NEI 15-09 [Revision 0]

# Cyber Security Event Notifications

February 2016

[BLANK PAGE]

NEI 15-09 [Revision 0]

# Nuclear Energy Institute

# Cyber Security Event Notifications

February 2016

*Nuclear Energy Institute, 1201 F Street, NW, Suite 1100, Washington D.C. (202.739.8000)*

# ACKNOWLEDGMENTS

The Nuclear Energy Institute (NEI) appreciates the efforts of the following industry personnel in preparation of NEI 15-09.

- Matt Coulter, Duke Energy Corporation
- Nathan Faith, Exelon Corporation
- Adam Goodman, Duke Energy Corporation
- William Gross, Nuclear Energy Institute
- David Neff, Exelon Corporation
- Heather Pickard, Tennessee Valley Authority
- Jay Phelps, STP Nuclear Operating Company
- Robin Ritzman, First Energy Corporation
- Larry Tremonti, DTE Energy

# NOTICE

# EXECUTIVE SUMMARY

This document provides guidance for use by nuclear power reactor licensees when categorizing certain cyber security events, and the process for conducting notifications and submitting written security follow-up reports to the NRC for cyber security events. Regulatory Guide 5.83 (RG 5.83) uses a definition of Cyber Attack that is different than the definition approved by the NRC for use in the industry Cyber Security Plans. Consequently the terms and examples in RG 5.83 are different than those provided in NEI 15-09. This document is based on Regulatory Guide 5.83, rev 0 with incorporation of 1) NEI definition of cyber attack affecting the examples, 2) flowchart for reportability determinations, 3) guidance for determining when the reportability clock starts, 4) guidance for evaluating conditions that 'could have caused an adverse impact, 5) examples for use in program implementation and training, and 6) a Glossary of terms.

This guidance document was developed to streamline the process for making reportability determinations. The goal is to provide for consistent implementation and to minimize the burden on licensees and the NRC from over reporting events that do not rise to the level of an actual or potential cyber attack, while enabling NRC to inform the U.S. Department of Homeland Security (DHS) and federal intelligence and law enforcement agencies of cyber security-related events that could (1) endanger public health and safety or the common defense and security, (2) provide information for threat-assessment processes, or (3) generate public or media inquiries.

[BLANK PAGE]

# TABLE OF CONTENTS

[BLANK PAGE]

# CYBER SECURITY EVENT NOTIFICATIONS

## 1 INTRODUCTION

This new guide addresses cyber security event notification requirements. These notification requirements contribute to the NRC's analysis of the reliability and effectiveness of licensees' cyber security programs. Furthermore, they will play an important role in the NRC's continuing effort to provide high assurance that digital computer communication systems and networks are adequately protected against cyber attacks up to and including the design basis threat.

Prompt notification of a cyber attack could be vital to the NRC's ability to take immediate action in response to a cyber attack and, if necessary, notify other NRC licensees, Government agencies and critical infrastructure facilities, to defend against a multiple sector cyber attack. Notifications conducted and written reports submitted by licensees will be used by the NRC to respond to emergencies, monitor ongoing events, assess trends and patterns and identify precursors of more significant events. Timely notifications assist the NRC in achieving its strategic communication mission by enabling NRC to inform the U.S. Department of Homeland Security (DHS) and federal intelligence and law enforcement agencies of cyber security-related events that could (1) endanger public health and safety or the common defense and security, (2) provide information for threat-assessment processes, or (3) generate public or media inquiries.

In accordance with 10 CFR 73.54, licensees' cyber security programs are required to 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 of radiological sabotage as described in 10 CFR 73.1. Further, licensees are required to protect digital computer and communication systems and networks associated with safety-related and important-to-safety functions; security functions; emergency preparedness functions, including offsite communications; and support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness (SSEP) functions.

Additionally, in accordance with 10 CFR 73.54(a)(2) licensees are required to protect the systems and networks associated with SSEP functions against cyber attacks that would adversely impact the integrity or confidentiality of data and/or software; deny access to systems, services, and/or data; and adversely impact the operation of systems, networks, and associated equipment. Furthermore, in staff requirements memorandum (SRM), "COMWCO-10-0001 Regulation of Cyber Security at Nuclear Power Plants" (Ref. 5), the Commission determined that, as a matter of policy, 10 CFR 73.54 should be interpreted to include structures, systems and components (SSC) in the balance of plant (BOP) that have a nexus to radiological health and safety at NRC-licensed nuclear power plants. Therefore, cyber security events related to BOP SSCs that could directly or indirectly affect reactivity of a nuclear power plant are also required to be reported or recorded in accordance with the requirements of 10 CFR 73.77.

The NRC has established notification requirements for certain cyber security activities because they may be indicative of preoperational malevolent activities, and malevolent actors have demonstrated the capability to simultaneously attack multiple independent targets. The NRC forwards appropriate reports of these cyber security activities to DHS, federal law enforcement agencies and the intelligence community as part of the national threat assessment process as outlined in the National Cyber Incident Response Plan. Analysis of individual cyber security events (at separate facilities or activities) may reveal to the NRC, law enforcement authorities, or the intelligence community potential threats or patterns that warrant increasing the security posture for NRC-regulated facilities and activities, other government facilities and activities, and other national critical-infrastructure facilities. The DHS considers licensees to be "key resource owners and operators." Licensees can find additional guidance and examples of suspicious events (to include events related to cyber activity) in the U.S. Department of Homeland Security's, "Terrorist Threats to the U.S. Homeland: Reporting Guide for Critical Infrastructure and Key Resource Owners and Operators."

Consistent with 10 CFR 73.77, a cyber security event must be reported within the time specified in 10 CFR 73.77(a). These timeframes are within specified hours after, for example, discovery of a cyber attack or suspected attack. Refer to APPENDIX B-GUIDANCE FOR DETERMINING START OF REPORTABILITY CLOCK for guidance for cyber incident investigations and determining when sufficient information exists for making a reportability determination.

This guidance has been developed based on examples taken from prior experience with cyber security events and interactions between NRC staff and licensees. This guide is intended to provide assistance to licensees in evaluating whether a broad range of potential cyber security events should be reported or recorded under the provisions of 10 CFR 73.77. The specific cyber security events listed in this guide are examples of reportable or recordable cyber security events using the definition of Cyber Attack that is provided in NEI 08-09 rev 6 as amended by the NRC in letter dated June 6, 2010 (Reference 11). As such, these lists are not exhaustive or exclusive. Many of the examples listed herein have been created from actual cyber security events at NRC-regulated facilities or from licensee discussions with NRC staff on whether a particular cyber security event was reportable, recordable, or neither. The evaluation of cyber security events is very fact specific. Therefore, for virtually every example provided, the addition or subtraction of a single aspect not explicitly detailed in this guide could easily move it into a higher or lower reporting timeframe. Accordingly, licensees should always consider their particular circumstances before determining how to comply with 10 CFR 73.77.

Licensees should report suspected or actual cyber security events, including those substantiated by observations by staff or law enforcement personnel, evidence of the presence of unknown personnel, unauthorized access or modification of critical digital assets (CDAs), telephone and other electronic contacts, suspicious documents and files, and testimony of credible witnesses. Licensee's corporate and contractor personnel may also be sources of this information. Licensees should consider obtaining access to the NRC's Protected Web Server (PWS) to obtain routine threat bulletins and analyses the

NRC receives from the Federal Bureau of Investigation (FBI) and the DHS on critical national infrastructure and key resources. Licensees desiring access to the NRC's PWS should make their request through the security staff in their applicable NRC regional office.

Notifications conducted under 10 CFR 73.77 should focus on the occurring or suspected cyber security event, not the resolution, final analysis, suspected motivation of any participants, or technical evaluations. While those actions should be considered part of the response function and should eventually be reported, they should not affect the timely notification of the occurring event.

## 1.1 SCOPE

This document provides guidance licensees may use to create procedures and training documents for addressing the reporting requirements of 10CFR73.77, Cyber Security Event Notifications.

## 1.2 PURPOSE

The purpose of this document is to provide guidance for use by nuclear power reactor licensees when categorizing certain cyber security events, and the process for conducting notifications and submitting written security follow-up reports to the NRC for cyber security events. RG 5.83 uses a definition of Cyber Attack that is different than the definition approved by the NRC for use in the industry Cyber Security Plans. Consequently the terms and examples in RG 5.83 are different than those provided in NEI 15-09.

## 1.3 APPLICABLE RULES AND REGULATIONS

The regulations in Title 10, of the *Code of Federal Regulations* (10 CFR), "Physical Protection of Plants and Materials," Part 73, (Ref. 1). Section 73.77, "Cyber Security Event Notifications" requires licensees subject to the provisions of 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks" to notify the NRC Headquarters Operations Center via the Emergency Notification System (ENS) as described below.

- Section 73.77(a)(1) requires licensees to notify the NRC within one hour 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.

- Section 73.77(a)(2) requires licensees to notify the NRC within four hours:

  (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.

(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.

(iii) After notification of a local, State, or other Federal agency of an event related to implementation of the licensee's cyber security program for digital computer and communication systems and networks within the scope of 10 CFR 73.54 that does not otherwise meet a notification under 10 CFR 73.77(a).

- Section 73.77(a)(3) requires licensees to notify the NRC within eight hours 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 within the scope of 10 CFR 73.54.

- Section 73.77(b) requires licensees to use their site corrective action program (CAP) to record vulnerabilities, weaknesses, failures and deficiencies in their cyber security program as well as record notifications made under paragraph (a) of 10 CFR 73.77 within twenty four hours of their discovery.

