GPA

Cybersecurity

TABLE OF CONTENTS

1. Cybersecurity

GPA has adopted the NIST Framework for Improving Critical Infrastructure Cybersecurity. New system refers to the system that will be implemented for the project.

CONTRACTOR will deliver a system that is cyber secure and physically secure. GPA will be acquiring services for vulnerability assessments and penetration testing.

2. Standards

The CONTRACTOR shall design communications, physical and electronic security based on but not limited to the following standards:

- IEEE Standards
  - C37.1-2007, IEEE Standard for SCADA and Automation Systems
  - C37.2-2008, IEEE Standard for Electrical Power System Device Function Numbers, Acronyms, and Contact Designations
  - C37.90.1-2012, IEEE Standard for Surge Withstand Capability (SWC) Tests for Relays and Relay Systems Associated with Electric Power Apparatus
  - C37.238-2011, IEEE Standard Profile for Use of IEEE 1588™ Precision Time Protocol in Power System Applications
  - 487-2007, IEEE Recommended Practice for the Protection of Wire-Line Communication Facilities Serving Electric Supply Locations
  - 789-1988, IEEE Standard Performance Requirements for Communications and Control Cables for Application in High Voltage Environments
  - 1379-2000, IEEE Recommended Practice for Data Communications Between Remote Terminal Units and Intelligent Electronic Devices in a Substation (W/D)
  - 1402-2000, IEEE Guide for Electric Power Substation Physical and Electronic Security
  - 1613-2009, IEEE Standard Environmental and Testing Requirements for Communications Networking Devices Installed in Electric Power Substations
  - 1615-2007, IEEE Recommended Practice for Network Communication in Electric Power Substations
  - 1646-2004, IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation
  - 1686-2013, IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities
  - 1062-1998 (R2002), IEEE Recommended Practice for Software Acquisition
  - 1220-2005, IEEE Standard for Application and Management of the Systems Engineering Process
  - 15026-1-2011, IEEE Trial-Use Standard--Adoption of ISO/IEC TR 15026-1:2010 Systems and Software Engineering--Systems and Software Assurance--Part 1: Concepts and Vocabulary
  - 15026-2-2011, IEEE Standard--Adoption of ISO/IEC 15026-2:2011 Systems and Software Engineering--Systems and Software Assurance--Part 2: Assurance Case
  - 15288-2008, IEEE Systems and software engineering — System life cycle processes
  - 15289-2011, Systems and software engineering -- Content of life-cycle information products (documentation)
  - 15939-2008, IEEE Standard Adoption of ISO/IEC 15939:2007— Systems and Software Engineering— Measurement Process

    - 16085-2006, IEEE Systems and software engineering — Life cycle processes — Risk management
    - 16326-2009, ISO/IEC/IEEE Systems and Software Engineering--Life Cycle Processes--Project Management
    - 24748-1-2011, IEEE Guide--Adoption of ISO/IEC TR 24748-1:2010 Systems and Software Engineering--Life Cycle Management--Part 1: Guide for Life Cycle Management
    - 1220-2005, IEEE Standard for Application and Management of the Systems Engineering Process
    - 29148-2011, ISO/IEC/IEEE Systems and software engineering -- Life cycle processes -- Requirements engineering
    - 42010-2011(E) (Revision of ISO/IEC 42010:2007 and IEEE Std 1471-2000), ISO/IEC/IEEE Systems and software engineering -- Architecture description
    - IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads
- National Institute of Standards and Technology (NIST)
    - Framework for Improving Critical Infrastructure Cybersecurity

3. Guides

The CONTRACTOR shall design communications, physical and electronic security based on but not limited to the following guides:

- National Renewable Energy Laboratory (NREL)
    - INEEL/EXT-04-01517
- Roadmap to Achieve Energy Delivery Systems Cybersecurity, DOE (2011)
- Roadmap to Secure Control Systems in the Energy Sector, DOE (2006 Roadmap)
- Cross-Sector Roadmap for Cybersecurity of Control Systems, DHS Industrial Control Systems Joint Working Group (ICSJWG) (2011)
- Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline, DOE (2014)
- Energy Sector Cybersecurity Framework Implementation Guidance, DOE (2015)
- The CERT® Resilience Management Model (CERT®-RMM), Software Engineering Institute
- NERC Cyber Risk Preparedness Assessment (CRPA): Improving the Cyber Security
- Posture of the North American Bulk Power System, North American Electric Reliability Corporation (NERC)
- NIST Interagency Report (NISTIR) 7628, Guidelines for Smart Grid Cyber Security, National Institute of Standards and Technology (NIST)
    - Vol. 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements
    - Vol. 2 - Privacy and the Smart Grid
    - Vol. 3 - Supportive Analyses and References
- NIST Special Publication 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy (2009)
- NIST Roadmap for Improving Critical Infrastructure Cybersecurity (2014)
- PNNL-20776, Secure Data Transfer Guidance for Industrial Control and SCADA Systems (2011)
- Cyber Attack Task Force (CATF) Final Report, North American Electric Reliability Corporation (NERC)
- Cybersecurity Procurement Language for Energy Delivery Systems (2014)

- Roadmap to Secure Control Systems in the Chemical Sector (2009), U.S. Department of Homeland Security and the Chemical Sector Coordinating Council
- Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), DOE (2014)
- Vulnerability Analysis of Energy Delivery Control Systems, DOE (2011)
- Cybersecurity Risk Management Process Guideline, DOE (2011)
- Cybersecurity and the Smarter Grid, DOE (2014).

4. Minimum Hardware/Software Requirements For Secure Network Services

Minimum Hardware/Software requirements for securing network services include:

- Log Event Manager (LEM) – we must be able to collect events and status for the entire network and be able to use the collected data for analysis whenever required. Data collected by the LEM can be used for forensics and post-analysis from any cyber-related incident.
- Network Management System (NMS) – provides status on device health, network performance, link status, server health, and a multitude of other data the will be useful in monitoring the overall status of the network.
- Firewall Pair – a firewall pair (for High-availability) must stand in between the Enterprise network and the network to create a separation between the security zones.
- Intrusion Prevention/Detection System (IPS/IDS) pair – an IDS/IPS system should be used to monitor and detect threats and anomalies moving in and out of the security zones.
- Backup/Archiving Hardware and Software – this will serve as a contingency plan in the event of system or device failures.
- Perimeter Anti-virus appliance/solution – primary defense against malicious code (Malware) which usually serves as a precursor for a cyber-attack.

4.1. High-Level Minimum Requirements for Network Security Related Hardware

High-Level minimum Hardware/Software requirements for securing new system network services include:

1) Server Hardware
- Technical specifications (CPU, memory, NIC capacity, etc.) will be dependent on vendor recommendations.
- Supports 1GbE and 10GbE interfaces.
- Redundant “Hot-swappable” power supplies.
- Supports Fiber Channel (FC).
- Blade server system is preferred but not required.

2) Firewall/s (pair is required)
- High-availability (HA) features such as clustering, active/active, and/or active/standby modes.
- Minimum of 6 Gigabit Ethernet (RJ-45/SFP) ports.
- Performs stateful inspection.
- Capable of supporting Dynamic Routing Protocols RIP, OSPF, and BGP.

- Capable of performing route distribution.
- Supports NetFlow, SNMPv3, and Syslog.
- Supports VLANs.
- Supports Remote Access VPN (SSL and IPSec) and Site-to-site VPN.

Maintenance contract must allow for a device replacement time frame of no later than 3 days.

3) Intrusion Prevention/Detection System (pair is required)

- High-availability (HA) features such as clustering, active/active, and/or active/standby modes.
- Minimum of 6 Gigabit Ethernet (RJ-45/SFP) ports or able to support 3 Gigabit inline-pairs .
- Individual sensors for each inline-pair.
- "Fail-open" feature
- Supports SNMPv3 and Syslog.
- Redundant "Hot-swappable" power supplies (preferred but not required).
- Advanced Threat Detection and Global Correlation capabilities.
- IPS Throughput of 500Mbps
- Supports LDAP and RADIUS integration.
- Maintenance contract must allow for a device replacement time frame of no later than 3 days.

