# U.S. NUCLEAR REGULATORY COMMISSION

## DRAFT REGULATORY GUIDE DG-5079

***Proposed Revision 1 to Regulatory Guide 5.83***

**Issue Date: April 2023**
**Technical Lead: Dan Warner**

# CYBERSECURITY EVENT NOTIFICATIONS

## A. INTRODUCTION

### Purpose

This regulatory guide (RG) describes an approach and methodology that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable for use by nuclear power reactor licensees when categorizing certain cybersecurity events, and the process for making notifications and submitting written security follow-up reports to the NRC for cybersecurity events.

As an alternative to the approach in RG 5.83, the NRC staff also approves for use Nuclear Energy Institute (NEI) 15-09, Revision 1, "Cyber Security Event Notifications," issued May 2022 (Ref. 1), as an acceptable method that licensees can use to meet the requirements of Title 10 of the *Code of Federal Regulations* (10 CFR) 73.77, "Cybersecurity Event Notifications" (Ref. 2).

### Applicability

This RG applies to nuclear power reactor licensees subject to 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities" (Ref. 3), or 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants" (Ref. 4).

### Applicable Regulations

- 10 CFR Part 50 provides regulations for licensing production and utilization facilities.
    - 10 CFR 50.72, "Immediate notification requirements for operating nuclear power reactors," requires each nuclear power reactor licensee to notify the NRC Headquarters Operations Center, through the Emergency Notification System (ENS), of a declaration of any of the emergency classes specified in the licensee's approved emergency plan, as well as of certain nonemergency events that occurred within three years of the date of discovery.

- 10 CFR Part 52 governs the issuance of early site permits, standard design certifications, combined licenses, standard design approvals, and manufacturing licenses for nuclear power facilities.

- 10 CFR Part 73, "Physical Protection of Plants and Materials," prescribes requirements for establishing and maintaining a physical protection system for the protection of special nuclear material at fixed sites and in transit.

    - 10 CFR 73.4, "Communications," requires licensees follow prescriptive methods for communications and reports to the NRC.

    - 10 CFR 73.21, "Protection of Safeguards Information: Performance Requirements," requires that each licensee who produces, receives, or acquires Safeguards Information ensure that it is protected against unauthorized disclosure.

    - 10 CFR 73.22, "Protection of Safeguards Information: Specific Requirements," contains specific requirements for the protection of Safeguards Information in the hands of any person subject to the requirements of § 73.21(a)(1)(i).

    - 10 CFR 73.54(a), "Protection of digital computer and communication systems and networks," requires licensees subject to the requirements of this section 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 (DBT) as described in § 73.1.

    - 10 CFR 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 of cybersecurity events, through the ENS, as described below.

    - 10 CFR 73.77(a)(1) requires licensees to notify the NRC within one hour after discovery of a cyberattack 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 impact on safety, security, or emergency preparedness (SSEP) functions within the scope of 10 CFR 73.54.

    - 10 CFR 73.77(a)(2) requires licensees to notify the NRC within four hours of the following:

        - After discovery of a cyberattack that could have caused an adverse impact on 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 whose compromise could adversely impact SSEP functions within the scope of 10 CFR 73.54.

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

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

    - 10 CFR 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 preoperational planning related to a cyberattack against digital computer and communication systems and networks within the scope of 10 CFR 73.54.

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

    - 10 CFR 73.77(c) provides the process for making cybersecurity event notifications to the NRC.

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

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

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

**Related Guidance**

- RG 5.71, "Cybersecurity Programs for Nuclear Power Reactors" (Ref. 5) provides an approach that the NRC staff deems acceptable for complying with NRC regulations regarding the protection of digital computers, communications systems, and networks from a cyberattack, which is one of the characteristics of both the DBT of radiological sabotage and the DBT of theft or diversion set forth in 10 CFR 73.1.

