U.S. NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REGULATORY RESEARCH

July 2015
Division 5

REGULATORY GUIDE

Technical Lead
Brad Bergemann

REGULATORY GUIDE 5.83

(Draft was issued as part of DG-5019, Revision 2 of Regulatory Guide 5.62, dated January 2011)

CYBER SECURITY EVENT NOTIFICATIONS

A. INTRODUCTION

Purpose

This regulatory guide (RG) describes approaches and methodologies that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable 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.

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.

Written suggestions regarding this guide or development of new guides may be submitted through the NRC's public Web site under the Regulatory Guides document collection of the NRC Library at http://www.nrc.gov/reading-rm/doc-collections/reg-guides/contactus.html.

Electronic copies of this regulatory guide, previous versions of this guide, and other recently issued guides are available through the NRC's public Web site under the Regulatory Guides document collection of the NRC Library at http://www.nrc.gov/reading-rm/doc-collections/. The regulatory guide is also available through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html, under ADAMS Accession No. ML14269A388. The regulatory analysis may be found in ADAMS under Accession No. ML14170B076 and the staff responses to the public comments on DG-5019 may be found under ADAMS Accession No. ML14136A214.

(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.

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).

- 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).

Purpose of Regulatory Guides

The NRC issues regulatory guides to describe to the public methods that the staff considers acceptable for use in implementing specific parts of the agency's regulations, to explain techniques that the staff uses in evaluating specific problems or postulated accidents, and to provide guidance to

applicants. Regulatory guides are not substitutes for regulations and compliance with them is not required. Methods and solutions that differ from those set forth in regulatory guides will be deemed acceptable if they provide a basis for the findings required for the issuance or continuance of a permit or license by the Commission.

Paperwork Reduction Act

This regulatory guide contains information collection requirements covered by 10 CFR Part 73 that the Office of Management and Budget (OMB) approved under OMB control number 3150-0002. The NRC may neither conduct nor sponsor, and a person is not required to respond to, an information collection request or requirement unless the requesting document displays a currently valid OMB control number.

B. DISCUSSION

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.

Background

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. The NRC understands that the licensee may conduct a preliminary assessment if signs of a cyber attack are not obvious (e.g., antivirus protection alert, intrusion detection system alert) in order to rule out other common degradations or failures such as mechanical or electrical. The NRC staff encourages licensees to report cyber security events and subsequently retract them, if appropriate (e.g., not meeting the threshold of a reportable event) rather than delaying the initial notification to gather more information and thus have greater confidence in whether or not to make a notification. If a licensee has questions about whether to report or record a cyber security event, the licensee can, if time permits, discuss the cyber security event with their appropriate NRC regional or Headquarters security staff before making an official report or record. However, if the questions cannot be resolved, licensees should report all cyber security events within the most appropriate timeframe specified in 10 CFR 73.77, rather than waiting for confirmation that the event is one that must be reported.

The NRC staff has developed this guide 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. As such, the NRC staff does not consider these lists to be 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 NRC staff notes that 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.

Harmonization with International Standards

The NRC staff reviewed guidance from the International Atomic Energy Agency (IAEA), International Organization for Standardization (ISO), and International Electrotechnical Commission (IEC) and did not identify any standards that provided useful guidance to NRC staff, applicants, or licensees.

C. STAFF REGULATORY GUIDANCE

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).

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.

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>:

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.

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.

c. A cyber attack that adversely impacted the capability to detect, delay, assess, or respond to malevolent activities. For example, a cyber attack that disrupts a security function responsible for the implementation of the site's physical protection program and/or protective strategy such as, an intrusion detection and assessment system, a physical barrier (e.g., active vehicle barrier, delay barrier), an access control system, an alarm station, or a communication system.

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

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

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.

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. 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:

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 presence of malware or unauthorized access/activity had occurred.

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 presence of malware or unauthorized access/activity had occurred to the CDA.

c. The degradation or failure of a CDA or of the cyber security controls that protect CDAs that is indicative of unauthorized activity (e.g., cyber attack, physical tampering), and 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.

d. An active cyber attack, (e.g., virus, or worm logic bomb) 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.

