Overview of Nuclear Cyber Security Program on Suppliers

Presented by
Barbara Weber

Cyber Security Program

The NRC's cyber security rule - 10 CFR 73.54 "Protection of digital computer and communication systems and networks" requires:

Each nuclear plant licensee to

- protect specific functions in critical systems from cyber-attacks and submit a cyber security plan and schedule that implements the requirements contained in the regulation.

Cyber Security Program

The goal of the cyber security program is to protect the health and safety of the public from a radiological event due to a successful cyber attack on a system that performs or is associated with:

- **Safety-related**
- **Important-to-safety**
- **Physical security, and**
- **Emergency preparedness functions** --

commonly called “SSEP functions”

Cyber Security Program

It also includes Balance of Plant (BOP) Critical Systems functions:

- Structures, systems, and components **(SSCs) in the balance of plant (BOP)** that could directly or indirectly affect reactivity at a nuclear power plant and could result in an unplanned reactor shutdown or transient.

Cyber Security Program

The Cyber Security Program provides "high assurance" that Critical Digital Assets (CDAs) are protected:

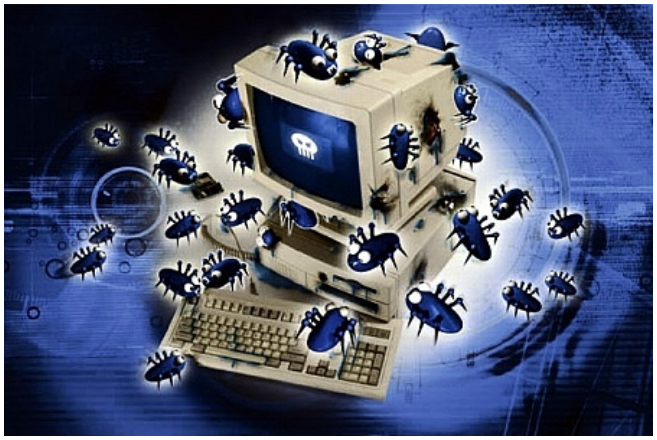
- A critical digital asset is a subcomponent of a critical system that consists of or contains a **digital device, computer or communication system, or network** that performs or supports an SSEP function.

Cyber Security Program

The Cyber Security Program establishes a Cyber Security Assessment Team that:

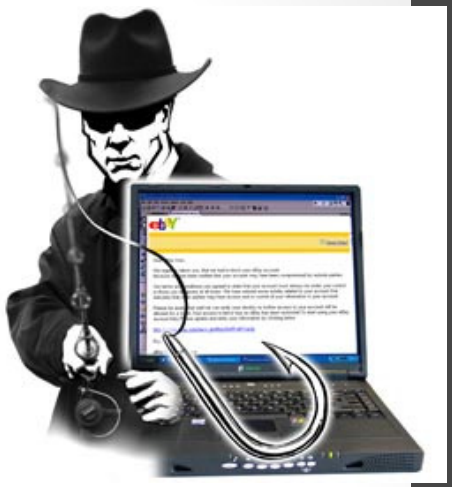
- Identifies Critical Systems and Critical Digital Assets
- Assesses the implementation of cyber security controls on Critical Digital Assets
- Articulates the required cyber security controls for suppliers and their products in **CDA-Related and associated service procurements**.

Cyber Security Program



- The supplier must apply cyber security controls to CDAs to prevent them from providing a pathway to or vulnerabilities to cyber attacks.
- The supplier's products must ensure that the product can apply these controls. Examples follow.

Supplier Validation - Secure Development and Operating Environment



The supplier must be aware of the cyber threats in the world, and to have established a secure development and operating environment (SDOE) that provides a high assurance the product(s) they deliver are free of malicious and non-malicious acts.

Examples of Supplier Awareness

Examples of supplier awareness is demonstrated by the following:

- A written cyber security strategy and how the strategy is implemented.
- Development environment that is isolated from the business environment.
- A Physical Security Plan that provides high assurance that assets are protected while in the Supplier's possession.
- Audit process to insure the supplier's policies are being implemented.
- Documented policies and procedures for patch management and updating their environments. This includes how the supplier protects their environments from third party suppliers.
- Well documented procedure and framework for conducting code reviews.

Supplier Validation - Trustworthy Staff

The supplier must have verified the trustworthiness of their people who will work on CDA-Related procurements.

Examples of supplier's verification of a trustworthy staff are such things as the following:

- Evidence that the project and environment personnel have passed an investigation that included a credit check and a national and local background check in the last 5 years.
- Cyber Awareness training for their staff.
- An effective behavior observation program to insure personnel remain trustworthy.
- Evidence the programming/manufacturing staff use quality and validation methods to minimize flawed or malformed software and equipment.

Supplier Validation - Trustworthy Supply Chain

The supplier must have measures in place that protect the product against supply chain threats and maintain the integrity of software and objects supplied to them.

Examples of supplier's protection against supply chain threats are such things as the following:

- Evidence of established trusted distribution paths.
- Evidence of validating their suppliers.
- Evidence of how the supplier insures the items they receive have not been tampered with

Supplier Validation - Problem Resolution

The supplier must provide upgrades and patches to their systems/equipment when security issues are identified.

Examples of problem resolution capabilities are such things as the following:

- A process to inform customer in writing of a flaw with any third party products supplied by the supplier in a timely manner
- A process for users to submit problems and requests for resolution. This process will include how customer's vulnerabilities are protected from public disclosure.
- A program to discover flaws and exploits associated with the products.

Product Specification - Access Control

The objective of access control is to provide high assurance that only authorized persons or processes can access CDAs and perform authorized functions.

Examples of access control are the following:

- At a minimum the product will have separate roles for normal operation, maintenance functions and security functions. No guest accounts.
- User rights and permissions for each account will be established at logon. The practice of least privilege will be followed. No user can escalate their privileges.
- Documentation will be provided showing the existence of any vendor configured or manufacturer default accounts, usernames, password, security setting, security codes or any other access methods.
- User credentials will not be transmitted in the clear.

Access Control (continued)

Examples of access control:

- Access methods or parameters are changed, disabled or removed.
- Any Human Machine Interface (HMI) stations expected to remain logged in continuously will be documented and only permitted to execute operational functions. No maintenance or security functions.
- The product will have a configurable account password management system that supports the customer's Password Standard.
- No wireless access while in operation.

Product Specification – System Hardening

The supplier's product must be hardened against cyber vulnerabilities. Hardening is the process where changes are made to the default configurations of a product to reduce security vulnerabilities.

System Hardening examples includes some of the following:

- A written list detailing all services and ports needed for normal and emergency operation. This list will include the reason the listed services and ports are required.
- All services and users will execute at the least privilege possible.
- All services not needed for operation will be removed.
- All patches and security options are applied at the time of delivery, including any third party software supplied.
- Disable all unneeded communication ports, portable media ports, or provide physical barriers.
- Host intrusion detection will be supplied where possible.

What Cyber Security Program?

- Licensee implementation stages vary:
  - ✓Identify CDAs
    - ✓Assess CDAs and Implement Controls
      - ✓Articulate controls in CDA-Related Procurements
        - ✓Maintain Cyber Security Program
- Licensee full program due dates:
  - ✓End of 2016 through end of 2017