insurance which may be maintained by the CUSTOMER.

Schedule C

Acceptable Use Requirements

The intent of this Schedule is to document requirements as they pertain to the Acceptable Use of the Electronic Devices and Cyber-infrastructure of Avangrid, Inc. and any of its subsidiaries (hereinafter "Avangrid") by contractors, consultants or other third parties.

Employees and other persons acting on behalf of Avangrid vendors shall be required to read, acknowledge their understanding of, and commit to comply with these Avangrid Acceptable Use Requirements.

Definitions

- A **User** is defined as any contractor, consultant or other third parties, including any employee of an Avangrid vendor, with access to or using Avangrid Electronic Devices or Cyber-infrastructure.

- **Cyber-infrastructure** Includes electronic information and communications systems and services, and the information contained in these systems and services. Those systems and services are composed of all hardware and software that process (creation, access, modification, and destruction), store (paper, magnetic, electronic, and all other media types), and communicate (sharing and distribution) information, or any combination of these elements.

- **Electronic Devices** include standard computer (workstation desktop/ laptop) with network connections, digital storage media used in standard computers (e.g. hard drives), telephone and voicemail systems, mobile phones, smartphones, tablets, Personal Digital Assistants (PDA), End Point Storage Devices (EPSD), digital and video cameras (including CCTV), mobile navigation systems, printers, photocopiers and scanners, fax machines, and all other similar of associated devices, etc.

    - **Avangrid Electronic Devices** are Electronic Devices owned and managed by Avangrid.

    - **Personally Owned Devices (POD)** are Electronic Devices (e.g. smart phones, tablets, laptops) privately owned and managed by Users.

    - **End Point Storage Devices (EPSD)** applies to the storage of data on devices that can be connected either by a USB drive, data cable or by wireless connection direct to any computing equipment within Avangrid, e.g. USB sticks, drives, thumb nails, pen drives, flash drives, memory cards, etc.

1. Requirements and Practices

1.1 Electronic Devices

Avangrid Electronic Devices and resources are property of Avangrid and may be provided to Users for the pursuit of their professional activity.

1.1.1 The determining authority and responsibility for issuance of an Electronic Device shall rest with the Avangrid Business Area Leader (BAL) or department hiring manager.

1.1.2 Avangrid Electronic Devices shall be provided to Users configured with the required security hardware and software protections.

a. Compromising or interfering with the Electronic Devices' operating system, hardware, software or protection mechanisms is prohibited.

1.1.3 Users shall be responsible for the appropriate use of authorized Electronic Devices in accordance with their duties and responsibilities, including, but not limited to:

a. Protecting Electronic Devices from misuse.

b. Logging off or protecting Electronic Devices with a screen and/or keyboard locking mechanism, when unattended and when not in use.

i. Desktop and laptop computers shall be switched off or hibernating when unattended for a period more than one hour and always at the end of the workday.

ii. Desktop and laptop computer screens shall be locked by Users always when unattended.

c. Taking the following preventative measures to ensure that any Electronic Devices used to connect to Avangrid's Cyber-infrastructure are physically secured by:

i. **Protecting Avangrid assets from unauthorized access and use by others,**

ii. **Leaving Electronic Devices in secured locations (e.g. locked cabinet or drawer, locked rooms in locked buildings as applicable),**

iii. **Not leaving Electronic Devices in plain view in unattended vehicles,**

iv. **Not leaving Electronic Devices in vehicles overnight,**

v. **Carrying laptops as hand luggage when traveling,**

vi. **Positioning Electronic Devices so that they (and the information displayed) are not visible from outside a ground floor window, and**

vii. **Positioning the display screen of Electronic Devices such that it cannot be viewed by others in public places (e.g. train, aircraft, restaurants, etc.).**

1.1.4 Users shall follow Avangrid procedures for immediately reporting lost, compromised, or stolen Electronic Devices.

a. The User shall notify the Service (Help) Desk and their Avangrid contact.

1.1.5 User shall follow Avangrid procedures for the return of Avangrid owned Electronic Devices when the use of those devices is deemed no longer necessary.

a. Users shall return all Avangrid Electronic Devices to their Avangrid contact immediately upon separation/ termination, which shall be responsible for collecting all Avangrid

Electronic Devices.

1.1.6 The use of hot desks/ shared network access equipment shall be reserved for Users who do not regularly require the use of a portable Electronic Device (e.g. laptop) for their professional activities.

a. Users of hot desks/shared network access shall have a current network login.

1.2 Connection to Avangrid Cyber-infrastructure

1.2.1 All Electronic Devices which connect to the Avangrid Cyber-infrastructure network shall be Avangrid approved assets which have been configured in accordance with Avangrid standard configurations.

a. Non-Avangrid approved Electronic Devices shall not connect directly to the Avangrid Cyber-infrastructure (e.g. through Ethernet connection).

b. Wireless connections from an Avangrid office shall only be accomplished through Avangrid Electronic Devices and the Avangrid supported wireless infrastructure.

c. Guest wireless network accounts shall only be supplied on ‘as-need-be-basis’ following Avangrid approval processes.

d. Remote desk connections shall only be supplied on ‘as-need-be-basis’ following Avangrid approval processes.

1.3 Use of Mobile Devices (for Remote Access)

1.3.1 The determining authority and responsibility for issuance of a mobile electronic device to perform Avangrid professional activities; access the Avangrid Cyber-infrastructure or store/transmit Avangrid information/data remotely shall rest with the Avangrid Business Area Leader (BAL) or department hiring manager.

a. Users shall remotely access Avangrid’s Cyber-infrastructure utilizing only authorized hardware, software and access control standards (e.g. Avangrid approved VPN technology for Avangrid Electronic Devices or Citrix client).

b. At no time shall a remote User initiate two simultaneous connections to different networks (e.g., no split tunneling and no multi-homed connection).

c. Avangrid issued SIM cards shall not be swapped or used in non-Avangrid issued Electronic Devices.

d. Configuring a non-Avangrid issued Electronic Device for connection to the Avangrid corporate email system is strictly prohibited.

e. Users should be aware that Avangrid may monitor emails sent from and to non-Avangrid issued devices.