- Section 73.77(c) provides the process for conducting cyber security event notifications to the NRC.

- Section 73.77(d) provides the process for submitting written security follow-up reports to the NRC for cyber security event notifications.

- Section 73.77(d)(3) requires licensees to prepare written security follow-up reports on NRC Form 366.

- Appendix A to 10 CFR Part 73, "U.S. Nuclear Regulatory Commission Offices and Classified Mailing Addresses," contains contact information for the NRC Headquarters Operations Center and directions on communicating classified events to the NRC.

## 1.4 RELATED GUIDANCE

- Regulatory Guide 5.69, "Guidance for the Application of Radiological Sabotage Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements" (SGI) provides background on cyber attacks, up to and including the design basis threat (DBT) of radiological sabotage as described in 10 CFR 73.1 (Ref. 3).

- Regulatory Guide 5.83, "Cyber Security Event Notifications," provides NRC

guidance for use by nuclear power reactor licensees when categorizing certain cyber security events, and the process for conducting notifications and submitting written security follow-up reports to the NRC for cyber security events. RG 5.83 uses a definition of Cyber Attack that is different than the definition approved by the NRC for use in the industry Cyber Security Plans. Consequently the terms and examples in RG 5.83 are different than those provided in NEI 15-09.

- U.S. Department of Homeland Security, "Terrorist Threats to the U.S. Homeland: Reporting Guide for Critical Infrastructure and Key Resource Owners and Operators," (OUO) provides additional guidance and examples of suspicious events (including events related to cyber activity) (Ref. 4).

# 2 REGULATORY GUIDANCE

## 2.1 CYBER SECURITY EVENT NOTIFICATIONS

Licensees subject to the provisions of 10 CFR 73.54 are required to notify the NRC Headquarters Operations Center of the below events via the ENS in accordance with the requirements of 10 CFR 73.77(c).

### 2.1.1 One-hour Notifications

As stated in 10 CFR 73.77(a)(1) licensees are required to notify the NRC within one hour 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. Cyber Security incidents evaluated for reportability for one-hour notifications under 10 CFR 73.77(a)(1) should also be evaluated, by the appropriate departments, for reportability under 10 CFR 73.71(a) and for entry into the station's Emergency Plan.

Licensees should evaluate events that are not reportable under this requirement for reporting or recording under the other provisions of 10 CFR 73.77.

<u>One-hour Notification Examples</u>

1.a. A cyber attack that adversely impacted (e.g., interruption) the normal operation of the facility through the unauthorized use of, or tampering with, digital computer and communication systems and networks.

1.b. A cyber attack that adversely impacted 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.

1.c. A cyber attack that adversely impacted the capability to detect, delay, assess, or respond to malevolent activities. For example, a cyber incident involving an intentional act resulting in an adverse impact on a CDA 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, or a communication system.

1.d. A cyber attack that adversely impacted the capability to call for, or communicate with, offsite assistance.

1.e. A cyber attack that adversely impacted emergency response capabilities to implement appropriate protective measures in the event of a radiological emergency.

1.f. A cyber attack that adversely impacted 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.

### 2.1.2 Four-hour Notifications

As stated in 10 CFR 73.77(a)(2)(i) licensees are required to notify the NRC within four hours 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 § 73.54. These could be attacks that exploit a CDA, critical system (CS) or a protected network (i.e., a network that is isolated (air gapped) or behind a data diode that contains one or more CDAs), that could have but did not cause an adverse impact to SSEP functions. Only one (1) plausible assumption needs to be considered when evaluating if the cyber attack could have caused an adverse impact (Refer to APPENDIX C, EXAMPLES FOR IMPLEMENTATION AND TRAINING USE, examples involving 'could have caused'). For example, activity logs, antivirus protection or an intrusion detection system indicated the presence of malware or unauthorized access/activity occurred on a CDA, CS or protected network. For cyber attacks that reach unprotected networks (i.e., not isolated or behind a data diode containing CDAs), or that are mitigated by boundary and/or CDA cyber security controls and no exploitation of a CDA occurs, notification to the NRC would not be needed under 10 CFR 73.77(a)(2)(i).

As stated in 10 CFR 73.77(a)(2)(ii) licensees are required to notify the NRC within four hours 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. These are attacks that are initiated by employees, contractors, or vendors that have physical or electronic access to a CDA, CS or a protected network. This could include corporate Information Technology (IT) personnel that may not have unescorted access to the plant, but do have electronic access to digital computer and communication systems and networks within the scope of 10 CFR 73.54. It could also include personnel that do have unescorted access to the plant, but may not have electronic access to digital computer and communication systems and networks within the scope of 10 CFR 73.54. These attacks should be reported within four hours regardless of their impact on SSEP functions.

As stated in 10 CFR 73.77(a)(2)(iii) licensees are required to notify the NRC within four hours 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 that does not otherwise require a notification under 10 CFR 73.77(a).

Licensees should evaluate events that are not reportable under this requirement for reporting or recording under the other provisions of 10 CFR 73.77.

Four-hour Notification Examples

4.a. A CDA that was isolated or on a protected network was found to be connected to an unprotected network (wired or wireless) and cyber security controls (e.g., activity logs, antivirus protection, an intrusion detection system, etc.) indicated the pathway had been exploited as evidenced by the presence of malware or unauthorized access/activity had occurred.

4.b. 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, an intrusion detection system, etc.) indicated the pathway had been exploited as evidenced by the presence of malware or unauthorized access/activity had occurred.

4.c. The degradation or failure of a CDA or of the cyber security controls that protect CDAs that is indicative of unauthorized and malicious activity (e.g., cyber attack, physical tampering), and could have but does not have an immediate or adverse impact on SSEP functions because, for example, the CDA has an analog backup. This does not include common degradations or failures such as mechanical or electrical.

4.d. A cyber attack, (e.g., virus or worm logic bomb initiated by an intentional and malicious act) on a CDA, CS or protected network, that could have, but did not cause an adverse impact to SSEP functions or that could have compromised support systems and equipment, which if compromised, could have adversely impacted SSEP functions.

4.e. A cyber attack that caused an adverse impact to a CDAs and/or CSs confidentiality, integrity or availability, could have but did not cause an adverse impact to SSEP functions or that could have compromised support systems and equipment, which if compromised, could have adversely impacted SSEP functions. For example, if a remote digital control to an active vehicle barrier has been disabled (e.g., loss of communications due to an intentional and malicious act), but the barrier is in the denial position and has not and will not allow unauthorized access as a result of the cyber attack.

4.f. Control of a mobile or portable media device (PMD) is lost or misplaced and there are signs of malicious exploitation. For example, a PMD used for maintenance and testing is misplaced or lost, if the PMD is recovered and shows signs of malicious tampering (e.g., physical tampering, malware installed, etc.) or

PMDs that are maintained and tested by the lost or misplaced PMD show signs of malicious exploitation (malware, unauthorized access/activity, etc.).

### 2.1.3 Eight-hour Notifications

As stated in 10 CFR 73.77(a)(3) licensees are required to notify the NRC within eight hours 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.

Generally, eight-hour notifications should include behavior, activities, or statements that are coordinated and/or targeted. Only information deemed to be credible by security should be considered for this reportability criterion.

Additionally, licensees should evaluate events that are not reportable under this requirement for reporting or recording under the other provisions of 10 CFR 73.77.

Eight-hour Notification Examples

8.a. 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, or 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. (i.e., these inquiries are targeted).

8.b. Unauthorized personnel in a static position in vicinity of the plant (protected area) that are in possession and operating equipment (e.g., laptop, 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 (i.e., these activities are targeted).

8.c. The recognition of the theft or suspicious loss of smart cards, tokens, or other "two factor" authentication devices required for accessing a CDA or CS.

8.d. The detection of forged or fabricated smart cards, tokens or other "two factor" authentication devices required for accessing a CDA/CS or performing authorization activities.

8.e. The detection of falsified identification badges, key cards, or other access-control devices that allow unauthorized individuals access to a CDA or CS.

8.f. A targeted spear phishing email (payload) followed-up with a telephone call to the targeted individual attempting to trigger the spear phishing email (social engineering) with intent to adversely impact an SSEP function. Investigation

reveals the attempt is credible and involves or has the potential to involve digital computer, computer communication system or network under the scope of the Cyber Security Rule.

8.g. The recognition of the exfiltration of data (intelligence gathering) from an unprotected network from an unknown source, in conjunction with malware (payload) that was surreptitiously delivered and executed by the unknown source without licensee knowledge.

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

## 2.2 24-HOUR RECORDABLE EVENTS

As stated in 10 CFR 73.77(b) licensees are required to use their site CAP to record vulnerabilities, weaknesses, failures and deficiencies in their 10 CFR 73.54 cyber security program as well as record notifications made under paragraph (a) of 10 CFR 73.77 within twenty-four hours of their discovery.

This includes items or events such as: (1) when a cyber security control for a system, component or program has been reduced to the degree that it is rendered ineffective for the intended purpose (e.g., cessation of proper functioning); (2) a defect in equipment, personnel, or procedure that degrades the function or performance of the cyber security program necessary to meet the requirements of 10 CFR 73.54; (3) a feature or attribute in a system's design, implementation, operation, or management that could render a CDA open to exploitation, or an SSEP function susceptible to adverse impact.

Licensees should utilize the site CAP to perform periodic evaluations to identify any noticeable trends and/or increases in failures and deficiencies in their cyber security program (e.g., equipment vulnerabilities and failures, procedural and/or training weaknesses and deficiencies) to assist in identifying and developing program improvements.

24-hour Recordable Event Examples

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

24.b. Improper usage 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 exploitation (e.g., no malware transferred, no unauthorized activity/access occurred).