**Purpose of Regulatory Guides**

The NRC issues RGs to describe methods that are acceptable to the staff for implementing specific parts of the agency's regulations, to explain techniques that the staff uses in evaluating specific issues or postulated events, and to describe information that the staff needs in its review of applications for permits and licenses. Regulatory guides are not NRC regulations and compliance with them is not required. Methods and solutions that differ from those set forth in RGs are acceptable if supported by a basis for the findings required for the issuance or continuance of a permit or license by the Commission.

**Paperwork Reduction Act**

This RG provides voluntary guidance for responding to the mandatory information collections in 10 CFR Parts 50, 52, 73, and NRC Form 366 and the voluntary information collections in NRC Form 361 that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). These information

collections were approved by the Office of Management and Budget (OMB) under control numbers 3150-0011, 3150-0151, 3150-0002, 3150-0104, and 3150-0238 respectively.

Send comments regarding this information collection to the FOIA, Library, and Information Collections Branch (T6-A10M), U.S Nuclear Regulatory Commission, Washington, DC 20555 0001, or by e-mail to Infocollects.Resource@nrc.gov, and to the OMB Office of Information and Regulatory Affairs, Attn: Desk Officer for the Nuclear Regulatory Commission, 725 17th Street, NW Washington, DC 20503.; e-mail: oira_submission@omb.eop.gov.

**Public Protection Notification**

The NRC may not conduct or sponsor, and a person is not required to respond to, a collection of information unless the document requesting or requiring the collection displays a currently valid OMB control number.

# Table of Contents

# B. DISCUSSION

**Reason for Revision or Issuance**

This guide is being revised, primarily, to align the definitions in the glossary with definitions provided in recent updates to RG 5.71; to provide clarification, in the eight hour notification section, about the reportability of malicious activity against devices that reside on the same networks as critical digital assets (CDAs) or that support CDAs, consistent with 10 CFR 73.77(a)(3); and to conform to NUREG-1379, Revision 3, "NRC Editorial Style Guide" (Ref. 6). The revised RG also approves NEI 15-09, Revision 1, for use as another acceptable method for meeting the requirements of 10 CFR 73.77.

**Background**

This guide addresses requirements for cybersecurity event notifications, which help the NRC analyze the reliability and effectiveness of licensees' cybersecurity programs. Furthermore, these event notifications are important to the NRC's continuing efforts to provide high assurance that digital computer communication systems and networks are adequately protected against cyberattacks up to and including the design-basis threat.

Prompt notification could be vital in enabling the NRC to take immediate action in response to a cyberattack and, if necessary, to notify other NRC licensees, Government agencies, and critical infrastructure facilities to defend against a multiple-sector cyberattack. The NRC will use cybersecurity event notifications and written reports submitted by licensees to respond to emergencies, monitor ongoing events, assess trends and patterns, and identify precursors of more significant events. Timely notifications help the NRC achieve its strategic communication mission by enabling it to inform the U.S. Department of Homeland Security (DHS) and Federal intelligence and law enforcement agencies of cybersecurity-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' cybersecurity programs are required to provide high assurance that digital computer and communication systems and networks are adequately protected against cyberattacks, up to and including the design-basis threat of radiological sabotage as described in 10 CFR 73.1. Furthermore, 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 whose compromise would adversely impact 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 cyberattacks that would adversely impact the integrity or confidentiality of data or software; deny access to systems, services, or data; or adversely impact the operation of systems, networks, and associated equipment. Furthermore, in the staff requirements memorandum to COMWCO-10-0001, "Regulation of Cyber Security at Nuclear Power Plants," dated October 21, 2010 (Ref. 7), the Commission determined that, as a matter of policy, 10 CFR 73.54 should be interpreted to include structures, systems, and components (SSCs) in the balance of plant (BOP) that have a nexus to radiological health and safety at NRC-licensed nuclear power plants. Therefore, cybersecurity 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 10 CFR 73.77.