1.4 Personally Owned Devices

1.4.1 The use of Personally Owned Devices for access to and/or handling of Avangrid information/data and Avangrid Cyber-infrastructure is prohibited.

1.5 Treatment of Software and Applications

1.5.1 The acquisition and installation of software on Avangrid Electronic Devices shall be made using approved methods.

a. All access to company software and/or applications shall be subject to formal request and approval processes.

1.5.2 Users shall be prohibited from introducing or installing any unauthorized software, content or material.

1.5.3 The installation of any type of network access program peer (P2P) or similar (e.g., BitTorrent, Emule), as well as any other application for file sharing that could saturate Internet bandwidth, prevent access to other Users or slow down connections to technology and information resources is prohibited.

1.5.4 Intellectual property, licensing and regulatory requirements shall be observed always. Downloading, obtaining, copying or redistributing materials protected by copyright, trademark, trade secret or other intellectual property rights (including software, music, video, images) is prohibited, even where such material is to be used for the pursuit of the professional activity.

a. Where materials protected by copyright, trademark, trade secret or other intellectual property rights are required for the pursuit of an Avangrid professional activity the appropriate license/permission shall be obtained prior to use.

1.6 Treatment of Information/Data

1.6.1 Information/data assets obtained or created during the engagement with Avangrid are the property of Avangrid and shall be treated in accordance with the applicable Agreement and Data Security Rider.

1.6.2 The storage of Avangrid information/data on Personally Owned Devices or non-Avangrid controlled or authorized environments, including non-authorized Electronic Devices is prohibited. Users shall not store AVANGRID owned information/data on devices that are not issued by AVANGRID unless explicitly and contractually agreed by both parties.

1.6.3 Where access to Personal Data is part of a Users' professional role and responsibilities, access shall be treated in accordance with all applicable data protection and/or privacy law(s) and regulation(s) and under strict access and usage guidelines.

1.6.4 Corporate storage spaces and network resources shall be used for file storage and/or exchange of professional information.

1.6.5 Users shall store and share information/data in accordance with the terms and conditions with Avangrid and any applicable Data Security Rider.

1.6.6 Use of an End Point Storage Device (EPSD) (e.g., USB) shall be limited to those devices acquired through the Information Technology (IT) request process (e.g. ITSM/ServiceNow).

1.6.7 Printed information/data (hard copy) shall be:

a. Stored based on critically, e.g., hardcopy containing confidential and/or sensitive information/data shall be locked away when not required (or not in use).

b. Discarded, when no longer needed, based on criticality, e.g. confidential and/or sensitive hardcopy shall be shredded.

c. To be removed from printers, fax machines, copier rooms, and conference/ meeting rooms immediately.

1.7 User Access Credentials and Passwords

1.7.1 Requests for access shall be made following access provisioning procedures.

1.7.2 Applications and network resources access shall be activated\deactivated in accordance with Avangrid activation\ deactivation procedures.

1.7.3 Users requiring duly justified privileged access rights will be assigned a specific “Privileged User ID”

a. Privileged User IDs shall be reviewed and confirmed at least semi-annually.

b. Regular professional activities shall not be performed from a privileged ID.

1.7.4 Users shall use strong, complex passwords and securely maintain secret authentication information (e.g. passwords, cryptographic keys, smart cards that produce authorization codes), including:

a. Not sharing or disclosing their Avangrid credentials (log on IDs-user names and/or passwords) with others inside or outside the company.

b. Keeping secret authentication information confidential, ensuring that it is not divulged to any other parties, including senior management and technical support.

c. Not recording (e.g. on paper, software file or hand-held device) secret authentication information, unless this can be stored securely, and the method of storing has been approved (e.g. password vault) by Corporate Security.

d. Changing secret authentication information when there is any indication of a possible compromise.

e. Reporting any incidents or suspected compromises by following Avangrid incident reporting procedures.

1.8 Internet Use and Social Media

1.8.1 Avangrid may make available internet access to users depending on their role and responsibilities.

a. Internet access shall be provided as a tool for business purposes, shall be used with moderation and shall be proportional to the work being undertaken.

b. Access to restricted websites shall be enabled at the discretion of Avangrid and shall be provisioned following the security exception process.

c. Only Avangrid approved surfing software shall be used to access the Internet.

1.8.2 A moderate and proportional use of the internet shall be allowed for non-professional activities, although web surfing is expressly prohibited for:

a. Accessing or posting of any racist or sexual content or any material that is offensive or defamatory in nature.

b. Accessing games, downloading video, music (MP3 or another format), or downloading any other files not related to the Avangrid related responsibilities.

1.8.3 Limited and occasional use of Avangrid Electronic Devices and resources to engage in Social Networking and Blogging is acceptable, provided that:

a. It is done in a professional and responsible manner.

b. It does not violate the Code of Ethics or any relevant Avangrid policy, procedure or rule.

c. It is not detrimental to Avangrid's best interests.

d. It does not interfere with regular work duties.

e. There is no breach of the prohibitions identified in these requirements.

1.8.4 Avangrid reserves the right to determine which websites and social media platforms can be accessible through Avangrid Electronic Devices or Cyber –infrastructure.

1.9 E-mail Use

1.9.1 All information created, sent, or received via Avangrid's e-mail system(s), including all e-mail messages and electronic files shall be the property of Avangrid.

1.9.2 Avangrid reserves the right to monitor, inspect and access such emails and electronic files.

1.9.3 The forwarding of Avangrid owned information/data to a personal e-mail account is prohibited.

1.9.4 Removing or circumventing any of the security controls enforced on the company email system (e.g. SPAM filtering, automatic email disclaimers, etc.) is prohibited.

1.9.5 Users shall not permit others to use their e-mail accounts. Based on user established permissions; calendars and/or mailboxes may be shared.

1.9.6 Limited use of an Avangrid e-mail account for personal purposes shall be regarded as acceptable provided that:

a. Use does not interfere with the normal performance of professional duties.

b. Messaging does not violate applicable laws, regulations, the Code of Ethics, or Avangrid policies.

c. Use is moderate both in terms of frequency and amount of memory and resources consumed.