24.c. 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.

24.d. 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.

## 2.3 NOTIFICATION PROCESS

As stated in 10 CFR 73.77(c), each licensee is required to make notifications required by 10 CFR 73.77(a) to the NRC Headquarters Operations Center via the ENS. If the ENS is inoperative or unavailable, the licensee shall make the notification via commercial telephone service or other dedicated telephonic system or any other methods that will ensure a report is received by the NRC Headquarters Operations Center within the specified timeframe. Commercial telephone numbers for the NRC Headquarters Operations Center are specified in appendix A to Part 73, "U.S. Nuclear Regulatory Commission Offices and Classified Mailing Addresses." Notifications can be annotated on an "Event Notification Worksheet" (NRC Form 361). Licensees may obtain an event number and time during notifications. If an LER is required, the licensee may include this information in the LER to provide a cross-reference to the notification, making the event easier to trace.

The individual responsible for conducting the notification should be properly trained and sufficiently knowledgeable of the event to report it correctly.

The NRC records all conversations with the NRC Operations Center. The recordings are saved for one month in case there is a public or private inquiry.

Additionally, if needed, licensees should conduct additional notifications describing substantive changes, additions, or modifications to the initial notification in a timely manner after taking immediate actions to protect the facility or stabilize operations, in accordance with emergency and contingency response procedures.

More than one event can be reported in a single ENS or LER if (1) the events are related (i.e., they have the same general cause or consequence) and (2) they occurred as a single activity over a reasonably short time (e.g., within four or eight hours for ENS notifications, or within 60 days for a LER). Generally, a LER is intended to address a specific event and unrelated events should not be reported in one LER. However, multiple notifications may be addressed in a single telephone call.

Discussion of an event requiring notification under 10 CFR 73.77 with the NRC staff (e.g., resident inspector) does not constitute the required notification to the NRC Headquarters Operations Center. Nor does identification or discovery of events by the NRC staff relieve a licensee from the requirements to notify the NRC Headquarters Operations Center within the timeframes specified in 10 CFR 73.77(a).

### 2.3.1 Notifications Containing Safeguards Information

Under 10 CFR 73.22(f)(3), licensees may make notifications of cyber security events specified in 10 CFR 73.77, which are considered to be extraordinary conditions, containing Safeguards Information to the NRC Headquarters Operations Center without using a secure communications system. Licensees should not delay notification of such events beyond one hour after discovery to wait for secure communications. However, if available, a licensee should use a secure communications system to make the notification and protect the Safeguards Information contained in the report from unintentional or inadvertent disclosure. Additionally, licensees should apply this exception to actual events only. As such, it should not be applied to simulated events communicated as part of a drill or exercise, or to routine events (e.g., the retraction of a previous security report as invalid).

### 2.3.2 Notifications Containing Classified Information

Licensees making notifications under 10 CFR 73.77 that contain classified National Security Information (NSI) or Restricted Data (RD) should notify the NRC Headquarters Operations Center using a secure communications system equivalent (at a minimum) to the classification level of the notification. Licensees making classified notifications should contact the NRC Headquarters Operations Center at the commercial telephone numbers specified in appendix A to Part 73 and request a number to a secure telephone. If the licensee's secure communications capability is unavailable (e.g., because of the nature of the event), the licensee should provide as much information to the NRC as is required by 10 CFR 73.77, without revealing or discussing any classified information. The licensee should also indicate to the NRC at the beginning of the notification that its secure communications capability is unavailable, in order to prevent the inadvertent disclosure of classified information.

If the nature of the cyber security event warrants, NRC Emergency Response Management may direct the licensee to use any available non-secure communications method to immediately communicate classified information to the NRC (regarding cyber security event notifications required by 10 CFR 73.77). If so directed, the licensee should provide the classified information to the NRC over the best available non-secure system (i.e., the NRC staff considers using an available non-secure land-line as preferable to using an available non-secure cellular or satellite system).

In the written security follow-up report for the classified cyber security event notification over non-secure communications, the licensee should document the direction given by the NRC, the reason for the unavailability of a secure communications capability, and the specific classified information that was communicated to or from the NRC over the non-

secure communications. The written security follow-up report should be appropriately marked and classified by the licensee. The NRC will use the information in the written security follow-up report to assess the level of impact of the compromise of classified information communicated by the licensee, or the NRC over non-secure communications, in accordance with Executive Order 13526, "Classified National Security Information" (Ref. 6).

### 2.3.3 Continuous Communications

For some cyber security events notifications conducted under 10 CFR 73.77(a)(1), the NRC may request that the licensee maintain an open and continuous communication channel with the NRC Headquarters Operation Center. Human-to-human communication may be beneficial in order to provide for follow-up questions and clarifications, requests for information or actions, and to facilitate NRC response activities. Note: Because notifications have specified timeframes and are based on "after discovery of" an event, the NRC realizes that the initial notification may be conducted by an individual not knowledgeable about cyber-related activities. However, a cyber security event requiring notification to the NRC should prompt activation of an investigation to determine appropriate immediate and corrective actions (e.g., a Cyber Security Incident Handler (IH) or the Cyber Security Incident Response Team (CSIRT)). After ensuring safe and secure operations of the plant, a member of the investigation (e.g., the IH of CSIRT member) (i.e., knowledgeable about cyber-related activities as well as the current cyber security event) should follow-up the initial notification if there are any additions or modifications to the initial notification.

### 2.3.4 Retraction of Notifications

Licensees desiring to retract a previous cyber security event notification that they have determined (through analysis or investigation) to be non-reportable (e.g., does not meet the threshold of a one, four or eight hour notification) must notify the NRC Headquarters Operations Center by telephone, in accordance with 10 CFR 73.77(c)(5), and indicate the notification being retracted and the basis for the retraction.

Cyber security events may be retracted at any time following the notification to the NRC. However, if a written security follow-up report has already been submitted licensees should refer to the additional guidance in Section 2.4.3 below on documenting retractions.

### 2.3.5 Declaration of Emergencies

Licensees reporting cyber security events under 10 CFR 73.77 that also involve the declaration of an Emergency Classification (e.g., Notification of Unusual Event (NOUE), Alert, Site Area Emergency, or General Emergency), in accordance with their NRC-approved Emergency Response Plan, should follow the appropriate regulations regarding the declaration of an emergency. In other words, emergency declarations have primacy over cyber security event notifications. Consequently, to reduce unnecessary burden and duplication, licensees should make a single report of the events that are subject to both

emergency response and cyber security event notifications. Licensees should indicate in their notification all of the applicable reporting requirements for the event. However, a licensee may need to report additional information regarding a cyber security event that would not be included in an emergency response notification.

### 2.3.6 Elimination of Duplication

Licensees are not required to make separate notifications for cyber security events that also result in the declaration of an emergency. In such circumstances, licensees should make the emergency notifications in accordance with existing regulations (e.g., 10 CFR 50.72). Duplicate notifications are not required for other types of events (e.g., notification of a local, state or other federal agency) that meet the threshold of more than one of NRC's reporting regulations. However, when making such a notification, the licensee should indicate to the NRC that the notification is also to report a cyber security event under a specific paragraph of 10 CFR 73.77.

### 2.3.7 Content of Notifications

Licensees should be prepared to provide following information, if available at the time of the notification:

1. caller name and callback number,
2. facility name and location,
3. emergency classification (if declared),
4. current event status (e.g., in progress, recovered),
5. event date and time (discovery of, and actual occurrence if known),
6. event description including the following information if available or known:
    a. cyber security controls involved/affected (if any)
    b. system(s) involved/affected (SSEP functions, BOP functions, CDAs, CS)
    c. method used to identify the event (e.g., security controls, audit, failed equipment)
    d. what occurred during the event
    e. why the event occurred, if known
    f. how the event occurred, if known
7. safety, security, EP responses and corrective actions taken,
8. offsite assistance (e.g., requested or not requested, arrived, status),

9. media interest, if any, including licensee issued press releases,

10. source of information (e.g., U.S. Computer Emergency Readiness Team, law enforcement) if a law enforcement agency, provide contact telephone number.

### 2.3.8 Voluntary Notifications

Licensees are permitted and encouraged to report any cyber-related event or condition that does not meet the criteria for required reporting, if the licensee believes that the event or condition might be of safety or security significance or of generic interest or concern to the NRC or other licensees. Assurance of safe operation of all plants depends on accurate and complete reporting by each licensee and of all events having potential safety/security significance. For example, a cyber–related event or condition identified and mitigated outside the plant network with no impact on SSEP functions may be indicative of a recently identified or known cyber threat. Such activities should be voluntarily reported to the NRC to support Federal situational awareness activities.

Licensees may make voluntary ENS notifications about cyber-related events or conditions that the licensee believes might be of interest to the NRC. The NRC responds to any voluntary notification of an event or condition as its safety or security significance warrants, regardless of the licensee's classification of the reporting requirement. If it is determined later that the event is reportable, the licensee can change the ENS notification to a required notification under the appropriate 10 CFR 73.77 reporting criterion without adverse consequences as long as the voluntary report met the appropriate timeframe and information required of the required notification. Voluntary notifications do not require a written security follow-up report unless later it is determined the event was reportable under 10 CFR 73.77 reporting criteria.

