Cyber Security for the Nuclear Supply Chain

Nebraska Public Power District

"Always there when you need us"

June 21, 2017

The 26th Annual NUPIC Vendor Meeting

George Lipscomb
Owner / Principal Consultant
Goldwing Services, LLC

Talisa Chambers
QA Engineer
Cooper Nuclear Station

Agenda

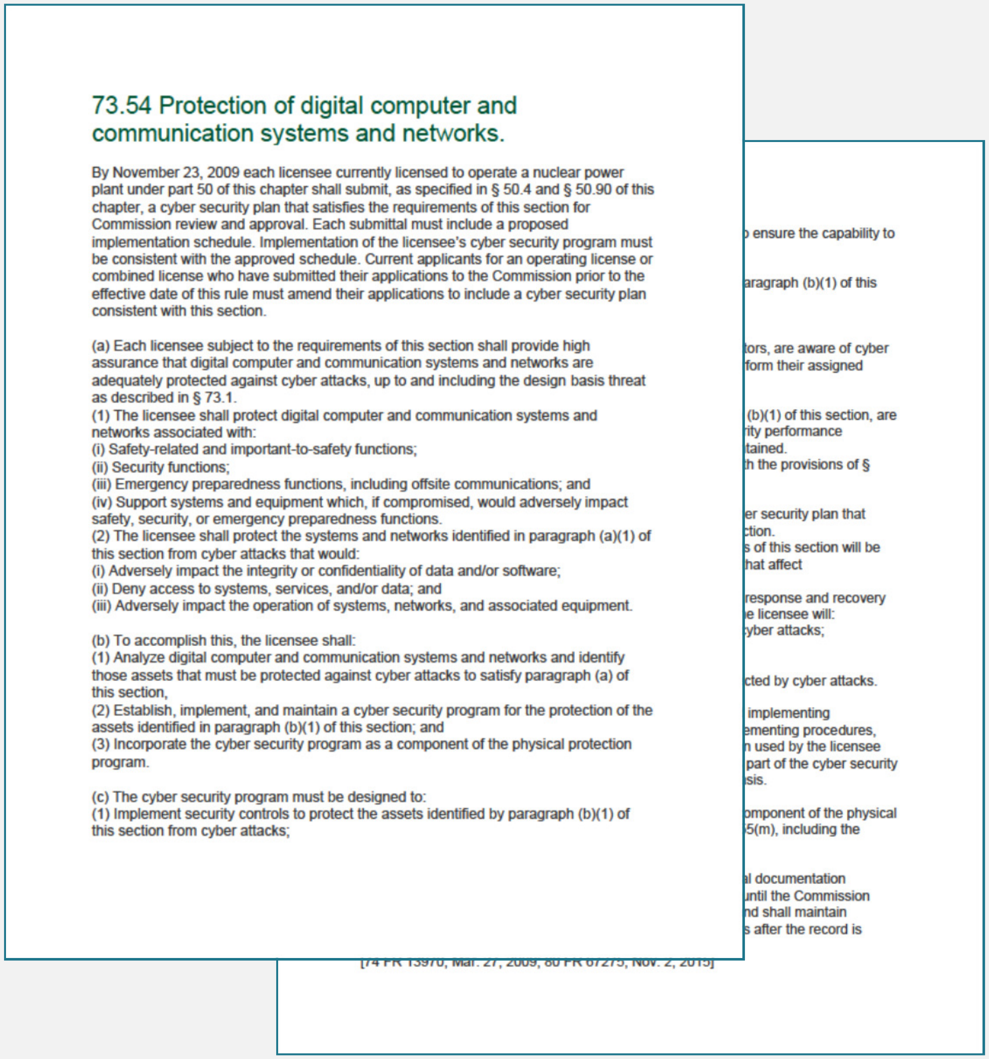
- Why is this important?
- Requirements and guidance
- Licensee programs
- Supply chain impact
- CNS CS Vendor Audits
- Questions

Why is this important?