1.9.7 Avangrid e-mails or messages containing company information/ data shall not be forwarded to external parties except where there is a specific business 'need to know'.

1.9.8 Avangrid electronic messaging shall not be used for transmitting, retrieving or storing any messages, files or attachments which constitute:

a. Harassing or discriminatory messages which relate to gender, race, sexual orientation, religion, disability or other characteristics protected by applicable laws and regulations.

b. Defamatory messages which adversely affect the reputation of a person or company.

c. Messages that violate copyright, trademark, trade secret or other intellectual property rights.

d. Obscene materials or images of a sexual nature.

e. Files or documents of an indeterminate origin or that, for any reason, may include computer viruses or in any way breach the security systems of the company or the recipient of the file or document, or may damage their IT systems.

f. Any material or images that might reasonably be expected to cause personal offense to the recipient.

g. Messages in violation of applicable laws, regulations, the Code of Ethics, or Avangrid policies.

1.9.9 The retention period for e-mail messages shall be 18 months. Once the retention period has been reached, emails shall be automatically eliminated from the user's mailbox.

a. a.Users shall store messages and/or associated attachments in Avangrid provided network folders. Storage of messages and/or associated attachments on hard drives in .pst (personal mail folders) folders is prohibited.

1.9.10 Users shall report suspicious email messages (e.g., spam, phishing, etc.) the Service (Help) Desk

and/or using the reporting tool REPORTER, available in Outlook.

1.10 Incident reporting

1.10.1 Users shall immediately report any unusual activity, incident or suspected event following Avangrid incident reporting procedures (e.g., Service (Help) Desk, REPORTER, etc.)

1.11 Contract Termination

1.11.1 Avangrid Electronic Devices assigned to or in the possession of a User shall be returned to Avangrid on or before the contract termination date or whenever it is determined that the use of the Electronic Device is no longer necessary. This includes the return of facility access badges.

1.11.2 Access to Cyber-infrastructure shall be deactivated (revoked) on or before a User's termination date in accordance with Avangrid access management processes.

2. No Expectation of Privacy

All contents of the Avangrid Electronic Devices and Cyber-infrastructure are the property of the company. Therefore, Users should have no expectation of privacy whatsoever in any e-mail message, file, data, document, facsimile, telephone conversation, social media post, conversation, or any other kind or form of information or communication transmitted to, received, or printed from, or stored or recorded on Avangrid's Electronic Devices or Cyber-Infrastructure.

3. Monitoring

3.1 Avangrid reserves the right to use monitoring controls, including software, to ensure compliance with these Acceptable Use Requirements document, and to record and/or monitor one or more Users' Electronic Devices and resources, e-mails and/or internet activity in accordance with regulatory and legal requirements.

a. This includes the right to monitor, intercept, access, record, disclose, inspect, review, retrieve, print, recover or duplicate, directly or through third parties designated for such purpose, any information/data contained on and any uses of the Electronic Devices and Cyber-Infrastructure. Avangrid may store copies of such information/data for a period of time after they are created and may delete such copies from time to time without notice. Users consent to such monitoring by acknowledging these requirements and using the Electronic Devices and Cyber-Infrastructure.

b. Accordingly, Users should not harbor any expectation of privacy in respect to the use of Avangrid Electronic Devices or Cyber-Infrastructure and should not consider the data contained on them as private.

4.2 Monitoring may take place at any time and without the need to notify or inform the User in advance, taking into consideration legal or regulatory limitations, where applicable.

4. Non Compliance

Violation and non-conformance to this guidance by third party workers may result in appropriate actions, including contract termination.

Schedule D

CCPA Contract Clauses for Service Providers

1. Definitions. The following definitions and rules of interpretation apply in this Schedule:
    a. "Agreement" has the meaning set forth in the Rider.
    b. "CCPA" means the California Consumer Privacy Act of 2018, as amended, including by the California Privacy Rights Act of 2020 (2020 Cal. Legis. Serv. Proposition 24) (Cal. Civ. Code §§ 1798.100 to 1798.199.95), the CCPA Regulations (Cal. Code Regs. tit. 11, §§ 7000 to 7102), and any related regulations or guidance provided by the California Attorney General. Terms defined in the CCPA, including personal information and business purposes, carry the same meaning in this Schedule.
    c. "Contracted Business Purposes" means the services described in the Agreement or the Rider for which the service provider receives or accesses personal information.
    d. "CUSTOMER" has the meaning set forth in the Rider.
    e. "Rider" means the Privacy and Data Security Rider to which this Schedule is appended.
    f. "VENDOR" has the meaning set forth in the Rider.
2. Scope of Application

This Schedule applies only where, and to the extent that, VENDOR processes personal information that is subject to the CCPA on behalf of CUSTOMER in connection with the Agreement.

3. Service Provider's CCPA Obligations
    a. Personal information is disclosed by CUSTOMER to VENDOR only for the specific Contracted Business Purposes. VENDOR will only collect, use, retain, or disclose personal information for the Contracted Business Purposes for which CUSTOMER provides or permits personal information access and in accordance with CUSTOMER's instructions.
    b. VENDOR will not sell or share personal information.
    c. VENDOR will not use, retain or disclose personal information for VENDOR's own commercial purposes or in a way that does not comply with the CCPA. If a law requires the VENDOR to disclose personal information for a purpose unrelated to the Contracted Business Purpose, the VENDOR must first inform the CUSTOMER of the legal requirement and give the CUSTOMER an opportunity to object or challenge the requirement, unless the law prohibits such notice.
    d. VENDOR will not use, retain or disclose personal information outside of the direct business relationship between VENDOR and CUSTOMER.
    e. VENDOR will not combine personal information that it receives from, or on behalf of, CUSTOMER with personal information it receives from, or on behalf of, another person or persons, or collects from its own interactions with the consumer.
    f. VENDOR will limit personal information collection, use, retention, and disclosure to activities reasonably necessary and proportionate to achieve the Contracted Business Purposes.

g. VENDOR must promptly comply with any CUSTOMER request or instruction requiring the VENDOR to provide, amend, transfer, or delete the personal information, or to stop, mitigate, or remedy any unauthorized processing, including any unauthorized use, of personal information.
h. If the Contracted Business Purposes require the collection of personal information from individuals on the CUSTOMER's behalf, VENDOR will always provide a CCPA-compliant notice at collection that the CUSTOMER specifically pre-approves in writing. VENDOR will not modify or alter the notice in any way without the CUSTOMER's prior written consent.
i. If VENDOR determines that it can no longer meet its obligations under the CCPA, VENDOR must promptly notify CUSTOMER.