## 2.4 WRITTEN SECURITY FOLLOW-UP REPORTS

Telephonic notifications to the NRC Headquarters Operations Center for cyber security events specified in paragraphs (a)(1), (a)(2)(i) and (a)(2)(ii) of 10 CFR 73.77 require submission of a written security follow-up report to the NRC within 60 days of the notification in accordance with 10 CFR 73.77(d). Licensees should follow the procedures set forth in 10 CFR 73.4 when submitting their follow- up report. The NRC does not require licensees who have made a notification to the NRC Headquarters Operations Center for cyber security events specified in 10 CFR 73.77(a)(2)(iii), and (a)(3) to submit written security follow-up reports. In addition, cyber security events recorded in the site CAP under 10 CFR 73.77(b) do not require written security follow-up reports.

Written security follow-up reports submitted should be of a format and quality to allow legible reproduction and processing. The written security follow-up reports should contain sufficient details, information, and analysis to allow a knowledgeable individual to understand what occurred during the event. For example, whether any administrative or technical errors occurred, what equipment was involved and/or malfunctioned, what CDAs and/or SSEP functions were affected, if the event involved new hardware and/or software being installed to include patches and updates, or from changes in system

settings or configuration. Additionally, the licensee should indicate whether any immediate corrective actions were taken (to include compensatory measures if applicable) and any long-term corrective actions that are planned to prevent recurrence. In accordance with 10 CFR 73.77(d)(12), licensees must retain a copy of any written security follow-up reports submitted to the NRC for at least three years or until the termination of the license, whichever comes first.

### 2.4.1 NRC Form 366 and 366A

Nuclear power reactor licensees should submit any written security follow-up reports to the NRC required by 10 CFR 73.77 using NRC Form 366, "Licensee Event Report (LER)" and NRC Form 366A, "Licensee Event Report Continuation Sheet" if additional pages are needed.

For licensees utilizing the NRC Form 366, items 1 through 15 should be completed as labeled (if known or applicable). For example, the first item "1. Facility Name" enter the name of the facility (e.g., Indian Point, Unit 1) at which the event occurred. For item 11, check the block that indicates the appropriate requirement (e.g., 10 CFR 73.77(a)(1)). If it is a voluntary LER, check the "Other" block and indicate "voluntary report" in the space below. For item 16, "Abstract" provide a brief description of the cyber event including any failures or degradations that contributed to the event (e.g., user error, procedure violation, cyber security controls) include any CDAs and/or SSEP functions that were impacted by the occurrence and to what extent (e.g., temporarily lost remote (digital) control of the Protected Area Active Vehicle Barrier System due to bad firmware update, barriers were in the up position, and were controlled manually until previous firmware was re-loaded, no unauthorized accesses occurred during this event.).

The NRC Form 366A should be used to provide additional details about the cyber security event to include the content requested from Section 2.4.6 below.

Generally, licensee submitted LERs will be made publically available by the NRC. However, information that is designated by the licensee as, for example, proprietary, safeguards, or classified information, will be withheld (redacted) from the public, as appropriate. Licensees should create, store, mark, label, handle and transmit LERs in accordance with applicable NRC regulations (e.g., 10 CFR 2.390, 73.21, 73.22, part 95). When designated information (e.g., proprietary, safeguards, classified) is included with the LER it should only be entered in item 17, "Narrative" of NRC Form 366A and not included on the NRC Form 366. In addition, the text should clearly indicate what information is designated as proprietary, safeguards classified, etc.

### 2.4.2 Significant Supplemental Information and Correction of Errors

Licensees who discover significant supplemental information after the submission of a written security follow-up report to the NRC should submit a revised written report, in accordance with the same process as used to submit the initial written report. Additionally, licensees who discover errors in a written report previously submitted to the NRC should submit a revised written report, in accordance with the same process as used

to submit the initial written report. A revised written report should replace the previous written report (i.e., the updated report should be complete and should not be limited to only the supplementary or revised information). The revised report should indicate the revision number with revision bars to assist the reader.

### 2.4.3 Retraction of Previous Written Security Follow-up Reports

If a licensee subsequently retracts a notification made under 10 CFR 73.77 and has not yet submitted the written security follow-up report required by 10 CFR 73.77(d), the NRC does not require the licensee to submit the written security follow-up report. However, if the licensee has already submitted a written security follow-up report to the NRC before it retracts the notification, the licensee should then submit a revised written report to the NRC indicating the initial event has been retracted and the basis for that conclusion. This supplemental written security follow-up report is necessary because without the supplemental report (retracting the notification), the only official agency record on the notification would be the initial written security follow-up report, which would not include the retraction.

### 2.4.4 Written Security Follow-up Reports Containing Safeguards Information

Licensees who submit written security follow-up reports to the NRC containing Safeguards Information should create, store, mark, label, handle, and transmit these written reports in accordance with the requirements in 10 CFR 73.21 and 73.22. Licensees should perform a safeguards designation of such reports. Written security follow-up reports should be portion marked to indicate the designation level of the report's information.

### 2.4.5 Written Security Follow-up Reports Containing Classified Information

Licensees who submit written security follow-up reports to the NRC containing classified NSI or RD should create, store, mark, label, handle, and transmit these reports in accordance with the requirements of 10 CFR Part 95, "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data" (Ref. 7). Licensees should perform a derivative classification of such reports in accordance with the classification guide(s) applicable to their facility or activity. Written security follow-up reports should be portion marked to indicate the classification level of the report's information. If the written security follow-up report requires an original classification determination, then the licensee should make a provisional classification decision; mark, handle, store, and transmit the document according to that provisional decision; and forward the document to the NRC for an original classification determination.

### 2.4.6 Content of Written Security Follow-up Reports

Licensees preparing written security follow-up reports should include sufficient information for the NRC to analyze the cyber security event. The NRC staff recommends that written security follow-up reports contain, at a minimum, the following information, as applicable:

1. date and time of the event, including chronological timeline, if applicable,
2. date and time of notification to the NRC, and/or local, State and Federal agencies,
3. the reactor's operating mode at time of event (e.g., shut down, operating),
4. SSEP functions directly or indirectly affected by the event (e.g., compromised, failed, degraded),
5. support systems or equipment directly or indirectly affected that could have compromised SSEP functions (e.g., compromised, failed, degraded),
6. CDAs and/or CS affected by the event (compromised, failed, degraded),
7. security controls involved in the event (e.g., compromised, performed as intended),
8. 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),
9. 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),
10. immediate actions taken in response to the event and any compensatory measures established,
11. description of media interest and press releases,
12. indications or records of previous similar events,
13. procedural or human errors or equipment failures, as applicable,
14. 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),
15. corrective actions taken or planned, including dates of completion,
16. name and phone number of a licensee's point of contact,
17. For failures, degradations, or discovered vulnerabilities of the cyber security program, licensees should also provide the following information, as applicable, in addition to items a. through p. above:

    a. description of failed, degraded, or vulnerable equipment, systems or controls (e.g., manufacturer and model number, procedure number),

b. 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),

c. security settings/configuration of the components, systems or controls that failed, or became degraded or vulnerable,

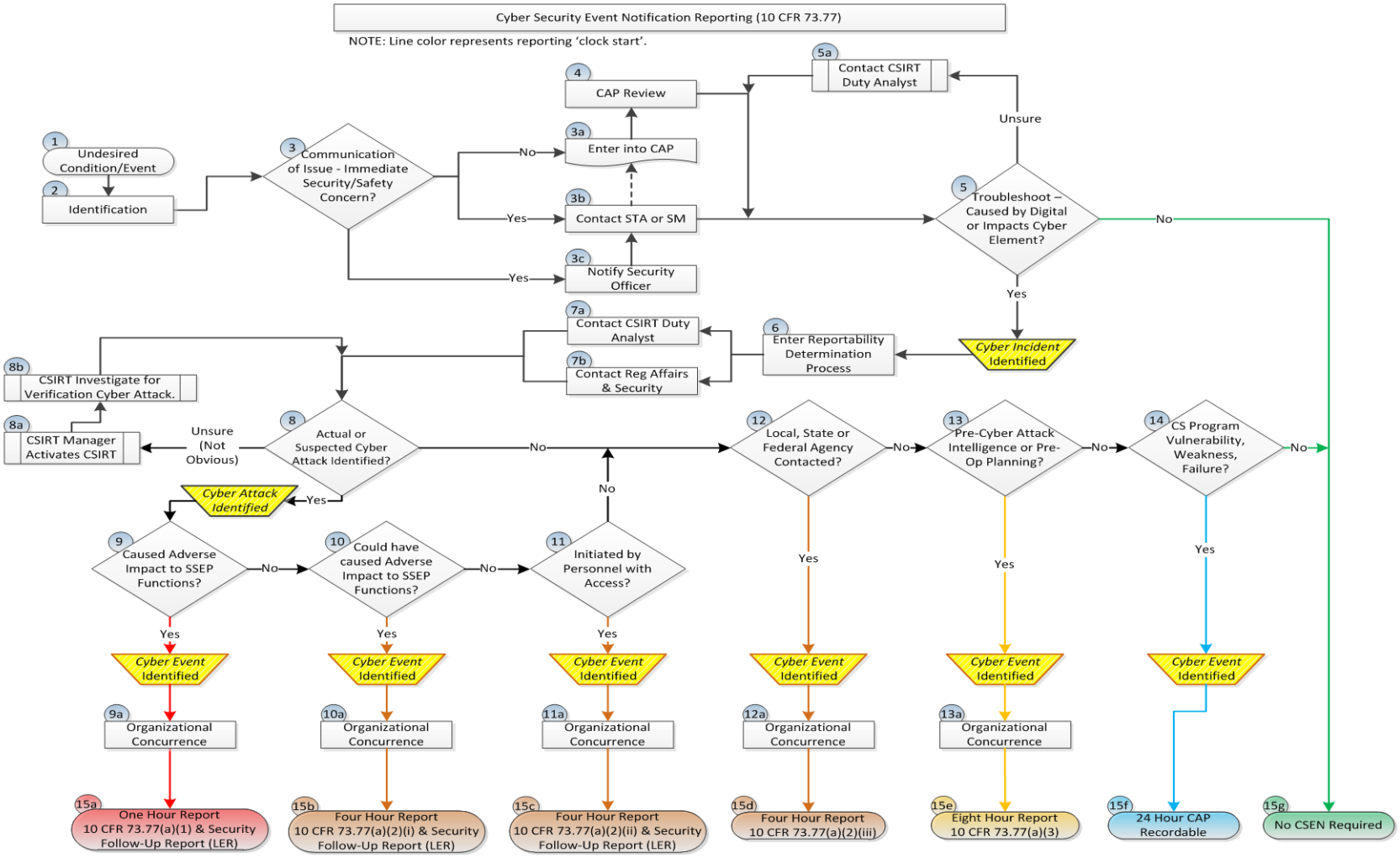
d. apparent cause of component, system or control failure, degradation, or vulnerability.