- Security of critical infrastructure
  - Financial
  - Government operations
  - Basic community services
  - Power, gas, and water
  - Health care
  - Communications
- Recent examples
- Nuclear industry

Cyber Rule – 10 CFR 73.54

- Applicability:
  - Licensees
  - Digital computers, communication systems, and networks
  - Broader than safety-related
- Reporting
  - 10 CFR 73.77



73.54 Protection of digital computer and communication systems and networks.

By November 23, 2009 each licensee currently licensed to operate a nuclear power plant under part 50 of this chapter shall submit, as specified in § 50.4 and § 50.90 of this chapter, a cyber security plan that satisfies the requirements of this section for Commission review and approval. Each submittal must include a proposed implementation schedule. Implementation of the licensee's cyber security program must be consistent with the approved schedule. Current applicants for an operating license or combined license who have submitted their applications to the Commission prior to the effective date of this rule must amend their applications to include a cyber security plan consistent with this section.

(a) Each licensee subject to the requirements of this section shall provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in § 73.1.
(1) The licensee shall protect digital computer and communication systems and networks associated with:
(i) Safety-related and important-to-safety functions;
(ii) Security functions;
(iii) Emergency preparedness functions, including offsite communications; and
(iv) Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.
(2) The licensee shall protect the systems and networks identified in paragraph (a)(1) of this section from cyber attacks that would:
(i) Adversely impact the integrity or confidentiality of data and/or software;
(ii) Deny access to systems, services, and/or data; and
(iii) Adversely impact the operation of systems, networks, and associated equipment.

(b) To accomplish this, the licensee shall:
(1) Analyze digital computer and communication systems and networks and identify those assets that must be protected against cyber attacks to satisfy paragraph (a) of this section,
(2) Establish, implement, and maintain a cyber security program for the protection of the assets identified in paragraph (b)(1) of this section; and
(3) Incorporate the cyber security program as a component of the physical protection program.

(c) The cyber security program must be designed to:
(1) Implement security controls to protect the assets identified by paragraph (b)(1) of this section from cyber attacks;

o ensure the capability to

aragraph (b)(1) of this

tors, are aware of cyber
form their assigned

(b)(1) of this section, are
rity performance
tained.
h the provisions of §

er security plan that
ction.
s of this section will be
hat affect

response and recovery
e licensee will:
yber attacks;

cted by cyber attacks.

implementing
ementing procedures,
n used by the licensee
part of the cyber security
sis.

omponent of the physical
5(m), including the

l documentation
until the Commission
nd shall maintain
s after the record is

[74 FR 13970, Mar. 27, 2009; 80 FR 67275, Nov. 2, 2015]

NEI 08-09

- Available on the NRC website:
  - NEI 08-09, Rev. 6 (ML101180437 – April 2010)
  - Safety Evaluation (ML101190371 - May 5, 2010)
- Applicable to licensees (operating plants)
- Provides a template for a *Cyber Security Plan*
- *Cyber Security Plan* provides the licensing basis for the *Cyber Security Program*
- Based on NIST SP 800-82 and 800-53

NEI
NUCLEAR ENERGY INSTITUTE

Regulatory Guide 5.71

- Available on the NRC website:
  - RG 5.71, Rev. 0 (ML090340159 – January 2010)
- Applicable to new applications (including new plant builds)
- Also based on NIST SP 800-82 and 800-53
- Regulatory Guide 5.71 differences

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Update to RG 5.71

- https://www.nrc.gov/reading-rm/doc-collections/reg-guides/protection/rg/
  - Draft Guide 5061 – public comments soon
  - RG 5.71, Rev. 1 – update planned for late 2017
- Clarification of guidance
  - Supply chain emphasis area
- Lessons learned from NRC inspections
- Update with new regulation since 2010

Supply Chain Guidance

- RG 5.71, Rev. 0 – Appendix C.12.2
- NEI 08-09, Rev. 6 – Appendix E.11.2
  - Trusted distribution paths
  - Validation of vendors
  - Tamper proof / evident seals on products
  - Analysis of each acquisition that meets technical, operational, and management controls (RG only)
  - Heterogeneity to mitigate sole source (RG only)