4. Assistance with Customer's CCPA Obligations
    1. VENDOR will reasonably cooperate and assist CUSTOMER with meeting the CUSTOMER's CCPA compliance obligations and responding to CCPA-related inquiries, including responding to verifiable consumer requests, taking into account the nature of VENDOR’s processing and the information available to VENDOR.
    2. VENDOR must notify CUSTOMER immediately if it receives any complaint, notice, or communication that directly or indirectly relates either party's compliance with the CCPA. Specifically, VENDOR must notify the CUSTOMER within 2 working days if it receives a verifiable consumer request under the CCPA.
5. Subcontracting
    a. If CUSTOMER authorizes VENDOR to engage subcontractors in accordance with the terms of the Agreement and the Rider, any subcontractor used must qualify as a service provider under the CCPA and VENDOR cannot make any disclosures to the subcontractor that the CCPA would treat as a sale or share.
    b. For each subcontractor used, VENDOR will:
        i. Promptly notify CUSTOMER of the engagement.
        ii. Engage the subcontractor pursuant to a written contract binding the subcontractor to observe all the requirements set forth in the Rider and this Schedule.
        iii. Provide CUSTOMER with the following information: the subcontractor's name, address, and contact information, the type of services to be provided by the subcontractor, and the personal information categories to be disclosed to the subcontractor.
    a. VENDOR remains fully liable to the CUSTOMER for the subcontractor's performance of its agreement obligations.
    b. Upon the CUSTOMER written request, VENDOR will audit a subcontractor's compliance with its personal information obligations and provide the CUSTOMER with the audit results.
6. CCPA Warranties and Certification

a. When collecting, using, retaining, disclosing or, in general, processing personal information, VENDOR will comply with all applicable requirements of the CCPA and provide the same level of privacy protection as required by the CCPA.
b. VENDOR certifies that it understands this Schedule's and the CCPA's restrictions and prohibitions on selling and sharing personal information and retaining, using, or disclosing personal information outside of the parties' direct business relationship, and it will comply with them.

APPENDIX A
Personal Information Processing Purposes and Details

Personal Information Categories: The Agreement involves the following types of personal information, as defined and classified in CCPA

Personal Information Category	**Examples**	**Processed under this Agreement**
A. Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.	YES/NO
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.	YES/NO
C. Protected classification characteristics under California or federal law.	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	YES/NO
D. Commercial information.	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	YES/NO
E. Biometric information.	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a	YES/NO

	template or other identifier or identifying information, such as fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	
F. Internet or other similar network activity.	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	YES/NO
G. Geolocation data.	Physical location or movements.	YES/NO
H. Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information.	YES/NO
I. Professional or employment-related information.	Current or past job history or performance evaluations.	YES/NO
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	YES/NO
K. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	YES/NO

Sensitive Personal Information Category	**Processed under the Agreement**
Social security, driver's license, state identification card, or passport number.	YES/NO
Log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.	YES/NO
Precise geolocation.	YES/NO
Racial or ethnic origin, religious or philosophical beliefs, or union membership.	YES/NO
Mail, email, or text messages contents not direct to CUSTOMER	YES/NO
Genetic data.	YES/NO
Unique identifying biometric information	YES/NO

Health information	YES/NO

Schedule E

Connecticut Privacy Act Clauses for Processors

1. Definitions. The following definitions and rules of interpretation apply in this Schedule:
    a. "Agreement" has the meaning set forth in the Rider.
    b. "Connecticut Privacy Act" means Connecticut Act Concerning Personal Data Privacy and Online Monitoring (Public Act No. 22-15). Terms defined in the Connecticut Privacy Act, including personal data and processing, carry the same meaning in this Schedule.
    c. "CUSTOMER" has the meaning set forth in the Rider.
    d. "Rider" means the Privacy and Data Security Rider to which this Schedule is appended.
    e. "VENDOR" has the meaning set forth in the Rider.
2. Scope of Application

This Schedule applies only where, and to the extent that, VENDOR processes personal data that is subject to the Connecticut Privacy Act on behalf of CUSTOMER in connection with the Agreement.

1. Personal data processing by VENDOR
    a. The instructions for the processing of the personal data, the nature and purpose of the processing of the personal data, the type of personal data subject to the processing and the duration for the processing are set forth in section (d)(ii) of the Rider.
    b. The rights and obligations of CUSTOMER and VENDOR with respect to the processing of personal data are set forth in the Rider and this Schedule.
2. Processor's Connecticut Privacy Act Obligations
    a. VENDOR will ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data.
    b. At CUSTOMER's direction, VENDOR shall delete or return all personal data to the CUSTOMER as requested at the end of the provision of the services, unless retention of data is required by law.
    c. Upon reasonable request from CUSTOMER, VENDOR shall make available to CUSTOMER all information in its possession necessary to demonstrate the processor's compliance with the obligations in sections 1 to 11, inclusive, of the Connecticut Privacy Act.
    d. VENDOR shall, allow, and cooperate with, reasonable assessments by CUSTOMER or CUSTOMER's designated assessor, or the VENDOR may, at its own cost, arrange for a qualified and independent assessor to conduct an assessment of the VENDOR's policies and technical and organizational measures in support of the obligations under sections 1 to 11, inclusive, of the Connecticut Privacy Act, using an appropriate and accepted control standard or framework and assessment procedure for such assessments, and provide a report of such assessment to CUSTOMER upon request.
3. Subcontracting

c. If CUSTOMER authorizes VENDOR to engage subcontractors in accordance with the terms of the Agreement and the Rider, any subcontractor engaged by VENDOR to process personal data shall be engaged pursuant to a written contract that requires the subcontractor to meet the obligations of VENDOR with respect to personal data.