e. Training of Non-security Staff on Reporting and Recording Requirements

The discovery or identification of reportable or recordable events is not limited to members of the licensee's security organization. Employees, contractors, and vendors with physical or electronic access to digital computer and communications systems and networks within the scope of 10 CFR 73.54 should receive training on cyber security event notifications to foster awareness and to understand their responsibility to immediately notify site-security or management personnel of anomalies, failures, degradations, or vulnerabilities in the cyber security program to include activities that may indicate intelligence gathering or preoperational planning related to cyber attacks. Licensees may provide this training during general plant training and periodic refresher training. The NRC staff notes that some licensees have also found it beneficial to include training "tips" or elements of the training program in recurring plant publications, such as newsletters, electronic signs, or other organizational reminders.

[BLANK PAGE]

# APPENDIX A – REPORTABILITY DECISION FLOWCHART AND INSTRUCTONS



[BLANK PAGE]

| Step 1 | **BEGIN**: Undesired Condition/Event |
|---|---|
| Undesired condition or event exists.<br>• An Undesired Condition includes behavior, practice or event that warranted generation of condition report. | |
| Step 2 | Identification |
| Personnel identify the condition. The method by which adverse conditions may be identified varies greatly and may include, but is not limited to:<br>• An observed component failure, malfunction, deficiency, deviation, defect or an operational disturbance.<br>• 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 | |
| Step 3 | Communication of Issue – Immediate Security/Safety Concern? |
| Plant Personnel communicates issue commensurate with the safety significance. | |
| Step 3a | |
| Condition or issue is entered into CAP. | |
| Step 3b/c | Contact STA or SM / Notify Security Officer |
| If there is a known immediate security/safety concern, Plant Personnel notifies security and/or contacts the Shift Technical Advisor (STA) or Shift Manager (SM). The undesired condition is subsequently entered into CAP.<br><br>Physical Security may be contacted to report Security related issues. Per logic block 3c, the Security organization should notify the Operations Shift Technical Advisor or Shift Manager so that proper individuals are included in the investigation, which may lead to the initiation of an investigation team (e.g., cyber security Incident Handler (IH) or cyber security incident response team (CSIRT). The CSIRT is used for the remainder of the flowchart instructions). If Security has other processes that are followed when an incident is reported to them, make sure to review the process and identify any steps that could bypass the necessary steps to involve personnel that would evaluate the incident for cyber reporting. | |
| Step 4 | CAP Review |
| Regulatory Affairs and Operations reviews shift CAP entries for unidentified, potential reportability issues. | |
| Step 5 | Troubleshoot – Caused by or Impacts Digital or Cyber Element? |
| Operations and/or involved Plant Personnel evaluate the plant issue to determine the cause. If the issue involves, or has a known impact to, a digital system, digital component or an element of the Cyber Security Program, the issue must be screened to determine if an NRC Event Notification is required.<br>• If it is immediately apparent that the cause of the plant issue is the result of, or has a known impact to, a digital system, digital component or an element of the Cyber Security Program, the issue must be screened to determine if an NRC Event Notification is required.<br>• When the immediate cause of the issue is unknown, Operations and/or involved Plant Personnel may utilize standard processes to further investigate or troubleshoot the issue (e.g., troubleshooting procedures, field investigation, Failure Investigation Process, Operability Determinations, cause evaluation, etc.). If at any point it is determined that the cause of the plant issue is the result of, or has a known impact to, a digital system, digital component or an element of the Cyber Security Program, the issue must be screened to determine if an NRC Event Notification is required. | |

| Step 5a | Contact CSIRT Duty Analyst |
|---|---|

Operations should contact the Cyber Security Incident Response Team (CSIRT) Duty Analyst if assistance is needed to determine the questions posed in Step 5.

Step 5 and 5a in the flow chart represents the troubleshooting/evaluation that occurs when responding to an undesired condition/event. As described in the flow chart explanation, various departments and associated personnel will troubleshoot the issue using standard processes to determine the scope of the event, potential cause, extent of condition, magnitude of impact, etc. Logic block 5 is ultimately intended to determine whether the incident involves digital equipment or elements of the cyber security program that may require a report under 10 CFR 73.77. This step is not asking whether cyber is the cause of the event, but rather if digital equipment or cyber program elements are involved in the event to ensure the right personnel are contacted for investigation. As part of responding to the undesired condition/event, personnel should consider two things:

1) What is the intent of identifying whether the undesired condition/event involves digital assets or digital system, including digital support equipment?

For the purpose of this guidance, digital equipment includes, but is not limited to:

- Digital assets (i.e., HMI, digital flow transmitter, PLC, network switch, digital chart recorder)
- Digital support system (i.e., digital HVAC controls, digital power controller, digital fire protection equipment)
- Portable Media and Mobile Devices (PMMDs) (i.e., thumb drive, laptop, HART communicator, CD/DVD)

The involvement of digital equipment (directly or indirectly) in the event may indicate that a compromise of the digital equipment lead to the cause of the event and further investigation by cyber security point of contact is necessary to further determine if a cyber security report is required per 10 CFR 73.77.

2) What is referred to as a Cyber Element?

A cyber element refers to any cyber security controls, tools, or personnel behaviors that are associated with the cyber security program or outlined in the site Cyber Security Plan. If there is indication that someone or something has negatively impacted the cyber program, caused elements of the program to become less effective, or there is indication of intelligence gathering or pre-operational planning related to a cyber attack, this may warrant a cyber security report and further investigation is needed.

For example:

Cyber Security Control Impact –

a) System owner was called on by Operations to respond to a DCS alarm; the engineer immediately noticed a rogue connection that was a bypass of the defensive architecture per CSP 4.3.
b) During a walk-down of the turbine control system, an unauthorized thumb drive was found unattended and connected to the HMI. This situation would be considered traversing the protections of the PMMD program and requires further investigation and may require a cyber security report.

Cyber Security Tools – Tampering with or a compromise of the PMMD scanning station or whitelisting network.

Cyber Security Behaviors – Indication that someone is organizing or intelligence gathering for

conducting a cyber attack. These behaviors should be reported to Security for proper investigation.

During the response to a plant event, if either a digital asset or Cyber Element are suspected to be associated with the event, then the CSIRT duty analyst shall be contacted to further investigate and work with the appropriate organizations to determine if a cyber security notification is required. If it is evident that the event has nothing to do with digital equipment or the cyber security program, a cyber security notification is not required at this time.

| Step 6 | Enter Reportability Determination Process |
|---|---|

Where the identified condition or issue merits further investigation, as required by Step 5, to verify that a cyber security reportable event has occurred, Operations enters the reportability determination process and contacts the appropriate support personnel to initiate an evaluation using the following guidance:

| Step 7a | Contact CSIRT Duty Analyst |
|---|---|

If not already done so in support of Step 5, Operations should Contact the CSIRT Duty Analyst to coordinate obtaining the necessary technical resources for evaluating the issue and to assist in the reportability determination.

The Duty Analyst is contacted by Operations if there is reason to believe that the undesired condition/event is related to the characteristics described in logic block 5. This person is defined in the Incident Response procedure. The Duty Analyst is a member of the Digital Process Systems (DPS) Engineering team. The CSIRT Manager is the Manager of this DPS group. The Duty Analyst shall contact his/her Manager to keep them abreast of the issue reported to them. At some point, the CSIRT Manager may be required to obtain additional resources to respond to the plant event to help determine if cyber is the potential cause.

| Step 7b | Contact Regulatory Affairs and Security |
|---|---|

CSIRT and Operations should ensure that the appropriate Regulatory Affairs and Security personnel are aware of the issue and the ongoing evaluation and to solicit input/support in determining if the condition requires an NRC report.

| Step 8 | Actual or Suspected Cyber Attack Identified? |
|---|---|

CSIRT will perform an initial evaluation to determine if an actual or suspected Cyber Attack has occurred.

This step in the flowchart helps distinguish between attempts to infiltrate the Nuclear environment versus successful entry that could cause an adverse impact. During this step, members of the incident response team will need to convene in order to determine whether there is enough evidence (indication) that would lead to a cyber security notification. As part of evaluating the event, the clock starts for the notification once there is indication that one of the three report types is required.

