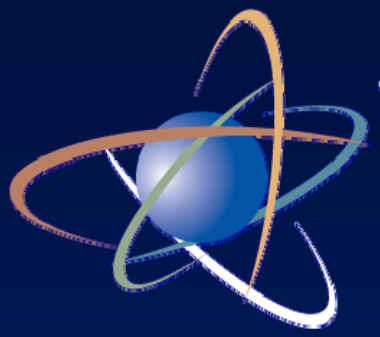


U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Cyber Security

Stacy Smith
Office of New Reactors

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Why are we talking about cyber security?

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

- White House Executive Order (2013): "cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront…"

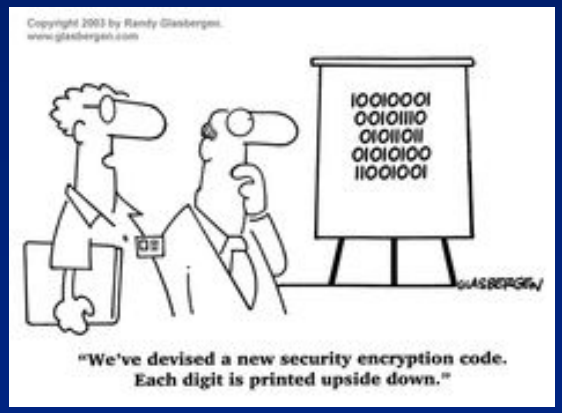
- In November 2014, NSA Director Navy Adm. Michael Rogers told the House Permanent Select Committee on Intelligence that a number of foreign governments had already managed to penetrate U.S. energy, water and fuel distribution systems, which has potential to damage essential services.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

- Hackers hit the bulls-eye on "several" of their nuclear targets: "These organizations reported that their enterprise networks were compromised and in some cases, exfiltration of data occurred," the DHS team wrote. It said that it is not aware of any successful breaches of nuclear control networks.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

What is cyber security?



"We've devised a new security encryption code.
Each digit is printed upside down."

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Cyber security is the protection of digital assets including digital instrumentation and control systems or equipment.

Cyber security at nuclear power plants promotes performance-based programmatic approaches supported by defense-in-depth strategies, including efforts to detect, prevent, delay, mitigate, and recover from cyber attacks.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

In 2009, the NRC published cyber security rule, 10 CFR 73.54 "Protection of Digital Computer and Communication Systems and Network". The cyber security rule is a performance-based programmatic requirement that ensures that the functions of digital computers, communication systems, and networks associated with safety, important-to-safety, security, and emergency preparedness are protected from cyber-attacks.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Why is the Office of New Reactors Involved?

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

- Vendors provide an instrumental role in the prevention of cyber threats

- NRO leads and performs routine and reactive vendor inspections and quality assurance implementation inspections for new and operating reactors due to the formation of the Centers of Expertise.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

- An Agencywide approach to Counterfeit, Fraudulent and Suspect Items (SECY-11-0154)
  - The staff will conduct NRC vendor inspections at suppliers of safety-related critical digital assets, in accordance with 10 CFR Part 21 and evaluate the results of these inspections to determine the need to expand the inspection sample to suppliers and sub-suppliers of non-safety-related critical digital assets

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Inspection Procedure 43002

e. Verify that there are provisions in the procedures to verify the validity of certificates and determine the effectiveness of the certification system when desired, such as during the performance of audits. Verify that certificates of conformance/compliance identify the material, equipment, or service supplied; identify specific procurement requirements (codes, standards, certificates, or other specifications such as cyber security requirements) that have been met as well as those that have not been met, together with an explanation and the means for resolving the nonconformance; and identify the supplier=s QA individual responsible for authenticating such certificates. If any criteria have not been met, verify if a nonconformance report was initiated and follow up on its resolution.

f. Verify that receiving inspections examine objective evidence of purchased items by verifying attributes specified in procurement documents. Receiving inspections should verify, as a minimum, item configuration, dimensions, physical characteristics, and identification and traceability of material and equipment, including status of inspection or tests performed, as required.

g. Verify that the vendor has a documented method for the identification and control of nonconforming material and components, including fraudulent parts, to preclude inadvertent use.

h. When possible, observe and assess actual techniques being used and their acceptability relative to contract/procedural requirements. (This includes implementation of cyber security requirements passed down from the licensee or applicant)

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Why are we (vendors) talking about cyber security now?

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Licensees are passing down cyber requirements to vendors though purchase orders

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

- The NRC issued RG 5.71, “Cyber Security Programs for Nuclear facilities” as a way for licensees and applicants to implement the Cyber Security Rule
  - promotes a defensive strategy consisting of a defensive architecture and a set of security controls
    - Includes supply chain controls

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

C.12.2 Supply Chain Protection

- [Licensee/Applicant] protects against supply chain threats and vulnerability by employing the following list of measures to protect against supply chain threats to maintain the integrity of the critical digital assets that are acquired:
  - establishment of trusted distribution paths
  - validation of vendors, and
  - requiring tamper proof products or tamper evident seals on acquired products.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

C.12.5 Developer Security Testing

- [Licensee/Applicant] documents and requires that system developers and integrators of acquired critical digital assets create, implement, and document a security test and evaluation plan to ensure that the acquired products meet all specified security requirements (1) that the products are free from known, testable vulnerabilities and malicious code by identifying and eliminating these following vulnerabilities and other vulnerabilities that may change with new technology:

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

What's going on today?

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

- Several licensee purchase orders to a vendor requiring:
  - No harmful code or malicious logic vendor shall have appropriate procedures in place to ensure that no viruses, malicious code or unintended code is transported into the production environment or the operational environment.
- Vendor did not have a documented cyber security program in place to meet purchase order requirements

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

- Information Notice 2016-01 Allen Bradley Relays
  - Manufacturer redesigned to use a complex programmable logic device (CPLD)
  - Led to loss of a safety function

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

How do we do better?

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

- A collaborative approach between the licensee and vendor
  - Have a questioning attitude
  - Know what you're providing
  - Understand what cyber specifications are being passed down and when they should be implemented
  - Know what procedures and programs need to be developed or used

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

- Cyber Security will be a continual challenge
  - Coordination is Essential

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Questions?

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

ADAMS Accession Numbers

- Inspection Procedure 43002
  - ML13148A361
- Cyber Vendor Inspection Report
  - ML15342A429
- Allen Bradley Information Notice
  - ML15295A173