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), but the barrier is in the denial position and has not and will not allow unauthorized access as a result of the cyber attack.

f. Control of a mobile or portable CDA is lost or misplaced and there are signs of exploitation. For example, a CDA used for maintenance and testing is misplaced or lost, if the CDA is recovered and shows signs of tampering (e.g., physical tampering, malware installed, etc.) or CDAs that are maintained and tested by the lost or misplaced CDA show signs of exploitation (malware, unauthorized access/activity, etc.).

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.

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:

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).

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).

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.

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.

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

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).

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.

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

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 system, component or cyber security control 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.

<u>24-hour Recordable Event Examples</u>:

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

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).

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.

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.

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).

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).

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).

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 the Cyber Security Incident Response Team (CSIRT). After ensuring safe and secure operations of the plant, a member of the CSIRT (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.

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 4.3 below on documenting retractions.

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.

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.

3.7 Content of Notifications

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

a. caller name and callback number,

b. facility name and location,

c. emergency classification (if declared),

d. current event status (e.g., in progress, recovered),

e. event date and time (discovery of, and actual occurrence if known),

f. event description including the following information if available or known:

(1) cyber security controls involved/affected (if any)
(2) system(s) involved/affected (SSEP functions, BOP functions, CDAs, CS)
(3) method used to identify the event (e.g., security controls, audit, failed equipment)
(4) what occurred during the event
(5) why the event occurred, if known
(6) how the event occurred, if known

g. safety, security, EP responses and corrective actions taken,

h. offsite assistance (e.g., requested or not requested, arrived, status),

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

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

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.

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.

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 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.

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.

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.

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.

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.

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:

a. date and time of the event, including chronological timeline, if applicable,

b. date and time of notification to the NRC, and/or local, State and Federal agencies,

c. the reactor's operating mode at time of event (e.g., shut down, operating),

d. SSEP functions directly or indirectly affected by the event (e.g., compromised, failed, degraded),

e. support systems or equipment directly or indirectly affected that could have compromised SSEP functions (e.g., compromised, failed, degraded),

f. CDAs and/or CS affected by the event (compromised, failed, degraded),

g. security controls involved in the event (e.g., compromised, performed as intended),

h. 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),

i. 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),

j. immediate actions taken in response to the event and any compensatory measures established,

k. description of media interest and press releases,

l. indications or records of previous similar events,

m. procedural or human errors or equipment failures, as applicable,

n. 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),

o. corrective actions taken or planned, including dates of completion,

p. name and phone number of a licensee's point of contact,

q. 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:

    (1) description of failed, degraded, or vulnerable equipment, systems or controls (e.g., manufacturer and model number, procedure number),
    (2) 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),
    (3) security settings/configuration of the components, systems or controls that failed, or became degraded or vulnerable,
    (4) apparent cause of component, system or control failure, degradation, or vulnerability.

5. 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.

D. IMPLEMENTATION

The purpose of this section is to provide information on how applicants and licensees[1] may use this guide and information regarding the NRC's plans for using this regulatory guide. In addition, it describes how the NRC staff complies with 10 CFR 50.109, "Backfitting" and any applicable finality provisions in 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants."

Use by Applicants and Licensees

Applicants and licensees may voluntarily[2] use the guidance in this document to demonstrate compliance with the underlying NRC regulations. Methods or solutions that differ from those described in this regulatory guide may be deemed acceptable if they provide sufficient basis and information for the NRC staff to verify that the proposed alternative demonstrates compliance with the appropriate NRC regulations. Current licensees may continue to use guidance the NRC found acceptable for complying with the identified regulations as long as their current licensing basis remains unchanged.

Licensees may use the information in this regulatory guide for actions which do not require NRC review and approval such as changes to a facility design under 10 CFR 50.59, "Changes, Tests, and Experiments." Licensees may use the information in this regulatory guide or applicable parts to resolve regulatory or inspection issues.