2. Connecticut Privacy Act Warranties
   a. VENDOR will comply with all applicable requirements of the Connecticut Privacy Act when processing personal data.

CIP-013 Security Control Requirements

The Federal Energy Regulatory Commission ("FERC") has approved the North American Electric Reliability Corporation ("NERC") Reliability Standard CIP-013 (Cyber Security—Supply Chain Risk Management). This Reliability Standard will supplement the current NERC Critical Infrastructure Protection ("CIP") Standards to mitigate cybersecurity risks associated with the supply chain for grid-related cyber systems.

Definitions

The following definitions apply only to the terms and conditions in this Annex.

"***CEII***" means Critical Energy Infrastructure Information and/or Critical Electric Infrastructure Information.

"***Company***" means the organization that acquires or procures a product or service.

"***Company Information***" means for purposes of these terms and conditions, any and all information concerning Company and its business in any form, including, without limitation, the products and services provided under this Agreement that is disclosed to or otherwise learned by Contractor during the performance of this Agreement.

"***Contractor***" or ***"Vendor"*** or ***"Supplier"*** means the organization or individual that enters into an agreement with the Company for supplying a product or service.

"***Contractor Proprietary Information***" means any Contractor information that is considered highly confidential where disclosure outside of the Company may result in significant loss of Contractor's intellectual property, PII, etc. and may cause damage to the operational effectiveness or otherwise substantially disrupt significant business operations, with examples including but not limited to: source code, private encryption keys, or Company Information.

"***Disclosed***" means any circumstance when the security, integrity, or confidentiality of any Company Information has been compromised, including but not limited to incidents where Company Information has been damaged, lost, corrupted, destroyed, or accessed, acquired, modified, used, or disclosed by any unauthorized person, by any person in an unauthorized manner, or for any unauthorized purpose.

"***PII***" means Personally Identifiable Information.

"***Security Incident***" means any circumstance when (i) Contractor knows or reasonably believes that Company Information hosted or stored by the Contractor has been Disclosed; (ii) Contractor knows or reasonably believes that an act or omission has compromised or may reasonably compromise the cybersecurity of the products and services provided to Company by Contractor or the physical, technical, administrative, or organizational safeguards protecting Contractor's systems or Company's systems storing or hosting Company Information that may affect the Company Information or that could pose a cyber security risk to the Company; or (iii) Contractor receives any third-party complaint, notice, or communication which relates directly or indirectly to a Security Incident involving (A) Contractor's handling of Company Information or Contractor's compliance with the data safeguards in this

Agreement or applicable laws; in connection with Company Information or (B) a verified impact to the cybersecurity of the products and services provided to Company that could pose a cybersecurity risk to the Company

“Vulnerability” means a weakness in an information system, system security procedures, internal controls, firmware, software, or implementation that could result in a Security Incident including being exploited or triggered by a threat source.

Requirement R1.2.1
Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity.
Contractor agrees to notify Company immediately at SOC at 855-548-7276 *and* [redacted] by email, after Contractor's knowledge or reasonably suspected of an occurrence of a Security Incident. The written notice shall include the date and time of the Security Incident's occurrence (or the approximate date and time of the occurrence if the actual date and time of the occurrence is not precisely known) and a summary of the facts and circumstances of the Security Incident, including a description, to the extent known, of a) why the Security Incident occurred (*e.g.*, a description of the reason for the system failure), (b) the amount and nature of Company Information known or reasonably believed to have been Disclosed (if applicable), and (c) the measures being taken to address and remedy the Security Incident and to prevent the same or a similar event from occurring in the future. In the event Contractor is required by law enforcement to withhold such notification, Contractor is under no obligation to notify Company until such withholding is no longer required. If such written notice is provided in the preceding paragraph, Contractor shall provide written updates to the initial written notice to Company addressing any new facts and circumstances learned after the initial written notice is provided and shall provide such updates within a reasonable time after learning of those new facts and circumstances. Contractor shall reasonably cooperate with Company in Company's efforts to determine the risk posed by the Security Incident to Company Information and Company assets.

Requirement R1.2.2
Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity.

Development and Implementation of a Response Plan: Contractor shall develop and implement a "Response Plan," which shall include policies and procedures to address Security Incidents. The Response Plan shall include appropriate provisions for mitigating the harmful effects of Security Incidents and addressing and remedying the occurrence(s) to prevent the recurrence of similar Security Incidents in the future. Contractor shall provide Company access to inspect Contractor's Response Plan, provided that Contractor shall have a right to redact any part of the Response Plan that contains Contractor Proprietary Information or information protected by legal privilege.

The development and implementation of the Response Plan shall follow industry standard practices, such as those that at a minimum are consistent with the contingency planning requirements of NIST Special Publication 800-61 Rev. 2, NIST Special Publication 800-53 Rev. 4, CP-1 through CP-13 and the incident response requirements of NIST Special Publication 800-53 Rev. 4, IR-1 through IR-10 as those standards may be amended.

Prevention of Recurrence: If the Security Incident arises from Contractor-provided software, hardware, or equipment, then, within *14* days of a Security Incident, Contractor shall develop and take necessary steps to execute a plan that reduces the likelihood of the same or a similar Security Incident from occurring in the future consistent with the requirements of its Response Plan and industry standards (e.g., NIST Special Publication 800-61 Rev. 2 and NIST Special Publication 800-184, as may be amended) and shall communicate to Company the implementation of such plan to reduce a similar Security Incident. If the Security Incident arises from a third-party supplier's software, equipment or services, then if Contractor is permitted to disclose such information, Contractor shall provide updates to Company of such third-party supplier's plan for the prevention of recurrence of such Security Incident. Except to the extent publicly available, any information provided hereunder by Contractor shall be treated as confidential and not disclosed to any third party without Contractor's prior written approval, unless required by applicable governmental entities.