The Security evaluation of the event needs to consider malicious intent of actions related to the adverse impact on a CDA or SSEP function to determine if the event involved a cyber attack.

| Step 8a | CSIRT Manager Activates CSIRT |
|---|---|

If signs of a Cyber Attack are not obvious, or there is no indication of a Cyber Attack, but further investigation is needed, a preliminary assessment may be required to rule out other common degradations or failures. In such situations, the CSIRT Manager will activate the CSIRT.

| Step 8b | CSIRT Investigates for Verification of Cyber Attack |
|---|---|

CSIRT performs the necessary investigation to verify that a Cyber Security Attack has occurred.

| Step 9 | Cyber Attack Caused Adverse Impact to SSEP Functions? |
|---|---|

CSIRT and supporting organizations determine if a one hour report is required per 10 CFR 73.77(a)(1):

- *A one hour report is required in accordance with 10 CFR 73.77(a)(1) when the Cyber Attack adversely impacted safety related or important-to-safety functions, security functions, or emergency preparedness functions (SSEP) (including offsite communications); or compromised support systems and equipment resulting in adverse impacts to safety, security, or emergency preparedness functions within the scope of § 73.54.*

| Step 9a | Organizational Concurrence |
|---|---|

If CSIRT determines that a cyber attack has occurred, and that it has adversely impacted SSEP functions (including support systems and equipment), CSIRT, Operations, Regulatory Affairs, Security and Emergency Preparedness (where applicable) should review the issue and gain concurrence on the appropriate reporting requirements.

| Step 10 | Cyber Attack Could have caused Adverse Impact to SSEP Functions? |
|---|---|

CSIRT and supporting organizations determine if a four hour report is required per 10 CFR 73.77(a)(2)(i):

- *A four hour report is required in accordance with 10 CFR 73.77(a)(2)(i) when the cyber attack could have caused an adverse impact to SSEP functions (including offsite communications); or that could have compromised support systems and equipment, which if compromised, could have adversely impacted SSEP functions within the scope of § 73.54.*

Only one (1) plausible assumption needs to be considered when evaluating if the cyber attack could have caused an adverse impact. If the answer to this question is not immediately apparent, consider if a four-hour report is already required under 10 CFR 73.77(a)(2)(ii) (Step 11).

| Step 10a | Organizational Concurrence |
|---|---|

If CSIRT determines that the cyber attack has occurred, and that it could have caused an adverse impact to SSEP functions (including support systems and equipment), CSIRT, Operations, Regulatory Affairs, Security and Emergency Preparedness (where applicable) should review the issue and gain concurrence on the appropriate reporting requirements.

| Step 11 | Cyber Attack Initiated by Personnel with Access? |
|---|---|

Where Step 9 or 10 does not result in a report, CSIRT and supporting organizations determine if a four report is required per 10 CFR 73.77(a)(2)(ii):

- *A four hour report is required in accordance with 10 CFR 73.77(a)(2)(ii) when a suspected or actual cyber attack was initiated by personnel with physical or electronic (i.e., logical) access to digital computer and communication systems and networks within the scope of § 73.54.*

| Step 11a | Organizational Concurrence |
|---|---|

If CSIRT determines that the cyber attack was initiated by personnel with physical or electronic (i.e., logical) access to digital computer and communication systems and networks, CSIRT, Operations, Regulatory Affairs, Security and Emergency Preparedness (where applicable) should review the issue and gain concurrence on the appropriate reporting requirements.

| Step 12 | Local, State or Federal Agency Contacted? |
|---|---|

CSIRT and supporting organizations determine if a four report is required per 10 CFR 73.77(a)(2)(iii):

- *A four hour report is required in accordance with 10 CFR 73.77(a)(2)(iii) after notification of a local, State, or other Federal agency (e.g., law enforcement, FBI, etc.) 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 § 73.54 that does not otherwise require a notification under paragraph (a) of this section.*

| Step 12a | Organizational Concurrence |
|---|---|
| If a local, state or federal agency is contacted at any time as a result of a cyber-related event, CSIRT, Operations, Regulatory Affairs, Security and Emergency Preparedness, where applicable, should review the issue and gain concurrence on the appropriate reporting requirements. | |
| Step 13 | Pre-Cyber Attack Intelligence or Preoperational Planning? |
| CSIRT and supporting organizations determine if an eight report is required per 10 CFR 73.77(a)(3):<br>o *An eight hour report is required in accordance with 10 CFR 73.77(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 within the scope of § 73.54.* | |
| Step 13a | Contact Regulatory Affairs & Security |
| After receipt or collection of information regarding observed behavior, activities, or statements that may indicate intelligence gathering or pre-operational planning for a cyber attack, CSIRT, Operations, Regulatory Affairs, Security and Emergency Preparedness, where applicable, should review the issue and gain concurrence on the appropriate reporting requirements. | |
| Step 14 | CS Program Vulnerability, Weakness, Failure? |
| CSIRT and supporting organizations determine if the issue constitutes a vulnerability, weakness, failure or deficiency of the Cyber Security Program and ensure any such issues are recorded in the site corrective action program within twenty-four hours of their discovery. | |
| Step 15 | **END**: Make Necessary Telephone Call to NRC |
| Where no CSEN report is required, exit process. | |

[BLANK PAGE]

# APPENDIX B – GUIDANCE FOR DETERMINING START OF REPORTABILITY CLOCK

Guidance for evaluating whether cyber is the cause of the event and for when sufficient information exists starting the reportability notification clock.

Time of discovery for reportability purposes begins when the Cyber Security incident lead (e.g., Incident Handler (IH) or Cyber Security Incident Response Team (CSIRT)) determines that one or more of the reporting criteria was met. Time of discovery does NOT start when a digital component (CDA) is found to be in a failed or compromised state. The discovery of a failed or compromised state does require a decision as to whether the failure was caused by a cyber attack or some other failure mechanism. The timeliness of the investigation needs to be commensurate with the safety significance of the issue (Reference 12). The investigations of the technical impact and the malicious intent aspect are both needed in the determination of reportability and should be pursued expeditiously. The outputs from these investigations come together in decision blocks 8, through 14 in APPENDIX A, REPORTABILITY DECISION FLOWCHART AND INSTRUCTIONS. Each reporting criterion is discussed below:

1 hour notification – required by 10 CFR 73.77(a)(1) if a cyber attack adversely impacted SSEP functions or compromised support systems and equipment resulting in adverse impacts to SSEP functions. This reporting criterion is triggered ONLY if actual damage to SSEP functions occurs and it is determined by the Shift Manager or IH or CSIRT that there is reason to believe the cause of the damage is or is likely to be a cyber attack as defined in the Cyber Security Plan. A cyber attack is any event in which there is reason to believe that an adversary has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause malicious exploitation of a CDA. In the context of a 1 hour notification, the adversary has to have successfully caused damage to one or more SSEP functions that resulted in an adverse impact.

4 hour notification – required by 10 CFR 73.77(a)(2)(i) if a cyber attack could have adversely impacted SSEP functions or could have compromised support systems and equipment resulting in adverse impacts to SSEP functions. This reporting criterion is triggered ONLY if it is determined by the Shift Manager or IH or CSIRT that an actual, unsuccessful, cyber attack as defined in the Cyber Security Plan occurred. A cyber attack is any event in which there is reason to believe that an adversary has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause malicious exploitation of a CDA. In the context of this 4 hour notification, the adversary has to have attempted to cause damage to one or more SSEP functions that, if successful, would have resulted in an adverse impact to one or more SSEP functions.

4 hour notification – required by 10 CFR 73.77(a)(2)(ii) if a cyber attack was initiated by personnel with physical or electronic access to digital computer and communication systems and networks within the scope of 10 CFR 73.54. This reporting criterion is triggered if it is determined by the Shift Manager or IH or CSIRT that there is reason to believe that an actual attack was initiated by personnel with physical or electronic access. It is also triggered if the IH or CSIRT suspects, but cannot absolutely confirm, that an actual attack was initiated by

personnel with physical or electronic access. In the context of this 4 hour notification, the key is the initiation, or attempt by personnel with physical or electronic access. The attack does not have to be successful, nor does it have been carried out to completion – it only has to be initiated.

4 hour notification – required by 10 CFR 73.77(a)(2)(iii) if any local, state, or federal agency is notified of an event related to the implementation of the cyber security program. For this criterion, making a notification, related to the cyber security program, to another government agency triggers the reporting criteria, and starts the clock as time of discovery. This is similar to four-hour reporting under 10CFR50.72(b)(2)(xi) for notifications made to other governmental agencies.

8 hour notification – required by 10 CFR 73.77(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. This information could either be received from an outside organization, such as the FBI, or collected by the site. In the event that the site is contacted from a governmental organization with credible information regarding intelligence gathering or pre-operational planning related to a cyber attack, time of discovery would be the receipt of the credible information. If the genesis of the information is the on-site collection of information, time of discovery is when the Security Manager or IH or CSIRT reviews the collected information and determines that it is indicative of intelligence gathering or pre-operational planning related to a cyber attack.

# APPENDIX C – EXAMPLES FOR IMPLEMENTATION AND TRAINING USE

- 1-hour notification – cyber attack that adversely impacted an SSEP function

C.1.1 A 1 hour notification is required if an SSEP function adversely affected by a digitally based change that was intentionally caused by an adversary with malicious intent.

C.1.2 After an unplanned outage, the vendor was brought in to work on the automatic voltage regulator (AVR) personal computer. The vendor's escort turned his back to take a phone call and the vendor made some changes to the system. Later, the AVR trips the unit causing another unplanned outage, due to the changes the vendor made while the escort's back was turned. A 1 hour notification reportability clock starts if it is determined that there is reason to believe there was malicious human intervention that intended to cause the malfunction.