The NRC has established notification requirements for certain cybersecurity activities because they may indicate preoperational malevolent activities, and malevolent actors have demonstrated the capability to simultaneously attack multiple independent targets. The NRC forwards appropriate reports of these cybersecurity activities to the 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 (Ref. 8). Analysis of individual cybersecurity 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 critical infrastructure facilities. The DHS considers licensees to be "key resource owners and operators." Licensees can find additional guidance and examples of suspicious events (including events related to cyberactivity) in the DHS's "Terrorist Threats to the U.S. Homeland: Reporting Guide for Critical Infrastructure and Key Resource Owners and Operators" (Ref. 9).

Consistent with 10 CFR 73.77, a cybersecurity event must be reported within the timeframes specified in 10 CFR 73.77(a). These timeframes are given as a number of hours after, for example, discovery of a cyberattack or suspected attack. The NRC understands that the licensee may conduct a preliminary assessment if signs of a cyberattack are not obvious (e.g., antivirus protection alert, intrusion detection system alert), to rule out other common degradations or failures, such as mechanical or electrical failures. The NRC staff encourages licensees to report cybersecurity events and subsequently retract their notifications, if appropriate (e.g., if the events do not meet the threshold for reportable events), rather than delaying the initial notification in order to gather more information to determine whether to make a notification. If a licensee has questions about whether to report or record a cybersecurity event, the licensee can, if time permits, discuss the event with the appropriate NRC regional or Headquarters security staff before making an official report or record. However, if the questions cannot be resolved, the licensee should report the event within the most appropriate timeframe specified in 10 CFR 73.77, rather than wait for confirmation that the event must be reported.

The NRC staff has developed this guide based on examples taken from prior experience with cybersecurity events and with interactions between the NRC staff and licensees. This guide is intended to help licensees evaluate whether to report or record a broad range of potential cybersecurity events under 10 CFR 73.77. The specific events listed in this guide are examples of reportable or recordable cybersecurity events; the NRC staff does not consider these examples to represent an exhaustive or exclusive list of reportable or recordable cybersecurity events. Many of the examples listed herein are based on actual cybersecurity events at NRC-regulated facilities, or based on licensee discussions with NRC staff about whether a particular event was reportable, recordable, or neither. The NRC staff notes that the evaluation of cybersecurity 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 necessitate a longer or shorter 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 cybersecurity events, including those substantiated through observations by staff or law enforcement personnel, evidence of the presence of unknown persons, unauthorized access or modification of CDAs, telephone and other electronic contacts, suspicious documents and files, and testimony of credible witnesses. Licensees' 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 the routine threat bulletins and analyses that the NRC receives from the Federal Bureau of Investigation (FBI) and the DHS about critical national infrastructure and key resources. Licensees desiring PWS access should make their requests through the security staff in the applicable NRC regional office.

Notifications made under 10 CFR 73.77 should focus on the occurring or suspected cybersecurity 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 timeliness of the event notification.

**Consideration of International Standards**

The International Atomic Energy Agency (IAEA) works with member states and other partners to promote the safe, secure, and peaceful use of nuclear technologies. The IAEA has established a series of security guides to address nuclear security issues relating to the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer, or other malicious acts involving nuclear material and other radioactive substances and their associated facilities. IAEA security guides present international good practices and increasingly reflect best practices to help users achieve high levels of security. To inform its development of this RG, the NRC considered IAEA Safety Requirements and Safety Guides pursuant to the Commission's International Policy Statement, "Nuclear Regulatory Commission International Policy Statement," dated July 10, 2014 (Ref. 10), and Management Directive and Handbook 6.6, "Regulatory Guides" (Ref. 11).

The following IAEA Nuclear Security Guides were considered in the update of the RG:

- IAEA Nuclear Security Series No. 42-G, "Computer Security for Nuclear Security," issued 2021 (Ref. 12).

- IAEA Non-serial Publications, "Computer Security Incident Response Planning at Nuclear Facilities," issued 2016 (Ref. 13).