4) Backup/Archiving Hardware

- Max data throughput of =>5TB/hr.
- Logical Capacity =>500TB / Usable Capacity of =>70TB.
- Supports at least 4x 8GB FC.
- Electronic Industries Alliance (EIA) rack mountable.
- Redundant Power Supplies.
- Supports RAID-5 and RAID-6.
- Supports Link Aggregation Control Protocol (LACP).
- Power input of 100-120/200-240VAC.

5. Guidelines And Recommendations

5.1. Security Controls

5.1.1. Minimum Operational and Administrative Requirements

Minimum operational and administrative requirements include:

- Automatic auditing of firewalls and other security devices.
- Backup and archiving of the new system information and the configuration of critical network devices should be a part of a contingency plan.
- Configuration Management policies and procedures must be included as part of the new system; Configuration change processes must be documented. (refer to NIST SP 800-12 and 800-70) for guidance.
- The Log Event Manager (LEM) and Network Management System (NMS) should be able to notify administrative personnel of high risk incidents.
- IPS/IDS systems must be installed as part of the network architecture. This will help in monitoring events and logging data of traffic patterns and file accesses for future analysis.
- Anti-virus and malware protection systems must be implemented to address vulnerabilities.

5.1.2. Minimum Technical Requirements

The Bidder shall perform the due diligence work to ensure adequate security controls. Minimum technical requirements include:

- Multi-factor authentication must be used to access the new system network.
- Network infrastructure related services must be separate from Enterprise network.
- Logically separate network traffic through the use of VLANs.
- Introduce Role-based access control (RBAC) to accurately define access and authorization controls.
- Use VPNs (IPsec/SSL/SSH) between endpoints within the new system network.
- ACL configurations should begin with a “deny all” then permit ACLs be configured above it explicitly. Certain traffic may also have to be denied explicitly.

5.2. Network Architecture

5.2.1. Firewalls

Minimum requirements include:

- State-full inspections should be the minimum required feature.
- Packet Filtering
- Stateful Inspection, Deep Packet Inspection, Stateful Protocol Analysis
- High-availability (HA) firewalls, which allow one firewall to take over for another if the first firewall fails or is taken offline for maintenance is a mandatory requirement

5.2.2. Logical Separation of Network (Network Segregation)

The Bidder must provide a GPA’s minimum requirements include:

- Firewalls must be used to separate control networks and to define security zones.
- New system network and Enterprise network MUST be in distinct security zones and separated through the use of firewalls.
- Networks belonging to the same security zone may be separated through the use VLANs.
- Dual-homed workstations and/or servers (Dual Network Interface Cards) is not acceptable in a new system network. Workstations requiring internet access must belong to a security zone other than the new system security zone (e.g Enterprise network).

5.2.3. Firewall Policies

Minimum requirements include:

- Enterprise to new system network access must be very limited and access to field devices from Enterprise network workstations should be prohibited.
- A new system DMZ network will be introduced into the overall network architecture. The objective is to limit access to the new system production network. New system services and data to be accessed will be accessible on the new system DMZ network.
- All untrusted (Outside network) traffic will be blocked from entering the network.

- ACLs in the Firewalls must be granularly designed by allowing specific port types (TCP/UDP) and port numbers.
- Unused or unneeded ports and services will be explicitly “denied” and will be defined in the design of the Firewall ACLs.
- All inbound traffic to the new system network must be “denied” and authorized traffic should be explicitly configured to be permitted.

5.2.4. Device Configurations (guided by defense-in-depth methodologies)

GPA minimum requirements include:

- All unused ports (routers and switches) must be administratively disabled.
- MAC address locking will be implemented to secure endpoint devices/hosts and in order to avoid “man-in-the-middle” attacks.
- All default passwords on devices must be changed with complex ones.
- AAA authentication will be implemented on all network devices.
- LDAP (Active Directory) and RADIUS will be the infrastructure service for authentication and authorization.
- Telnet, HTTP, and other forms of unsecure, “clear-text” access will explicitly disabled.
- All default configurations on devices and hosts should be changed before attaching into the GPA network.