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

Regulatory Guidance (RG 5.83) Cyber Security Event Notifications

February 11, 2015

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

Meeting Ground Rules

- Limit interruptions:
  - Turn off cell phones
  - Minimize side conversations
- Speak one at a time.
- Identify yourself when speaking
  - Please state your name, organization, and your comment or question.
  - If you are in the meeting room please use the microphone.
- Be respectful of other speakers/participants.
- If participating by webinar please use the:
  - Chat function to send questions or
  - Ask questions via the bridgeline at the designated opportunities.
  - Please mute your phone (*6)

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

Purpose

- Discuss Draft Final Regulatory Guide 5.83, "Cyber Security Event Notifications"

- No regulatory decisions will be made today

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

Meeting Agenda

- 8:00am – 8:15am: Welcome/Introductions
- 8:15am – 8:45am: NRC presentation of Regulatory Guide 5.83 for Cyber Security Event Notifications
- 8:45am – 9:45am: NRC/public discussion of Regulatory Guide 5.83 for Cyber Security Event Notifications
- 9:45am – 10:00am: Closing Remarks

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

Attendance and Feedback

- Personnel in attendance, sign-in before leaving today
- Feedback can be submitted by e-mail to Brad.Bergemann@nrc.gov
- Written feedback will be included as an attachment to the meeting minutes, which will be posted on www.regulations.gov

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

Regulatory Guide 5.83 Background

- The NRC published Draft Regulatory Guide (DG-5019), Reporting and Recording Safeguards Events as part of the enhanced weapons proposed rule package in February, 2011.
  - DG-5019 included cyber security events
- In January, 2014, the Commission bifurcated the Cyber Security Event Notification (CSEN) requirements from the enhanced weapons rule to speed up the issuance of the CSEN final rule.
  - With the bifurcation a separate regulatory guide (RG 5.83) was created for cyber security event notifications.
- All documentation related to the CSEN rulemaking to include the guidance can be reviewed on the regulations.gov website by searching for the NRC Docket ID "**NRC-2014-0036**".

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

Next Steps

- The next steps will be:
  - The NRC staff will review the feedback from the February 11, 2015, public meeting.
  - The NRC staff expects to issue the final CSEN rule in the first quarter of 2015.
- RG 5.83 will be issued at the same time as the final rule.

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

Draft Regulatory Guide 5.83 Outline

- One-hour notifications
- Four-hour notifications
- Eight-hour notifications
- 24-hour recordable events
- Notification Process
- Written Security Follow-up Reports

One-hour notification

- (a)(1) After discovery of a cyber attack that adversely impacted safety-related or important-to–safety functions, security functions, or emergency preparedness functions (including offsite communications); or that compromised support systems and equipment resulting in adverse impacts to safety, security, or emergency preparedness functions within the scope of 10 CFR 73.54.

One-hour Examples

- A cyber attack that adversely impacted:
  - The normal operation of the facility through the unauthorized use of, or tampering with, digital computer and communication systems and networks that fall within the scope of 10 CFR 73.54.
  - The capability to shut down the reactor and maintain it in a safe shutdown condition, remove residual heat, control the release of radioactive material or mitigate the consequences of an accident, even if the affected system was not required to perform its function during the period of impact.
  - The capability to delay, detect, assess, or respond to malevolent activities.
    - For example, a cyber attack that disrupts a security function responsible for the implementation of the site's physical protection program and/or protective strategy such as, an intrusion detection and assessment system, a physical barrier (e.g., active vehicle barrier, delay barrier), an access control system, an alarm station, a communication system.
  - The capability to call for, or communicate with, offsite assistance.
  - Emergency response capabilities to implement appropriate protective measures in the event of a radiological emergency.
  - A support system that falls within the scope of 10 CFR 73.54, even if the affected system was not required to perform its function during the period of impact.

Four-hour Notifications

- (a)(2)(i) After discovery of a cyber attack that could have caused an adverse impact to safety-related or important-to–safety functions, security functions, or emergency preparedness functions (including offsite communications); or that could have compromised support systems and equipment, which if compromised, could have adversely impacted safety, security, or emergency preparedness functions within the scope of 10 CFR 73.54.

- (a)(2)(ii) After discovery of a suspected or actual cyber attack initiated by personnel with physical or electronic access to digital computer and communication systems and networks within the scope of 10 CFR 73.54.