**Documents Discussed in Staff Regulatory Guidance**

In this RG, the NRC staff approves for use the guidance in NEI 15-09, Revision 1, as one method licensees can use to meet the requirements of 10 CFR 73.77. NEI 15-09, Revision 1, was prepared by an external organization and may contain references to other codes, standards, or third-party guidance documents ("secondary references"). If a secondary reference has itself been incorporated by reference into NRC regulations as a requirement, then licensees and applicants must comply with that standard as set forth in the regulation. If the secondary reference has been endorsed in an RG as an acceptable approach for meeting an NRC requirement, then the standard constitutes a method acceptable to the NRC staff for meeting that regulatory requirement as described in the specific RG. If the secondary reference has neither been incorporated by reference into NRC regulations nor endorsed in an RG, then the secondary reference is neither a legally binding requirement nor a "generic" NRC-approved acceptable approach for meeting an NRC requirement. However, licensees and applicants may consider and use the information in the secondary reference, if appropriately justified, consistent with current regulatory practice, and consistent with applicable NRC requirements.

# C. STAFF REGULATORY GUIDANCE

The NRC staff approves the guidance in NEI 15-09, Revision 1, as a method acceptable to the NRC staff for licensees to use to meet the requirements in 10 CFR 73.77.

In addition to NEI 15-09, the NRC staff provides the following guidance to licensees as a method acceptable to the NRC staff for licensees to use to meet the requirements in 10 CFR 73.77. Licensees that choose to implement the approach described in this RG or in NEI 15-09, Revision 1, should specify in their procedures that they are implementing the approach described in RG 5.83 or in NEI 15-09, Revision 1.

1. Cybersecurity Event Notifications

*10 CFR 73.77(a) states: "Each licensee subject to the provisions of § 73.54 shall notify the NRC Headquarters Operations Center via the Emergency Notification System (ENS), in accordance with paragraph (c) of this section."*

1.1 One hour Notifications

*10 CFR 73.77(a)(1) states: "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 § 73.54."*

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

1.1.2. One hour notification events include, but are not limited to, the following examples:

1.1.2.1 A cyberattack occurred that adversely impacted (e.g., interrupted) the normal operation of the facility through the unauthorized use of, or tampering with, digital computer and communication systems and networks.

1.1.2.2 A cyberattack occurred 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.

1.1.2.3 A cyberattack occurred that adversely impacted the capability to detect, delay, assess, or respond to malevolent activities.

1.1.2.3.1 For example, a cyberattack occurred that disrupted a security function involved in the implementation of the site's physical protection program 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.

1.1.2.4 A cyberattack occurred that adversely impacted the capability to call for, or communicate with, offsite assistance.

1.1.2.5 A cyberattack occurred that adversely impacted emergency response capabilities to implement appropriate protective measures in the event of a radiological emergency.

1.1.2.6 A cyberattack occurred that adversely impacted a support system 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

*10 CFR 73.77(a)(2)(i) requires licensees 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."*

1.2.1 These could be attacks exploiting a CDA, critical system (CS), or higher security level network (i.e., a network that is isolated (air gapped) or behind a data diode that contains one or more CDAs), that could have caused, but did not cause, an adverse impact on SSEP functions.

1.2.1.1 An example is an event in which activity logs, antivirus protection, or an intrusion detection system indicated the presence of malware or the occurrence of unauthorized access or activity on a CDA, CS, or higher security level network.

1.2.2 For cyberattacks that reach a lower security level network (i.e., a network that is not isolated or behind a data diode containing CDAs), or that are mitigated by boundary or CDA cybersecurity controls, or both, and in which no exploitation of a CDA occurs, a notification to the NRC is not needed under 10 CFR 73.77(a)(2)(i).

*10 CFR 73.77(a)(2)(ii) requires licensees 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 § 73.54."*

1.2.3 These attacks include those initiated by employees, contractors, or vendors having physical or electronic access to a CDA, CS, or higher security level network.

1.2.4 Attackers could include corporate information technology personnel who 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.

1.2.5 Attackers 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.

1.2.6 These attacks should be reported within four hours, regardless of their impact on SSEP functions.

*10 CFR 73.77(a)(2)(iii) requires licensees to notify the NRC within four hours "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."*

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

1.2.8 Four hour notification events include, but are not limited to, the following examples:

1.2.8.1 A CDA that was isolated or on a higher security level network was found to be connected to a lower security level network (wired or wireless), and cybersecurity controls (e.g., activity logs, antivirus protection, or an intrusion detection system) indicated the presence of malware or the occurrence of unauthorized access or activity in the CDA.

