SQAD – **7** REQUIREMENTS FOR CYBER SECURITY RELATED ITEMS OR SERVICES

1 GENERAL

Each item or service ordered for which this quality statement is referenced, shall require the supplier to comply with the cyber security procurement requirements outlined within this Special Quality Assurance Document (SQAD). These requirements apply to the immediate supplier, Original Equipment Manufacturer (OEM) distributor or any Third Party suppliers that manufactured the product or enhanced the product provided by the OEM.

2 SUPPLY CHAIN PROTECTION

Supplier, OEM, distributor or Third Party Supplier acknowledges and certifies that they have cyber security protection controls and measures in place to protect against supply chain cyber security threats in order to maintain the integrity of the Critical Digital Asset (CDA) during the design, manufacturing and distribution processes. The supplier shall certify that the product or service procured conforms to the following provisions:

2.1 Requirement of tamper proof products or tamper evident seals on acquired products:

Hardware and software shall be delivered to the owner using tamper-evident packaging, or shall be of a nature that the product itself is a tamper-proof product. For software, hash codes/with algorithm shall be provided if item is supplied without a tamper proof seal, so that the file integrity can be confirmed. **Items not meeting this requirement will be immediately returned.**

2.2 Establishment of Trusted Distribution Paths:

Supplier has established a trusted distribution path for the supplier/OEM and sub-supplier distribution paths shall use known, traceable, and reputable suppliers and distributors throughout the supply chain from component fabrication through delivery to the acquirer. Surplus, open box, or bid sites are considered untrusted sources.

2.3 Validation of Supplier:

The supplier shall have either a history of supplying defect free cyber security compliant material/services to the nuclear power industry or an Achilles cyber security program and process certification. Crediting other certifications or practices is subject to Exelon approval at the time of Purchase Order and/or Contract acceptance by the supplier.

3 RIGHT OF ACCESS

Exelon, its agents or assignees, shall have the right to inspect and evaluate those applicable cyber security areas of Supplier or sub-tier facilities and activities at a mutually agreed time during the procurement process. Inspections, surveillances, tests or non-financial audits performed by Exelon or its agents shall in no way relieve the supplier or your sub-tiers of any responsibilities under the Purchase Order / Contract.

4 TRUST WORTHINESS

The supplier certifies that the CDA being procured meets the cyber security requirements established in this document and requires that software developers employ recognized software assurance practices, quality controls and validation measures to minimize flawed or malformed software. This shall include methods to detect flawed or malicious elements in any open-source, purchased, or supplier proprietary source code used in the system being delivered.

5 INTEGRATION OF SECURITY CAPABILITIES

The Supplier, OEM, distributor, and Third Party involved in the manufacture or enhancement of the CDA product shall:

- Maintain cognizance of evolving cyber security threats and vulnerabilities pertaining to hardware and software that they use or produce.
- Maintain cognizance of evolving cyber security protective strategies and security controls.
- Maintain a process of analysis to determine the impact that advancements in cyber security threats and protective strategy could have on the security, safety, and operation of the nuclear critical assets, systems, CDAs, and networks that they produce, deliver, or use.

Distributors or Third Parties in the supply chain/distribution path that do not break the OEM seal are exempt from these requirements.

6 DEVELOPER SECURITY TESTING

The Supplier, OEM, distributor, or Third Party involved in the manufacture or enhancement of the product shall employ a cyber security test and evaluation plan to ensure that products are delivered to meet specified security requirements, as outlined in this document. The testing shall ensure the product is free from known vulnerabilities and malicious code at the time of design and product delivery.

7 PROCUREMENT OF SERVICES

Services furnished under this Contract, at Exelon Facilities, are classified as Cyber Security Related and shall be subject to the controls of the Exelon Cyber Security Program. When providing services on critical digital assets (hardware, firmware, operating systems, or application software) at Exelon facilities, supplier agrees to abide by Exelon Cyber Security Program as follows:

A. Contractors before being permitted access to Exelon network will be made aware of Exelon's cyber security program and must agree to abide by the relevant policies.
B. Contractors will adhere to the following Exelon cyber security policies:

1. Configuration management of the contractor's computers, to include virus protection, patch management, authentication requirements and secure Internet connections.

2. Maintain secure transfer and storage of information and code while off-site.

3. Duty to protect confidentiality.

8 CERTIFICATE OF COMPLIANCE

Each item or service for which this quality statement is specified shall require a certification that the item or service supplied complies with Exelon procurement clause SQAD-7 requirements specified in this document. The supplier shall submit under supplier's letterhead a signed Certificate of Compliance (C of C) as described below. A statement shall be included to the effect that the OEM, distributor, or Third Party has performed all the final inspections and tests required to verify conformance of the items or services supplied. This document shall reference the Exelon Purchase Order (PO)/Contract number. When needed, a separate Certificate of Compliance shall be included from the distributor or Third Party supplier that is responsible for breaking the seal to ensure compliance with this document.

Supplier Cyber Security "Certificate of Conformance"

The items or services supplied under this Purchase Order/Contract comply with the requirements of Exelon SQAD-7 and tamper proof seal requirement, except for any Exelon approved exceptions listed below.

Exelon PO/Contract Number/Line item number: _____
Exelon Stock Code/Catalog Id: _____
Any exceptions: _____
Exelon Approval of exceptions: _____
Authorized Supplier Representative: _____

OEM: _____ Title:_____ Date:_____

Distributor: _____ Title:_____ Date:_____

Third Party: _____ Title:_____ Date:_____

The date, title, and signature (written, electronic, facsimile, etc.) of a technical or quality representative shall appear indicating approval of the certificate.

9 RECEIPT INSPECTION – EXELON USE ONLY

Exelon receiving shall ensure:

A. Verify the tamper-proof seal is still intact or the product itself is a tamper proof product

B. Verify a completed Supplier Cyber Security Certificate of Compliance meeting the requirements of paragraph 5.0 was included from the OEM, distributor, and/or Third Party as applicable.

C. Verify all exceptions are resolved, complete and closed.