- (a)(2)(iii) After notification of a local, State, or other Federal agency (e.g., law enforcement, Federal Bureau of Investigation) of an event related to the licensee's implementation of their cyber security program for digital computer and communication systems and networks within the scope of 10 CFR 73.54.

Four-hour Examples

- A cyber security event that resulted in unauthorized access to a CDAs and/or CSs services, resources or information. For example, a CDA that was isolated or on a protected network was found connected to an unprotected network (wired or wireless) and cyber security controls (e.g., activity logs, antivirus protection, intrusion detection, etc.) indicates the presence of malware or unauthorized activity had occurred.

- An unauthorized transmitter (e.g., wireless router, modem) or unauthorized portable media (e.g., memory stick, smart phone) was attached or connected to a CDA, and cyber security controls (e.g., activity logs, antivirus protection, intrusion detection, etc.) indicates the presence of malware or unauthorized activity had occurred.

- The degradation or failure of a CDA or of the cyber security controls that protect CDAs that is indicative of unauthorized activity (e.g., cyber attack, physical tampering), and does not have an immediate or adverse impact on SSEP functions. For example, the CDA has an analog back-up. This does not include mechanical or electrical failures or degradations resulting from normal operations.

- An active cyber attack, (e.g., virus, or worm logic bomb) that, if cyber security controls were not in place, could have adversely impacted a SSEP function.

- A cyber attack that caused an adverse impact to a CDAs and/or CSs confidentiality, integrity or availability, but no SSEP functions have been adversely affected. For example, if a remote digital control to an active vehicle barrier has been disabled (e.g., loss of communications), but the barrier is in the denial position and has not and will not allow unauthorized access as a result of the cyber attack.

- Control of a mobile or portable CDA is lost or misplaced and signs of exploitation have occurred (e.g., activity logs, antivirus protection, intrusion detection, etc.). For example, a CDA used for maintenance and testing is misplaced or lost, if the CDA is recovered and shows signs of tampering (e.g., physical or malware installed, etc.) or CDAs that are maintained and tested by the lost or misplaced CDA show sign of exploitation (malware, misconfiguration, etc.).

Eight-hour Notification

- (a)(3) After receipt or collection of information regarding observed behavior, activities, or statements that may indicate intelligence gathering or pre-operational planning related to a cyber attack against digital computer, and communication systems and networks that fall within the scope of 10 CFR 73.54.

Eight-hour Examples

- Personnel or persons with an uncommon level of interest or making abnormal inquiries related to specific attributes of the licensee's cyber security program (e.g., CDAs, CSs, cyber security controls) or vulnerabilities associated with the cyber security program. Such interests or inquiries could occur onsite or offsite (e.g., cyber security symposium) by personnel, vendors, contractors or non-employees that do not have a need-to-know (e.g., are not part of, or support, the licensee's cyber security program). This does not include generic public or media inquiries related to plant operations, safety, etc.

- Unauthorized personnel in a static position in vicinity of the plant (protected area) that are in possession and operating equipment (e.g., a laptop or a Yagi antenna) capable of scanning for wireless networks. This does not include devices such as personal electronic devices (e.g., smartphones) carried by visitors that are configured to search or join wireless networks.

- Theft or suspicious loss of smart cards, tokens, or other "two factor" authentication devices required for accessing a CDA or CS.

- Forgery or fabrication of smart cards, tokens or other "two factor" authentication devices required for accessing a CDA/CS or performing authorization activities.

- Falsification of identification badges, key cards, or other access-control devices that could allow unauthorized individuals access to a CDA or CS.

- The recognition of a structured or sophisticated cyber attack or attacks that has not yet reached a CDA, CS or protected network but could represent a threat to the plant's cyber security or response capabilities (e.g., attempts to defeat or circumvent the cyber security controls). A structured attack may involve repeated attempts from the same source, or a large increase in number of attacks. A sophisticated attack may involve the use of social engineering techniques or attacks that evolve based on the controls or response actions encountered (e.g., a phishing attack followed-up with a telephone call using social engineering techniques to trigger the phishing attack).

- A website posting or notification indicating a planned cyber attack against the plant.

24-hour Recordable

- (b)(1) Licensees shall use their site CAP to record vulnerabilities, weaknesses, failures and deficiencies in their 10 CFR 73.54 cyber security program within 24-hours of discovery.
- (b)(2) Licensees shall use their site CAP to record notifications made under paragraph (a) of 10 CFR 73.77 within twenty-four hours of their discovery.