1.2.8.2 An unauthorized transmitter (e.g., wireless router, modem) or an unauthorized form of portable media (e.g., memory stick, smartphone) was attached or connected to a CDA, and cybersecurity controls (e.g., activity logs, antivirus protection, an intrusion detection system) indicated the presence of malware or the occurrence of unauthorized access or activity in the CDA.

1.2.8.3 The degradation or failure of a CDA, or of cybersecurity controls protecting CDAs, occurred that indicated unauthorized activity (e.g., cyberattack, physical tampering), and that could have caused, but did not cause, an immediate or adverse impact on SSEP functions, because, for example, the CDA had an analog backup. This does not include common degradations or failures such as mechanical or electrical failures.

1.2.8.4 An active cyberattack (e.g., a virus or worm logic bomb) occurred on a CDA, CS, or protected network that could have caused, but did not cause, an adverse impact on SSEP functions, or that could have compromised support systems and equipment whose compromise could have adversely impacted SSEP functions.

1.2.8.5 A cyberattack occurred that caused an adverse impact on the confidentiality, integrity, or availability of a CDA or CS that could have caused, but did not cause, an adverse impact on SSEP functions or that could have compromised support systems and equipment whose compromise could have adversely impacted SSEP functions.

1.2.8.5.1 For example, a remote digital control to an active vehicle barrier was disabled (e.g., causing loss of communications), but the barrier was in the denial position, so that the cyberattack did not lead to, and could not have led to, unauthorized access.

1.2.8.6 Control of a mobile or portable CDA was lost, or the CDA was misplaced, and there were signs of exploitation.

1.2.8.6.1 For example, a CDA used for maintenance and testing was misplaced or lost, and upon recovery, either the CDA itself showed signs of tampering (e.g., physical tampering, installation of malware), or other CDAs maintained and tested by the lost or misplaced CDA showed signs of exploitation (e.g., malware, unauthorized access or activity).

1.3 Eight hour Notifications

*10 CFR 73.77(a)(3) state; "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 § 73.54."*

1.3.1 Generally, eight hour notifications should include behavior, activities, or statements that are coordinated or targeted.

1.3.1.1 Only information deemed to be credible by security personnel should be considered reportable in accordance with the requirements of 10 CFR 73.77(a)(3).

1.3.2 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.

1.3.3 Eight hour notification events include, but are not limited to, the following examples:

1.3.3.1 Personnel or persons displayed an uncommon level of interest in, or made abnormal inquiries related to specific attributes of the licensee's cybersecurity program (e.g., CDAs, CSs, cybersecurity controls) or vulnerabilities associated with the cybersecurity program. Such interests or inquiries could occur onsite or off site (e.g., at a cybersecurity symposium) by personnel, vendors, contractors, or nonemployees who do not have a need to know (e.g., who do not participate in or support the licensee's cybersecurity program). This does not include generic public or media inquiries related to plant operations, safety, and other similar topics (these inquiries are considered targeted).

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

1.3.3.3 The licensee recognized theft or suspicious loss of smart cards, tokens, or other two-factor authentication devices required for accessing a CDA or CS.

1.3.3.4 The licensee detected forged or fabricated smart cards, tokens, or other two-factor authentication devices required for accessing a CDA or CS or for performing authorization activities.

1.3.3.5 The licensee detected falsified identification badges, key cards, or other access control devices that would allow unauthorized individuals access to a CDA or CS.

1.3.3.6 A targeted spear phishing email (payload) was sent, followed by a telephone call to the targeted individual in an attempt to trigger the spear phishing email (social engineering).

1.3.3.7 The licensee recognized the exfiltration of data (intelligence-gathering) from a lower security level network from an unknown source, in conjunction with malware (payload) that was surreptitiously delivered and executed by the unknown source without licensee knowledge.