Coordination of Incident Response with Company:

(a) Contractor will, at its sole cost and expense, assist and cooperate with Company with respect to any investigation of and response to a Security Incident and disclosures to affected parties in connection with a Security Incident or required under any applicable laws related to a Security Incident.

(b) In the event a Security Incident results in Company Information being Disclosed such that notification is required to be made to any person or entity, including without limitation any customer, shareholder, or current or former employee of Company under any applicable laws, including privacy and consumer protection laws, or pursuant to a request or directive from a governmental authority, such notification will be provided by Company, except as required by applicable law or approved by Company in writing. Company will have sole control over the timing and method of providing such notification.

Requirement R1.2.3

Notification by vendors when remote or onsite access should no longer be granted to vendor representatives.

Development and Implementation of Access Control Policy: Contractor shall develop and implement policies and procedures to address the security of Contractor's remote and onsite access to Company Information, Company systems and networks, and Company property (an "Access Control Policy") that is consistent with the personnel management requirements of industry standard practices (e.g., NIST Special Publication 800-53 Rev. 4 AC-2, PE-2, PS- 4, and PS-5 as may be amended) and also meets the following requirements:

Company Authority Over Access: In the course of furnishing products and services to Company under this Agreement, Contractor shall not access, and shall not permit its employees, agents, contractors, and other personnel or entities within its control ("Contractor Personnel") to access Company's property, systems, or networks or Company Information without Company's prior express written authorization. Such written authorization may subsequently be revoked by Company, at any time in its sole discretion. Further, any Contractor personnel access shall be consistent with, and in no case exceed the scope of, any such approval granted by Company. All Company-authorized connectivity or attempted connectivity to Company's systems or networks shall be in conformity with Company's security policies as may be amended from time to time with notice to the Contractor.

Contractor Review of Access: Contractor will review and verify Contractor personnel's continued need for access and level of access to Company Information and Company systems, networks and property on a quarterly basis and will retain evidence of the reviews for two year from the date of each review.

Notification and Revocation: Contractor will promptly notify Company, but no later than *2* hour(s) in) when

(i) any Contractor personnel no longer requires such access in order to furnish the services or products provided by Contractor under this Agreement,

(ii) any Contractor personnel is terminated or suspended or his or her employment is otherwise ended,

(iii) Contractor reasonably believes any Contractor personnel poses a threat to the safe working environment at or to any Company property, including to employees, customers, buildings, assets, systems, networks, trade secrets, confidential data, and/or Company Information,

(iv) there are any material adverse changes to any Contractor personnel's background history, including, without limitation, any information not previously known or reported in his or her background report or record.

(v) any Contractor personnel loses his or her U.S. work authorization, or

(vi) Contractor's provision of products and services to Company under this Agreement is either completed or terminated, so that Company can discontinue electronic and/or physical access for such Contractor personnel.

Contractor will take all steps reasonably necessary to immediately revoke such Contractor personnel's electronic and physical access to Company Information as well as Company property, systems, or networks, including, but not limited to, removing and securing individual credentials and access badges, multifactor security tokens, and laptops, as applicable. Further, for such revoked Contractor personnel, Contractor will return to Company any Company-issued property including, but not limited to, Company photo ID badges, keys, parking passes, documents, or electronic equipment in the possession of such Contractor personnel. Contractor will notify Company at SOC at 855-548-7276 *and* asoc@avangrid.com once access to Company Information as well as Company property, systems, and networks has been removed.

Requirement R1.2.4
Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity.
Contractor shall develop and implement policies and procedures to address the disclosure by Contractor of known Vulnerabilities and defects related to the products and services provided to Company under this Agreement including the following: (a) Prior to the delivery of the procured product or service, Contractor shall provide or direct Company to an available source of summary documentation of publicly disclosed vulnerabilities and material defects in the procured product or services, the potential impact of such vulnerabilities and material defects, the status of Contractor's efforts to mitigate those publicly disclosed vulnerabilities and material defects, and Contractor's recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds. (b) Contractor shall provide or direct Company to an available source of summary documentation of vulnerabilities and material defects in the procured product or services within thirty (30) calendar days after such vulnerabilities and material defects become known to Contractor, consistent with ISO/IEC 30111 and 29147 for Coordinated Vulnerability Disclosure. The summary documentation shall include a description of each vulnerability and material defect and its potential impact, root cause, and recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds (e.g., monitoring). (c) Contractor shall disclose the existence of all known methods for bypassing computer authentication in the procured product or services, often referred to as backdoors, and provide written attestation that all such backdoors created by Contractor have been permanently remediated. (d) Contractor shall implement a vulnerability detection and remediation program consistent with industry standards (e.g., ISO-27417 Vulnerability Disclosure, NIST Cybersecurity Framework v1.1 Reference RS.AN-5, NIST Special Publication 800-53 Rev. 4 RA-5, SA-11, and SI-2, as may be amended.) Disclosure of Vulnerabilities by Company: Whether or not publicly disclosed by Contractor and notwithstanding any other limitation in this Agreement and following reasonable written notice provided to and acknowledged by Contractor, Company may disclose any vulnerabilities, material defects, and/or other findings related to the products and services provided by Contractor to (a) the Electricity Information Sharing and Analysis Center ("E-ISAC"), the United States Cyber Emergency Response Team ("CERT"), or any equivalent U.S. governmental entity or program, (b) to any applicable U.S. governmental entity, upon mutual agreement of Company and Contractor, when necessary to preserve the reliability of the BES, or (c) any entity required by applicable law.

Requirement R1.2.5
Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System.

Hardware, Firmware, Software, and Patch Integrity and Authenticity:

(a) Contractor shall establish, document, and implement risk management practices for supply chain delivery of hardware, software (including patches), and firmware provided under this Agreement, in accordance with industry standards and until otherwise noted with end of sale, end of support, and/or end of life. Contractor shall provide documentation on its: chain-of-custody practices, inventory management program (including the location and protection of spare parts), information protection practices, integrity management program for components provided by sub-suppliers, instructions on how to request replacement parts, and commitments to ensure that for *24 months* spare parts shall be made available by Contractor.