24-hour Recordable Examples

- A cyber vulnerability assessment that was not performed within the period specified in the licensee's Cyber Security Plan (e.g., quarterly).

- Improper use of digital computer and communication systems and networks associated with SSEP functions; or support systems and equipment, which if compromised, could adversely impact SSEP functions. This could include training and procedure deficiencies involving a CDA, cyber security controls or SSEP functions without an adverse impact to their function (e.g., connection of unauthorized portable media to a CDA which resulted in no unauthorized activity or malware).

- A design flaw or vulnerability in an implemented cyber security control that could have allowed unauthorized access to a CDA, or substantively eliminated or significantly reduced the licensee's response capabilities. This is not intended to capture vendor discovered issues that are immediately fixed/patched/corrected. However, flaws or vulnerabilities discovered by a licensee should be recorded (e.g., a licensee scan discovers a vulnerability in cyber security hardware or software that has not been previously identified). Note: If a licensee believes the vulnerability or design flaw could pose an industry-wide risk the licensee should consider immediate notification using the voluntary notification process so the NRC can notify other licensees of the vulnerability or design flaw.

- A cyber security event that could have allowed undetected or unauthorized access or modification to a CDA, but was not exploited in an attack. For example, a cyber security control or alarm was temporarily disabled or accessed for maintenance and not enabled or secured immediately upon completion of the activity.

Notification Process

- To the NRC Headquarters Operations Center via the ENS

- Content of notification (if available at the time of the notification):
  - caller name and callback number
  - facility name and location
  - emergency classification (if declared)
  - current event status (e.g., in progress, recovered, unknown)
  - event date and time (discovery of, and actual occurrence if known)
  - event description including the following information if available or known:
    - cyber security controls involved/affected (if any)
    - system(s) involved/affected (SSEP functions, BOP functions, CDAs, CS)
    - method used to identify the event (e.g., security controls, audit, failed equipment)
  - what occurred during the event
  - why the event occurred, if known
  - how the event occurred, if known
  - safety, security, EP responses and corrective actions taken
  - offsite assistance (e.g., requested or not requested, arrived, status)
  - media interest, if any, including licensee issued press releases
  - source of information (e.g., U.S. Computer Emergency Readiness Team, law enforcement)

Written Follow-up Reports

- Submission within 60-days of the telephonic notification.
- Required for paragraphs (a)(1), (a)(2)(i) and (a)(2)(ii).
- Content of written report:
  - date and time of the event, including chronological timeline, if applicable
  - date and time of notification to the NRC, and/or local, State and Federal agencies
  - the reactor's operating mode at time of event (e.g., shut down, operating)
  - SSEP functions directly or indirectly affected by the event (e.g., compromised, failed, degraded)
  - support systems or equipment directly or indirectly affected that could have compromised SSEP functions (e.g., compromised, failed, degraded)
  - CDAs and/or CS affected by the event (compromised, failed, degraded)
  - security controls involved in the event (e.g., compromised, performed as intended)
  - personnel involved or contacted, such as contractors; security personnel; visitors; plant staff; perpetrators or attackers; NRC personnel; local, State, or Federal responders; and other personnel (specify)
  - method of discovery of the event, or information, such as routine patrol or inspection, test, maintenance, alarm annunciation, audit, communicated threat, unusual circumstances (include details)

Content of Written Report Continued…

- immediate actions taken in response to the event and any compensatory measures established
- description of media interest and press releases
- indications or records of previous similar events
- procedural or human errors or equipment failures, as applicable
- cause of the event, or the licensee's analysis of the event (including a brief summary in the report and references to any ongoing or completed detailed investigations, assessments, analyses, or evaluations)
- corrective actions taken or planned, including dates of completion
- name and phone number of a licensee's point of contact
- for failures, degradations, or discovered vulnerabilities of the cyber security program, licensees should also provide the following information, in addition to items a. through p. above:
  - description of failed, degraded, or vulnerable equipment, systems or controls (e.g., manufacturer and model number, procedure number)
  - unusual conditions that may have contributed to the failures, degradations, or discovered vulnerabilities of the equipment, systems or controls (e.g., environmental conditions, plant outage, software update)
  - security settings/configuration of the components, systems or controls that failed, or became degraded or vulnerable
  - apparent cause of component, system or control failure, degradation, or vulnerability

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

Questions and Discussion

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

Draft Regulatory Guide 5.83

Closing Remarks

Brad.Bergemann@nrc.gov
301-287-3797