Current Licensee Programs

- Milestones:
  - Cyber Security Assessment Team (CSAT)
  - Critical systems (CSs) and critical digital assets (CDAs)
  - Protective devices
  - Access control
  - Tampering prevention
  - Implement controls
  - Monitoring and assessment
  - Full cyber program implementation

2017

Supplier Applicability

- It’s all about the PO!
- Must affect Safety, Security, and Emergency Preparedness (SSEP)
- Component / system must have digital content
- Critical Digital Asset (CDA): *Subcomponent of a critical system affecting SSEP functions that contains a digital device, computer or communication system or network*

Impacted Scope of Supply

- Potentially LARGE scope:
  - Safety-related equipment
  - Important to safety (augmented quality) equipment
  - Equipment performing security functions
  - Equipment performing emergency preparedness functions (including offsite communications)
  - Related support systems and equipment
  - Equipment providing pathways to related equipment
  - Cyber security protection equipment

Accepting Purchase Orders

- Cyber discussion / program evaluation <u>might not</u> occur prior to licensee PO
- Avoid vague requirements or imposed regulations
- Take exceptions to elements of PO (if needed)
- Establish and implement actions prior to work
- Expect to issue a Certificate of Compliance
- Expect to be audited and inspected

Vendor QA Controls

- Supplier controls will vary based on component
- Leverage use of Criterion III, “Design Control”
- Apply other criteria, as needed:
  - Typical – training, CAP/NCR, records, audits
  - Potentially – procurement, testing, inspection, organization

Cooper Nuclear Station's Cyber Security Audits

- Why Cyber Security Audits?
- Audit Scope
- Pilot Audit Results

Why Cyber Security Audits

- Cyber Security Plan
  - Commitment Date (One of the first)
- NEI 08-09 Appendices E
- System and service Acquisition

Why Cyber Security Audits

- System and service Acquisition
  - Protection against supply chain threats and maintenance of integrity of CDAs that are **acquired**
  - Ensuring that CDAs meet defined levels of trustworthiness and that **software developers** use software quality and validation method to minimize flaws or malformed software

Why Cyber Security Audits

- Ensure that **new acquisitions** implement controls based on evolving CS threats and vulnerabilities, advancements in CS protective strategies and security controls, and the effects advancements could have on CDAs and networks

- Controls for **system developers/ integrators** of acquired CDAs to create a test and evaluation plan, implement the plan, and document the results

Why Cyber Security Audits

- Verification that CS requirements are being met
- Reduce Testing and Evaluation
  - Multiple products from a single vendor

Audit Scope

- Developed with Information Technology, Quality Assurance, Engineering
- Audited Areas
  - Physical Security
  - Trustworthiness
  - Supply Chain
  - Product Testing
  - Shipping and Handling
  - Design Control
- Suppliers of Direct CDAs

Direct vs. Indirect

- Direct:

  If compromised, could result in an **immediate** adverse impact to SSEP (Safety, Security and Emergency Preparedness) functions or systems, or equipment that are used or relied on for performing SSEP functions or for making SSEP-related decisions.

Direct vs. Indirect

- Direct:
  - CDAs associated with support systems and equipment that, if compromised, could adversely impact systems or equipment that are used for performing SSEP (Safety, Security and Emergency Preparedness) functions, or relied-on for making SSEP-related decisions
  - Not been determined to be indirect or EP-Only CDAs.