1.3.3.8 A website posting or notification indicated a planned cyberattack against the plant.

1.3.3.9 Malicious activity observed against devices residing on the same network as a CDA, such as on a boundary device protecting a network containing a CDA, or against devices that support CDAs, such as devices with monitoring and alerting functions (e.g., portable media scanning kiosks, security incident event monitoring systems, intrusion detection systems, or centralized logging systems). The malicious activity provided credible evidence of intelligence-gathering or preoperational planning that could affect the CDA.

1.3.3.10 The recognition of malicious activity observed on CDA monitoring, reporting, and alerting systems on higher security level or lower security level networks.

1.4 Twenty-Four hour Recordable Events

*10 CFR 73.77(b) states: "The licensee shall use the site corrective action program to record vulnerabilities, weaknesses, failures and deficiencies in their § 73.54 cyber security program within twenty-four hours of their discovery."*

1.4.1 This includes items or events such as the following:

1.4.1.1 A system, component, or cybersecurity control has been reduced to the degree that it is rendered ineffective for its intended purpose (e.g., it has ceased to function properly).

1.4.1.2 A defect in equipment, personnel, or procedure has degraded the functioning or performance of the cybersecurity program necessary to meet the requirements of 10 CFR 73.54.

1.4.1.3 A feature or attribute has been detected 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.

1.4.2 Licensees should use the site CAP to perform periodic evaluations to identify any noticeable trends or increases in failures and deficiencies in their cybersecurity program (e.g., equipment vulnerabilities and failures, procedural or training weaknesses and deficiencies), to help identify and develop program improvements.

1.4.3 Twenty-four hour recordable events include, but are not limited to, the following examples:

1.4.3.1 A cyber vulnerability assessment was not performed within the period specified in the licensee's cybersecurity plan (e.g., quarterly).

1.4.3.2 Improper usage occurred of digital computer and communication systems and networks associated with SSEP functions, or of support systems and equipment whose compromise could adversely impact SSEP functions. This could include training and procedure deficiencies involving a CDA, cybersecurity controls, or SSEP functions that did not adversely impact their function (e.g., connection of unauthorized portable media to a CDA which resulted in no exploitation—for example, no malware was transferred, and no unauthorized activity or access occurred).

1.4.3.3 A design flaw or vulnerability was detected in an implemented cybersecurity control that could have allowed unauthorized access to a CDA, or could have 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., if a licensee scan discovers a vulnerability that has not been previously identified in cybersecurity hardware or software). Note: If a licensee believes that the vulnerability or design flaw could pose an industrywide risk, the licensee should consider immediate notification using the voluntary notification process, so that the NRC can notify other licensees of the vulnerability or design flaw.

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

2 Notification Process

*10 CFR 73.77(c) requires licensees to make notifications required by 10 CFR 73.77(a) to the NRC Headquarters Operations Center through the ENS.*

2.01 If the ENS is inoperative or unavailable, the licensee must make the notification by commercial telephone service or other dedicated telephonic system, or by any other method that will ensure that the NRC Headquarters Operations Center receives the report within the specified timeframe.

- Appendix A to 10 CFR Part 73 provides commercial telephone numbers for the NRC Headquarters Operations Center. Notifications can be annotated on an "Event Notification Worksheet" (NRC Form 361).
- Licensees may obtain an event number and time during notifications.
- If a licensee event report (LER) is required, the licensee may include the event number and time in the LER to provide a cross-reference- to the notification, making the event easier to trace.

2.02 The individual responsible for making the notification should be properly trained and sufficiently knowledgeable about the event to report it correctly.

2.03 The NRC records all conversations with the NRC Headquarters Operations Center. The recordings are saved for 1 month in case there is a public or private inquiry.

2.04 If needed, licensees should make additional notifications to the NRC Headquarters Operations Center describing substantive changes, additions, or modifications to the initial notification in a timely manner, after taking immediate action to protect the facility or stabilize operations, in accordance with emergency and contingency response procedures.