(b) Upon request by Company and if such information is not confidential or Contractor's Proprietary Information or otherwise protected by legal privilege, Contractor shall specify how digital delivery for procured products (*e.g.*, software and data) including patches will be validated and monitored to ensure the digital delivery remains as specified. When product features and delivery mechanisms allow, Contractor shall apply encryption technology to protect procured products throughout the delivery process.

(c) If Contractor provides software or patches to Company, Contractor shall publish or provide a hash conforming to the Federal Information Processing Standard (FIPS) Security Requirements for Cryptographic Modules (FIPS 140-2) or similar standard information on the software and patches to enable Company to use the hash value as a checksum to independently verify the integrity of the software and patches.

(d) Contractor shall identify or provide Company with a method to identify the country (or countries) of origin, of the procured Contractor product and its components (including country of manufacture (hardware) and country of build (software and firmware). Contractor will identify the countries where the development, manufacturing, maintenance, and service for the Contractor product are provided. Contractor will notify Company of changes in the list of countries where product maintenance or other services are provided in support of the procured Contractor product. This notification in writing shall occur at least 180 days prior to initiating a change in the list of countries.

(e) Contractor shall provide a software bill of materials for procured (including licensed) products consisting of a list of components and associated metadata that make up a component.

(f) Contractor shall use or arrange for the use of trusted channels to ship procured products, such as U.S. registered mail and/or tamper-evident packaging for physical deliveries,

(g) Contractor shall demonstrate a capability for detecting unauthorized access throughout the delivery process.

(h) Contractor shall provide chain-of-custody documentation for procured products appropriate to scope of supply.

Patching Governance:

(a) Prior to the delivery of any products and/or services to Company or any connection of electronic devices, assets, or equipment to Company's electronic equipment, Contractor shall provide documentation regarding the patch management and vulnerability management/ mitigation programs and update Contractor's process (including for any third-party hardware, software, and firmware) for products, services, and any electronic device, asset, or equipment required by Contractor to be connected to the assets of Company during the provision of products and services under this Agreement. This documentation shall include information regarding:

(i) the resources and technical capabilities to sustain this program and process such as the method or recommendation for how the integrity of a patch is validated by Company; and

(ii) the approach and capability to remediate newly reported zero-day vulnerabilities for Contractor products.

(b) Unless otherwise approved by the Company in writing, products and services supplied by Contractor shall not require the use of any out-of-date, unsupported, or end- of-life version of third-party components (*e.g.*, Java, Flash, Web browser, etc.).

(c) Contractor shall verify and provide documentation that procured products (including third-party hardware, software, firmware, and services) have appropriate updates and patches installed prior to product or service supply to the Company.

(d) In providing the products and services described in this Agreement, Contractor shall provide or arrange for the provision of appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses for Contractor products within *30* days. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates, within 15 days. If updates cannot be made available by Contractor within these time periods, Contractor shall provide mitigations, methods of exploit detection, and/or workarounds within 10 days.

(e) In providing third-party hardware, software (including open-source software), and firmware is provided by Contractor to Company, Contractor shall provide or arrange for the provision of appropriate hardware, software, and/or firmware updates to remediate newly discovered vulnerabilities or weaknesses, if such vulnerabilities or weaknesses are applicable to the Company's use of the third-party product in its system environment, within 30 days of availability from the original supplier and/or patching source. Updates to remediate critical vulnerabilities applicable to the Contractor's use of the third-party product in its system environment shall be provided within a shorter period than other updates, within *30* days of availability from the original supplier and/or patching source. If applicable third-party updates cannot be integrated, tested, and made available by Contractor within these time periods, Contractor shall provide or arrange for the provision

of recommended mitigations and/or workarounds within 30 days.

Viruses Firmware and Malware:

(a) Contractor will use reasonable efforts to investigate whether computer viruses or malware are present in any software or patches before providing such software or patches to Company. To the extent Contractor is supplying third-party software or patches, Contractor will use reasonable effort to ensure the third-party investigates whether computer viruses or malware are present in any software or patches providing them to Company or installing them on Company's information networks, computer systems, and information systems.

(b) Contractor warrants that it has no knowledge of any computer viruses or malware coded or introduced into any software or patches, and Contractor will not insert any code which would have the effect of disabling or otherwise shutting down all or a portion of such software or damaging information or functionality. To the extent Contractor is supplying third-party software or patches, Contractor will use reasonable efforts to ensure the third-party will not insert any code which would have the effect of disabling or otherwise shutting down all or a portion of such software or damaging information or functionality.

(c) When install files, scripts, firmware, or other Contractor-delivered software solutions (including third-party install files, scripts, firmware, or other software) are flagged as malicious, infected, or suspicious by an anti-virus vendor, Contractor must provide or arrange for the provision of technical justification as to why the "false positive" hit has taken place to ensure their code's supply chain has not been compromised.

(d) If a virus or other malware is found to have been coded or otherwise introduced as a direct result of Contractor's breach of its obligations under this Agreement, Contractor shall upon written request by Company and at its own cost:

(i) Take all commercially reasonable action to eliminate the virus or other malware throughout Company's information networks, computer systems, and information systems; and

(ii) If the virus or other malware causes a loss of operational efficiency or any loss of data (A) where Contractor is obligated under this Agreement to back up such data, take all commercially reasonable steps necessary and provide all assistance required by Company and its affiliates, or (B) where Contractor is not obligated under this Agreement to back up such data, use commercially reasonable efforts, in each case to mitigate the loss of or damage to such data and to restore the efficiency of such data.

End of Life Operating Systems:

(a) Unless otherwise mutually agreed, Contractor-delivered solutions will not be required to reside on end-of-sale, end-of-support, and end-of-life operating systems, or any operating system that is known to be reaching such status six (6) months from the date of installation.

(b) As mutually agreed, Contractor solutions will support the latest versions of operating systems on which Contractor-provided software functions within twenty-four (24) months from official public release of that operating system version.