Direct vs. Indirect

- Indirect:

  Cannot have a near-term impact on, or degrade SSEP functions **prior to their compromise or failure being detected and compensatory measures being implemented.**

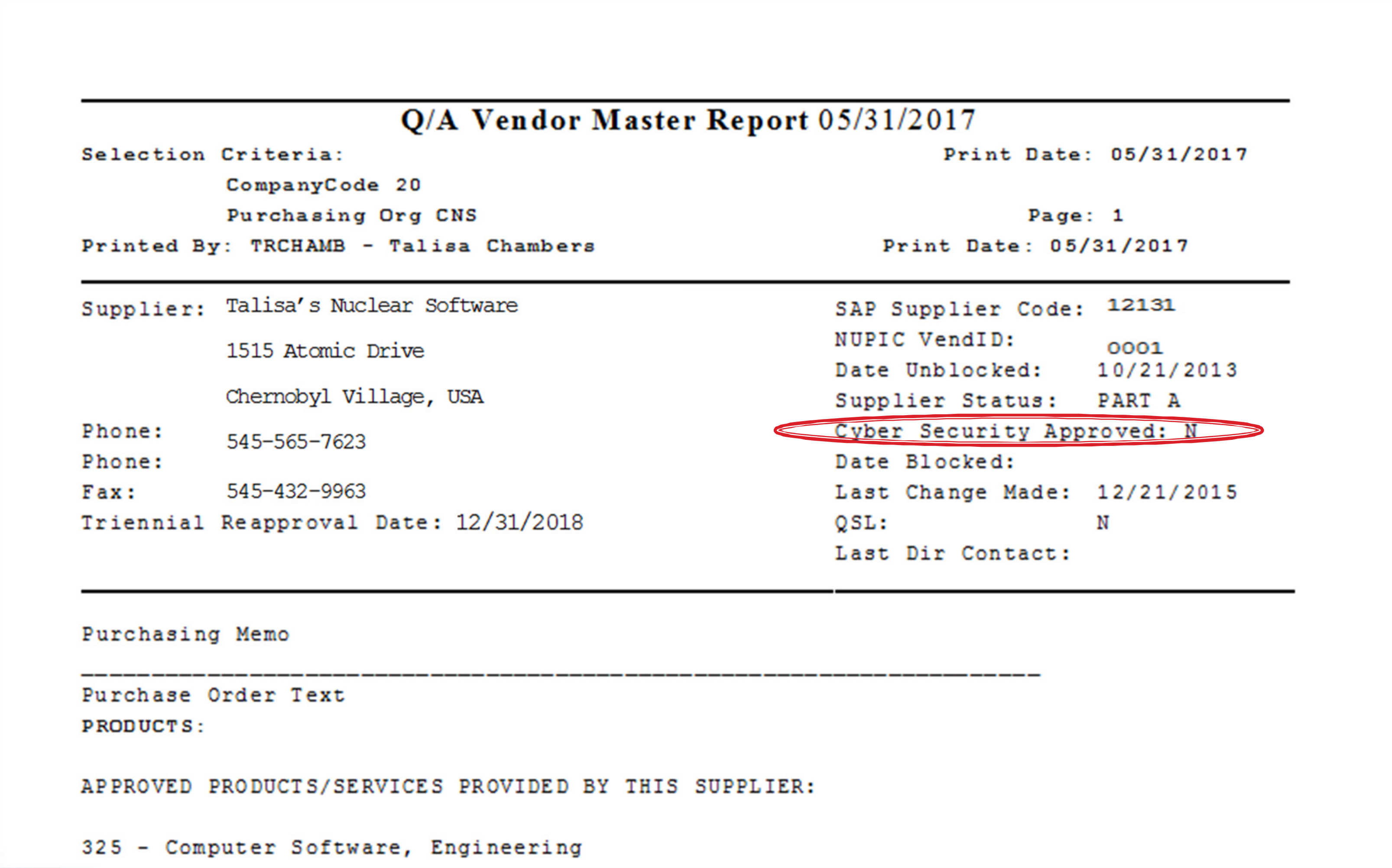
Direct vs. Indirect

- Indirect:
  - If compromised, would <u>not</u> have a direct impact on systems and equipment that perform safety or security functions;
  - Are not indicators/annunciators solely relied on for making safety or security-related decisions; and
  - The compromise of which can be detected and compensatory measures taken prior to an adverse impact to direct CDAs or safety or security functions.