C.1.3 The hand geometry readers deny access to authorized plant workers. All the hand geometry units at the protected area entrance, except the service door were in alarm status. Troubleshooting discovered that a parameter on the security computer was not valid. Site personnel are unsure how the parameter got changed, but it is known that only someone with elevated privileges can make this change. Since the security system is air-gapped, the only places the change could have taken place would have been in the CAS or SAS. An interview with the involved individuals is necessary to determine if there was malicious intent involved in the configuration change. A cyber attack may have been involved but an unintentional mistake is also plausible. The change to the parameter would have to have been initiated by someone with physical or logical access within the Protected Area (PA). A 1 hour notification reportability clock starts if the interview or investigation determines there is reason to believe that the officer intentionally changed the parameter due to some malicious intent.

C.1.4 At the time of a maintenance service outage of the backup phone system that provides communication to the EOF, the primary phone system experiences a distributed denial of service (DDOS) attack from the internet. The EP function is lost. A 1 hour notification reportability clock starts if it is determined that both phones systems are out of service since there was a malicious intent and an adverse impact to the SSEP function.

C.1.5 A security officer plugs his smartphone into the USB port on the security computer to charge it. The smartphone introduces malware on the network which compromises the badging database and causes a denial of service to the security system. Alarms will no longer clear on the security computer, the video feed from the security cameras appears jumpy, and certain vital area doors no longer require badge access to be opened. The antivirus software on the backup security server alerts on the virus and notifies the officer. A 1 hour notification is required because the malware infection resulted in a cyber attack that compromised an SSEP function. The origination of the malicious intent does not need to be

known. A 1 hour notification reportability clock starts if it is determined that that the SSEP function was adversely affected by the malware. If later the event was determined to not involve a malicious attempt to exploit a CDA, the notification may be retracted.

C.1.6 A maintenance worker misreads a procedure and fails to scan a PMD prior to planned maintenance and connects the PMD to each metal detector in the security main access detectors. A post work scan reveals the PMD contains a virus. Troubleshooting is immediately initiated and reveals the virus is on all of the metal detectors and the sensitivity of the detectors has been adversely affected. A 1 hour notification reportability clock starts if it is determined that the malware infection resulted in compromise of an SSEP function. While the maintenance worker did not deliberately infect the metal detectors, there was reason to believe there was malicious intent and an adversary behind the source of the virus.

- 1-hour notification – cyber attack that compromised support systems and equipment resulting in adverse impact of an SSEP function.

C.1.7 Someone tampered with digital HVAC controls that supply cooling to electrical equipment. The problem cannot be corrected, and temperature rises quickly causing the electrical equipment to shut off on high temperatures. Electrical components (switchgear, circuitry, and/or logic) are negatively affected by rising temperatures, and SSEP equipment is adversely impacted as a result. A 1 hour notification reportability clock starts if it is determined that someone tampered with the digital controls and the SSEP function of the equipment was compromised.

C.1.8 The discovery of an intentional unauthorized change of the control setpoint on the TSC HVAC system digital temperature control module that resulted in excessively high temperatures in the TSC making the TSC facility uninhabitable. A 1 hour notification is required once the adverse impact and the control setpoint change are determined.

C.1.9 A cyber attack on the onsite fiber optics system that operates the breakers in the switchyard that supply offsite power to the ESF and non-ESF busses. If the cyber attack was to the licensee's fiber optic network, then a CDA is adversely affected and reportability under 10 CFR 73.77 is involved. If the cyber attack resulted in adverse impact on an SSEP function (e.g., loss of power to the safeguards power bus resulting in Emergency Diesel Generator (EDG) start), then a 1 hour notification is required. A 1 hour notification reportability clock starts if the investigation reveals that some form of a cyber attack occurred (was not a mechanical equipment failure or was not an accidental trip).

- 4-hour notification – cyber attack that could have caused an adverse impact to an SSEP function

C.4.1 A 4 hour notification is required if a CDA or CS is affected by a digitally based change that was intentionally caused by an adversary with malicious intent and the change could have had but did not have an adverse impact on the SSEP function.

C.4.2 A security officer notices an unmarked and believed to be an unauthorized cable run around a cabinet door, connecting a CDA behind the data diode (or air gap) to a network switch on the business network. No signs of actual compromise exist on the CDA side of the data diode, and the cable is removed before any compromise occurred, however the cable was installed outside an authorized process. A 4 hour notification reportability clock starts if the investigation determines there is reason to believe that the cable was installed with malicious intent to the CDA. A 4 hour notification is required because, while there was no actual adverse impact to the SSEP function, there could have been if the pathway was used for compromise. Escalated to 1 hour notification if it is determined there was a compromise to a SSEP function due to the pathway. The assumption is that the individual who installed the rogue cable could have used the bypass to compromise CDAs and adversely impact an SSEP function.

C.4.3 Investigation of an alarm reveals a malicious malware virus on a Feedwater system computer control system. Investigation revealed the virus had the capability of modifying the control system software. The assumption is that the malware could have also compromised CDAs and adversely impacted an SSEP function. A 4 hour notification is required if it is determined that that virus had the capability of modifying the software.

C.4.4 With the backup phone system available to provide communication to the EOF, the primary phone system experiences a DDOS attack from the internet. The EP function is maintained by the adequately independent alternative capability. There is a malicious intent and there could be an adverse impact to the SSEP function assuming the backup capability became degraded. A 4 hour notification reportability clock starts if it is determined that the primary phone system went out of service due to the DDOS attack.

C.4.5 During a refueling outage, the polar crane was observed moving without an operator present. The crane controls were in their storage locations and were not in use. In the first instance, the crane raised the now secure reactor head up 3 feet in 4 seconds before immediately changing direction and lowering the head back down. Then, the crane moved the reactor head to the left approximately 10 feet before an operator pressed the emergency stop button. The head came to rest over no safety equipment, but was within 5 feet of a safety related pump. While investigating, it was determined that several of the crane's configuration parameters had been changed. Then, a suspicious box was found in a high radiation area. When security investigated the box, it was determined to be a

transmitter with electronic controls and an antenna that could control the crane remotely. A 4hour notification reportability clock starts if it is determined that a cyber attack had an adverse impact on the crane, but no SSEP functions were impacted. The assumption is that the crane could have moved further and released the reactor head on top of safety related equipment, causing an adverse impact to the SSEP function.

C.4.6 During review of a CSEN event reported by another licensee, a vulnerability scan with an updated scanning engine reveals a similar malicious virus with an unexpired timer is installed on several CDAs in the plant. A 4 hour notification is then required because there was no actual adverse impact to the SSEP function, but there could have been assuming the virus had been activated and resulted in an adverse impact on an SSEP function.

- 4-hour notification – cyber attack that could have compromised support systems and equipment, which if compromised, could have adversely impacted an SSEP function.

C.4.7 A 4 hour notification is required upon discovery of an unlocked cabinet containing CDAs or CS equipment that is required to be locked and tampering of the locking device(s) is determined to have occurred. The assumption is that the individual who opened the cabinet with malicious intent attempted to compromise CDAs within the cabinet and adversely impact an SSEP function.

- 4-hour notification – suspected or actual cyber attack initiated by personnel with physical or electronic access to digital computer and communication systems and networks (and not reportable as a 1 hour event)

C.4.8 An I&C worker changes a few of the parameters on a digital temperature indicating controller. Alarms go off in the main control room and an Aux Operator is dispatched to investigate. There is no adverse impact to the SSEP function of the device. The impact would only be to local temperatures. Device cannot be changed without human interaction at the HMI. This was not an equipment malfunction. It is suspected that human interaction was involved. Interview with the I&C worker revealed the worker was attempting to trip the affected system; therefore, a 4 hour notification is required. The event could escalate to a 1 hour notification if the condition was not corrected before an adverse impact to the SSEP function occurred.

C.4.9 A single hand geometry unit at the protected area entrance, is in alarm status (i.e., the security function is degraded but still available). Troubleshooting discovered that a parameter on the security computer was not valid. Site is unsure how the parameter got changed, but it is known that only someone with elevated privileges can make this change. Since the security system is air-gapped, the only places the change could have taken place would have been in the CAS or SAS. An interview with the involved individuals is necessary to determine if there was malicious intent involved in the configuration change. A cyber attack is suspected, but not confirmed, and the cyber attack would have to have been initiated by someone

with physical or logical access within the PA. A 4 hour notification is required if the interview determines that there is reason to believe there was malicious intent to cause adverse impact on a CDA.

- 4-hour notification – notification to law enforcement (LLEA, FBI, etc.) of an event related to the licensee's implementation of their Cyber Security Program for digital computer and communication systems and networks (and not otherwise reportable as a 1 or 4 hour notification).

  C.4.10 CSIRT identifies the need to interview a previously employed worker as part of an event investigation involving the discovery of a malicious virus on a CDA in the plant. The individual makes threats during a phone conversation. The Shift Manager and Security Manager are contacted who contact the local police to investigate the threat.

- 8-hour notification – information obtained regarding observed behavior, activities, or statements that may indicate intelligence gathering or pre-operational planning related to a cyber security attack against digital computer and communication systems and networks.

  C.8.1 A security officer overhears two maintenance workers talking in the cafeteria. They are complaining about having too much work to do and being under appreciated by the company. One says he is tasked with maintenance on the digital main feedwater controls tomorrow and suggests tampering with the controls "to teach the utility a lesson". The other agrees and says he'll be glad to help. Therefore, an 8 hour notification is required for pre-operational planning related to a cyber security threat.

- 24-hour CAP entry – identification of vulnerability, weakness, failures and deficiencies in cyber security program

  C.24.1 CS program implementation deficiencies identified by worker, supervisor, Licensee Self-Assessment, Nuclear Oversight, INPO, NRC.