Cryptographic Requirements:

(a) Contractor shall document how the cryptographic system supporting the Contractor's products and/or services procured under this Agreement protects the confidentiality, data integrity, authentication, and non-repudiation of devices and data flows in the underlying system. This documentation shall include, but not be limited to, the following:

(i) The cryptographic methods (hash functions, symmetric key algorithms, or asymmetric key algorithms) and primitives (*e.g.*, Secure Hash Algorithm SHA- 256, Advanced Encryption Standard AES-128, RSA, and Digital Signature Algorithm DSA-2048) that are implemented in the system, and how these methods are to be implemented.

(ii) The preoperational and operational phases of key establishment, deployment, ongoing validation, and revocation.

(b) Contractor will use only "approved" cryptographic methods as defined in the FIPS 140-2 Standard when enabling encryption on its products.

(c) As mutually agreed, Contractor shall provide or arrange for the provision of an automated remote key-establishment (update) method that protects the confidentiality and integrity of the cryptographic keys.

(d) Contractor shall ensure that:

(i) As mutually agreed, the system implementation includes the capability for configurable cryptoperiods (the life span of cryptographic key usage) in accordance with the Suggested Cryptoperiods for Key Types found in Table 1 of NIST 800-57 Part 1, as may be amended.

(ii) As mutually agreed, the key update method supports remote re-keying of all devices within *6 months* as part of normal system operations.

(iii) Emergency re-keying of all devices can be performed remotely or on-site within 30 days.

(e) Contractor shall provide or arrange for the provision of a method for updating cryptographic primitives or algorithms.

Requirement R1.2.6
Coordination of controls for (i) vendor-initiated interactive remote access, and (ii) system-to-system remote access with a vendor(s).
Contractor shall coordinate with Company on all remote access to Company's systems and networks, regardless of interactivity, and shall comply with any controls for interactive remote access and system-to-system remote access sessions requested by Company. Controls for Remote Access: Contractors that directly, or through any of their affiliates, subcontractors, or service providers, connect to Company's systems or networks agree to the additional following protective measures: (a) Contractor will not access and will not permit any other person or entity to access, Company's systems or networks without Company's written authorization and any such actual or attempted access will be consistent with any such written authorization. (b) Contractor shall implement processes designed to protect credentials as they travel throughout the network and shall ensure that network devices have encryption enabled for network authentication to prevent possible exposure of credentials. (c) Contractor shall ensure Contractor Personnel do not use any virtual private network or other device to simultaneously connect machines on any Company system or network to any machines on any Contractor or third-party systems, without (i) using only a remote access method consistent with Company's remote access control policies, (ii) providing Company with the full name of each individual who uses any such remote access method and the phone number and email address at which the individual may be reached while using the remote access method, and (iii) ensuring that any computer used by Contractor personnel to remotely access any Company system or network will not simultaneously access the Internet or any other third-party system or network while logged on to Company systems or networks. (d) Contractor shall ensure Contractor Personnel accessing Company networks are

Supporting Provisions

Contractor Cybersecurity Policy:

Contractor will demonstrate to Company the Contractor's cybersecurity policy which shall be consistent with industry standard practices (e.g., NIST Special Publication 800-53 (Rev. 4) as may be amended). Contractor will implement and comply with its established cybersecurity policy.

Any changes to Contractor's cybersecurity policy as applied to products and services provided to Company under this Agreement and Company Information shall not decrease the protections afforded to Company or Company Information and any material changes shall be communicated to the Company in writing by Contractor prior to implementation.

Return or Destruction of Company Information:

Upon the later of (i) completion of the delivery of the products and services to be provided under this Agreement, (ii) the termination of any applicable warranty period under the Agreement or (iii) the termination of this Agreement, Contractor will return to Company all hardware and removable media provided by Company containing Company Information. Company Information in such returned hardware and removable media shall not be removed or altered in any way. The hardware should be physically sealed and returned via a bonded courier or as otherwise reasonably directed by Company. If the hardware or removable media containing Company Information is owned by Contractor or a third-party, a notarized statement detailing the destruction method used and the data sets involved, the date of destruction, and the entity who performed the destruction will be sent to a designated Company security representative within thirty (30) calendar days after the later of (i) completion of the delivery of the products and services to be provided under this Agreement, (ii) the termination of any applicable warranty period under the Agreement or (iii) the termination of this Agreement. Contractor's destruction or erasure of Company Information pursuant to this Section shall be in compliance with industry standard practices (*e.g.*, Department of Defense 5220-22-M Standard, as may be amended).

Audit Rights:

Upon request, Contractor shall provide to Company the opportunity to review a copy of the Contractor's policies, procedures, evidence and independent audit report summaries, , that are part of a cyber security framework (e.g., ISO-27001, SOC2). Company or its third-party designee may, but is not obligated to, perform audits or other tests of Contractor's IT or systems environment and procedural controls to determine Contractor's compliance with the system, network, data, and information security requirements of this Agreement. Company audits of the Contractor system shall be done with at least 30 days advance notice. These audits and tests may include coordinated security tests as mutually agreed to not unduly affect Contractor operations, interviews of relevant personnel, review of documentation, and technical inspection of systems and networks as they relate to the receipt, maintenance, use,

retention, and authorized destruction of Company Information. Contractor shall provide all information reasonably requested by Company in connection with any such audits and shall provide reasonable access and assistance to Company upon request. Contractor will comply, within reasonable timeframes at its own cost and expense, with all reasonable recommendations that result from such inspections, tests, and audits. Company reserves the right to view, upon request, any original security reports that Contractor has undertaken or commissioned to assess Contractor's own network security. Any regulators of Company or its affiliates shall have the same rights of audit as described herein upon request.

Regulatory Examinations:

Contractor agrees that any regulator or other governmental entity with jurisdiction over Company and its affiliates may examine Contractor's activities relating to the performance of its obligations under this Agreement to the extent such authority is granted to such entities under the applicable law. Contractor shall promptly cooperate with and provide all information reasonably requested by the regulator or other governmental entity in connection with any such examination and provide reasonable assistance and access to equipment, records, networks, and systems reasonably requested by the regulator or other governmental entity. Contractor agrees to comply with reasonable recommendations that result from such
regulatory examinations within reasonable timeframes.

SCHEDULE J
AVANGRID CONTRACTOR SAFETY REQUIREMENTS