Pilot Audit Results

- Performed by our Vendor Audit Group (not a NUPIC Audit) with IT support
- Audit found:
  - Documented Controls not in place
  - Sub-supplier Controls were not in place
  - Physical Security Controls were adequate
- Results are to be evaluated by IT and QA
- Approved Supplier's List

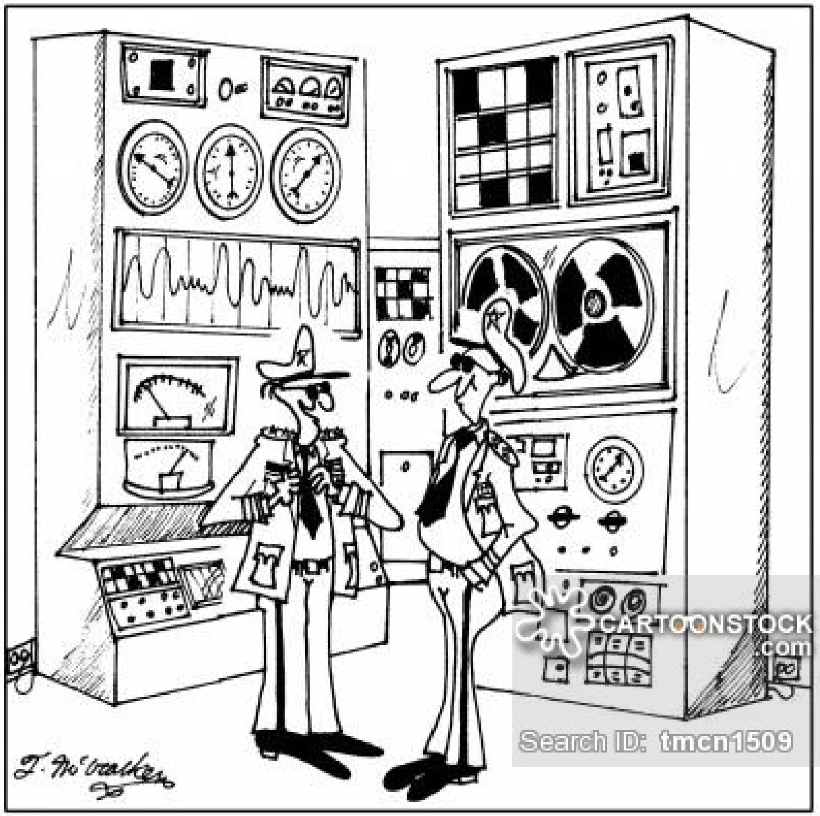
Approved Suppliers List



```
                    Q/A Vendor Master Report 05/31/2017
Selection Criteria:                                    Print Date: 05/31/2017
          CompanyCode 20
          Purchasing Org CNS                                 Page: 1
Printed By: TRCHAMB - Talisa Chambers              Print Date: 05/31/2017

Supplier: Talisa's Nuclear Software              SAP Supplier Code: 12131
                                                 NUPIC VendID:       0001
          1515 Atomic Drive                      Date Unblocked:    10/21/2013
                                                 Supplier Status:   PART A
          Chernobyl Village, USA                 Cyber Security Approved: N
Phone:    545-565-7623                           Date Blocked:
Phone:                                           Last Change Made:  12/21/2015
Fax:      545-432-9963                           QSL:               N
Triennial Reapproval Date: 12/31/2018            Last Dir Contact:

Purchasing Memo
_____________________________________________________________________
Purchase Order Text
PRODUCTS:

APPROVED PRODUCTS/SERVICES PROVIDED BY THIS SUPPLIER:

325 - Computer Software, Engineering
```

Conclusion

- Why is this important?
- Requirements and guidance
- Licensee programs
- Supply chain impact
- CNS CS Vendor Audits
- Questions



"It's a foolproof computer network, sir,
that no one can break into, not even a kid."

Questions?

Nebraska Public Power District

"Always there when you need us"

trchamb@nppd.com
(402) 825-5377

GLipscomb@goldwingservices.com
(919) 454-5299