  C.24.2 Missing USB port blocker – Escalates to 1 hour or 4 hour notification (dependent on adverse impact) if there is evidence that the CDA and SSEP function were compromised through the open port or could have been compromised had an adversary exploited the vulnerability.

  C.24.3 Portable Media Inventory identifies unaccounted for PMD due to an administrative error with PMD found.

  C.24.4 Portable Media Inventory identifies unaccounted for PMD due to PMD not immediately found. (potential path to a 4 hour event) Escalation to 4 hour notification if, once found, you determine it was compromised and used on CDA and could have adversely affected a SSEP function.

  C.24.5 Portable Media used but not scanned at KIOSK before or after use. Escalates to 1 hour or 4 hour notification (dependent on adverse impact) if malware on the PMD

reached a CDA and either did or could have caused adverse impact of an SSEP function.

C.24.6 A CDA cabinet is accidentally left unlocked after approved work, and there is no sign of tampering or compromise.

- 24-hour CAP entry – ENS notification under 10 CFR 73.77
  - No example needed
- Events not reportable

C.NR.1 Phishing email on a business network e.g., email with a request to click on a link

C.NR.2 The initial scan of a PMD at a scanning station identifies a virus before the PMD is authorized for use on a CDA.

C.NR.3 Security Information and Event Management (SIEM) or intrusion detection system identifies an occurrence that is determined to be a false positive.

C.NR.4 The hand geometry readers deny access to authorized plant workers. All the hand geometry units at the protected area entrance, except the service door were in alarm status. Troubleshooting discovered that a parameter on the security computer was not valid. Site is unsure how the parameter got changed, but it is known that only someone with elevated privileges can make this change. Since the security system is air-gapped, the only places the change could have taken place would have been in the CAS or SAS. An interview with the involved individuals is necessary to determine if there was malicious intent involved in the configuration change. A cyber attack is suspected, but not confirmed, and the cyber attack would have to have been initiated by someone with physical or logical access within the PA. No notification is required if the interview results in an admittance of human error or accidental keystrokes that led to the issue because a cyber attack has been ruled out.

C.NR.5 Someone hacked into the offsite fiber optics system that operates non-CDA equipment. If the hack occurred on a device outside the licensee's ownership (i.e., outside the NRC/NERC "bright-line" for the station), then the devices are not CDAs and no reporting requirement would apply. These SSCs are outside the licensee's control and include electrical distribution equipment past the first inter-tie with the Licensee's equipment and the offsite distribution system. A NERC and/or a DOE report may be required, but is outside the scope of this guidance.

# APPENDIX D – GLOSSARY

This glossary is intended to aid the reader in implementing this guide to meet the requirements set forth in 10 CFR 73.77. Definitions for certain security terms are also found in 10 CFR 73.2, "Definitions". The glossary defines only those terms that are specific to their usage in CSEN. Other terms should be referenced in the following order of preference.

1. Specific terms defined in Rules. (10 CFR 73.2, "Definitions")
2. Licensee Cyber Security Plan
3. NEI 08-09
4. NIST IR 7298 Glossary of Key Information Security Terms.
5. National Information Assurance (IA) Glossary CNSSI No. 4009
6. NRC RG 5.76, Physical Protection Programs at Nuclear Power Reactors
7. NRC RG 5.83 July 2015
8. NRC RG 5.71 Rev. 0, January 2010

**Access Control** — The control of entry or use, to all or part, of any physical, functional, or logical component of a CDA.

**Adverse Impact** — A direct deleterious effect on a CDA (e.g., loss or impairment of function, reduction in reliability, reduction in the ability to detect, delay, assess or respond to malevolent activities, reduction of ability to call for or communicate with offsite assistance, and the reduction in emergency response ability to implement appropriate protective measures in the event of a radiological emergency). In the case where the direct or indirect compromise of a support system causes a safety-related, important-to-safety, security or emergency preparedness system or support system to actuate or "fail safe" and not result in radiological sabotage (i.e., causes the system to actuate properly in response to established parameters and thresholds), this is not considered to be an adverse impact in the context of 10 CFR 73.54(a).

**Adversary** — Individual, group or organization that has adversely impacted or is attempting to adversely impact a CDA. [NEI 08-09]

**Attempts to Cause** — Efforts to accomplish a threat, even though it has not occurred or has not been completed because it was interrupted, stopped before completion, or may occur in more than two hours, as established through reliable and substantive information.[RG 5.76 Physical Protection Programs at Nuclear Power Reactors [U]]

| | |
|---|---|
| **Compromise** | Loss of confidentiality, integrity, or availability of data or system function. |
| **Credible** | Information received from a source determined to be reliable (e.g. law enforcement, government agency, etc.) or has been verified to be true. A threat can be verified to be true or considered credible when: Physical evidence supporting the threat exists, Information independent from the actual threat message exists that supports the threat, **or** a specific known group or organization claims responsibility for the threat.<br>[RG 5.76 Physical Protection Programs at Nuclear Power Reactors [U]] |
| **Critical Digital Asset (CDA)** | A digital computer, communication system, or network that has been identified through site-specific analysis required 10 CFR 73.54(b)(1) as requiring protection against a cyber attack. A CDA may be:<br>• a component of a critical system (this includes assets that perform SSEP functions; provide support to, protect, or provide a pathway to Critical Systems); or<br>• a support system asset whose failure or compromise as the result of a cyber attack would result in an adverse impact to an SSEP Function. |
| **Critical System (CS)** | A system that is associated with or provides safety-related functions; important-to-safety functions; security functions; emergency preparedness functions, including offsite communications; or support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions. |
| **Cyber Attack** | Any event in which there is reason to believe that an adversary has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause malicious exploitation of a CDA.[Reference 11] |
| **Cyber Incident** | A digitally related adverse condition. |
| **Integrity** | Quality of a system reflecting the logical correctness and reliability of the operation of the system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Additionally, integrity includes protection against unauthorized modification or destruction of information. |
| **Interruption of Normal Operation** | A departure from normal operations or conditions that, if accomplished, would result in a challenge to the facility's safety, security, or emergency response systems. This may also include an event that |

| | |
|---|---|
| | causes a significant redistribution of security, safety, or emergency response resources. This could include intentional tampering with systems or equipment that is normally in a standby mode, but would need to operate if called upon in an abnormal or emergency situation. Section 236 of the AEA (42 U.S.C. Section 2284) treats as sabotage the knowing interruption of normal operation of any such facility through the unauthorized use of, or tampering with, the machinery, components, or controls of any such facility, or attempting or conspiring to carry out such an act. |
| **Malware** | Malicious software designed to infiltrate or damage a CDA, CS or protected network without licensee consent. Malware includes computer viruses, worms, Trojan horses, Root kits, spyware, adware and other potentially unwanted programs. |
| **Mobile Code** | Programs or parts of programs obtained from remote control systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient. |
| **Patch** | A fix for a CDA or software program where the actual binary executable and related files are modified. |
| **Protected Network** | A network that is air gapped or behind a data diode that contains one or more CDAs. |
| **Recovery** | Steps taken to restore a system, function, or device to its original state of operation following a catastrophic or partial loss of functionality or when an original state of operation is challenged by either an event (such as a cyber attack) or anomaly (behavior not expected from normal operation). |
| **Social Engineering Techniques** | Attempts by unauthorized individuals to gain physical or electronic (e.g., password) access to systems via impersonation of authorized functions or personnel. |
| **Tampering (Cyber)** | Altering, disabling, or damaging digital computer and communications systems and networks or cyber security controls for improper purposes or in an improper manner. |

# REFERENCES[1]

1. *U.S Code of Federal Regulations* (CFR), "Physical Protection of Plants and Materials," Part 73, Chapter 1, Title 10, "Energy".

2. CFR, "Domestic Licensing of Production and Utilization Facilities," Part 50, Chapter 1, Title 10, "Energy".

3. NRC, Regulatory Guide (RG) 5.69, "Guidance for the Application of Radiological Sabotage Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements," Washington, DC.

4. U.S. Homeland Security's, "Terrorist Threats to the U.S. Homeland Reporting Guide for Critical Infrastructure and Key Resource Owners and Operators," dated January 24, 2005. (ADAMS No. ML112280232).

5. NRC, SRM-10-0001, "Regulation of Cyber Security at Nuclear Power Plants," Washington, DC, October 21, 2010. (ADAMS No. ML102940009).

6. Executive Order 13526, "Classified National Security Information," dated December 29, 2009 published December 29, 2009. (75 FR 707).

7. CFR, "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data," Part 95, Chapter 1, Title 10, "Energy".

8. U.S. Nuclear Regulatory Commission, "Backfitting Guidelines," NUREG-1409, Washington, DC, June 1990. (ADAMS No. ML 032230247).

9. NRC Management Directive 8.4, "Management of Facility Specific Backfitting and Information Collection," U.S. Nuclear Regulatory Commission, Washington, DC.

10. NEI 08-09, Rev 6, "Cyber Security Plan for Nuclear Reactors,"

11. NRC letter to NEI, Nuclear Energy Institute 08-09, "Cyber Security Plan Template, Rev. 6", dated June 6, 2010 (ML101550052) providing endorsement of definition of cyber attack.

12. NUREG-1022, "Event Report Guidelines 10 CFR 50.72(b)(3)(xiii)", Revision 3, Supplement 1

[1] Publicly available NRC published documents are available electronically through the NRC Library on the NRC's public Web site at http://www.nrc.gov/reading-rm/doc-collections/ and through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html The documents can also be viewed online or printed for a fee in the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, MD. For problems with ADAMS, contact the PDR staff at 301-415-4737 or (800) 397-4209; fax (301) 415-3548; or e- mail pdr.resource@nrc.gov.