Use by NRC Staff

The NRC staff does not intend or approve any imposition or backfitting of the guidance in this regulatory guide. The NRC staff does not expect any existing licensee to use or commit to using the guidance in this regulatory guide, unless the licensee makes a change to its licensing basis. The NRC staff does not expect or plan to request licensees to voluntarily adopt this regulatory guide to resolve a generic regulatory issue. The NRC staff does not expect or plan to initiate NRC regulatory action which would require the use of this regulatory guide. Examples of such unplanned NRC regulatory actions include issuance of an order requiring the use of the regulatory guide, requests for information under 10 CFR 50.54(f) as to whether a licensee intends to commit to use of this regulatory guide, generic communication, or promulgation of a rule requiring the use of this regulatory guide without further backfit consideration.

During regulatory discussions on plant specific operational issues, the staff may discuss with licensees various actions consistent with staff positions in this regulatory guide, as one acceptable means of meeting the underlying NRC regulatory requirement. Such discussions would not ordinarily be considered backfitting even if prior versions of this regulatory guide are part of the licensing basis of the facility. However, unless this regulatory guide is part of the licensing basis for a facility, the staff may not represent to the licensee that the licensee's failure to comply with the positions in this regulatory guide constitutes a violation.

If an existing licensee voluntarily seeks a license amendment or change and (1) the NRC staff's consideration of the request involves a regulatory issue directly relevant to this new or revised regulatory guide and (2) the specific subject matter of this regulatory guide is an essential consideration in the staff's

---

[1] In this section, "licensees" refers to licensees of nuclear power plants under 10 CFR Parts 50 and 52; and the term "applicants," refers to applicants for licenses and permits for (or relating to) nuclear power plants under 10 CFR Parts 50 and 52, and applicants for standard design approvals and standard design certifications under 10 CFR Part 52.

[2] In this section, "voluntary" and "voluntarily" means that the licensee is seeking the action of its own accord, without the force of a legally binding requirement or an NRC representation of further licensing or enforcement action.

determination of the acceptability of the licensee's request, then the staff may request that the licensee either follow the guidance in this regulatory guide or provide an equivalent alternative process that demonstrates compliance with the underlying NRC regulatory requirements. This is not considered backfitting as defined in 10 CFR 50.109(a)(1) or a violation of any of the issue finality provisions in 10 CFR Part 52.

Additionally, an existing applicant may be required to comply with new rules, orders, or guidance if 10 CFR 50.109(a)(3) applies.

If a licensee believes that the NRC is either using this regulatory guide or requesting or requiring the licensee to implement the methods or processes in this regulatory guide in a manner inconsistent with the discussion in this Implementation section, then the licensee may file a backfit appeal with the NRC in accordance with the guidance in NUREG-1409, "Backfitting Guidelines," (Ref. 8) and the NRC Management Directive 8.4, "Management of Facility-Specific Backfitting and Information Collection" (Ref. 9).

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".

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).

Compromise Loss of confidentiality, integrity, or availability of data or system function.

Critical digital asset (CDA) A subcomponent of a critical system that consists of or contains a digital device, computer or communication system or network.

Critical system (CS) An analog or digital technology based system in or outside of the plant that performs or is associated with a safety-related, important-to-safety, security, or emergency preparedness function. These critical systems include, but are not limited to, plant systems, equipment, communication systems, networks, offsite communications, or support systems or equipment, that perform or are associated with a safety-related, important-to-safety, security, or emergency preparedness function.

Cyber attack The manifestation of either physical or logical (i.e., electronic or digital) threats against computers, communication systems, or networks that may (1) originate from either inside or outside the licensee's facility, (2) have internal and external components, (3) involve physical or logical threats, (4) be directed or non-directed in nature, (5) be conducted by threat agents having either malicious or non-malicious intent, and (6) have the potential to result in direct or indirect adverse effects or consequences to critical digital assets or critical systems. This includes attempts to gain unauthorized access to a CDA and/or CS's services, resources, or information, the attempt to compromise a CDA and/or CS's integrity, availability, or confidentiality or the attempt to cause an adverse impact to a SSEP function. Further background on cyber attacks which are up to and including DBT can be found in Sections 1.1(c), 1.2, and 1.5 of Regulatory Guide 5.69, and the cyber attack may occur individually or in any combination.

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 A departure from normal operations or conditions that, if accomplished, would result

normal operation	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[3]

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.

[3] 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.