2.05 More than one event can be reported in a single ENS notification 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; unrelated events should not be reported in a single LER. However, multiple notifications may be addressed in a single telephone call.

2.06 Discussion of an event requiring notification under 10 CFR 73.77 with the NRC staff (e.g., with a resident inspector) does not constitute the required notification to the NRC Headquarters Operations Center. Nor does the 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).

2.1 Notifications Containing Safeguards Information

2.1.1 Under 10 CFR 73.22(f)(3), for cybersecurity events specified in 10 CFR 73.77, which are considered to be extraordinary conditions, licensees may make notifications containing safeguards information to the NRC Headquarters Operations Center without using a secure communication system. Licensees should not delay notification of such events beyond one hour after discovery to wait for secure means of communication. However, if available, the licensee should use a secure communication system to make the notification in order to protect the safeguards information in the report from unintentional or inadvertent disclosure. Licensees should apply this exception to actual events only. In particular, they should not apply it 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).

2.2 Notifications Containing Classified Information

*10 CFR 73.22(f)(3) states: "Except under emergency or extraordinary conditions, Safeguards Information shall be transmitted outside an authorized place of use or storage only by NRC approved secure electronic devices, such as facsimiles or telephone devices, provided that transmitters and receivers implement processes that will provide high assurance that Safeguards Information is protected before and after the transmission or electronic mail through the internet, provided that the information is encrypted by a method (Federal Information Processing Standard [FIPS] 140–2 or later) approved by the appropriate NRC Office; the information is produced by a self contained secure automatic data process system; and transmitters and receivers implement the information handling processes that will provide high assurance that Safeguards Information is protected before and after transmission. Physical security events required to be reported pursuant to § 73.1200 are considered to be extraordinary conditions. Cyber security event notifications required to be reported pursuant to § 73.77 are considered to be extraordinary conditions."*

2.2.1 Licensees making notifications under 10 CFR 73.77 that contain classified national security information (NSI) or restricted data (RD) must notify the NRC Headquarters Operations Center using a secure communication system equivalent (at a minimum) to the classification level of the notification.

2.2.1.1 Licensees making classified notifications must contact the NRC Headquarters Operations Center at the commercial telephone numbers specified in Appendix A to 10 CFR Part 73 and request a number to a secure telephone.

2.2.1.2 If the licensee's secure communications capability is unavailable (e.g., because of the nature of the event), the licensee must provide as much information to the NRC as required by 10 CFR 73.77, without revealing or discussing any classified information.

2.2.1.3 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.

2.2.2 If the nature of the cybersecurity event warrants, NRC Emergency Response Management may direct the licensee to use any available nonsecure communications method to immediately communicate classified information to the NRC (in relation to cybersecurity event notifications required by 10 CFR 73.77).

2.2.2.1 If so directed, the licensee should provide the classified information to the NRC over the best available nonsecure system (for example, the NRC staff considers a nonsecure landline preferable to a nonsecure cellular or satellite system).

2.2.3 In the written security follow-up report for the classified cybersecurity event notification over nonsecure 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 nonsecure communication system.

2.2.3.1 The licensee should appropriately mark and classify the written security follow-up report.

2.2.3.2 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 nonsecure communications, in accordance with Executive Order 13526, "Classified National Security Information," dated December 29, 2009 (Ref. 14).

2.3 Continuous Communications

2.3.1 For some cybersecurity event notifications made 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 Operations Center.

2.3.2 Human-to-human communication may be beneficial in facilitating follow-up questions and clarifications, requests for information or actions, and NRC response activities.

2.3.3 Note: Because notifications must be made within specified timeframes "after discovery of" an event, the NRC realizes that the initial notification may be made by an individual not knowledgeable about cyber-related activities.

2.3.4 However, a cybersecurity event requiring notification to the NRC should prompt activation of the Cyber Security Incident Response Team (CSIRT).

2.3.5 After ensuring safe and secure plant operations, a member of the CSIRT (i.e., an individual who is knowledgeable about cyber-related activities as well as the current cybersecurity event) should follow up with the NRC after the initial notification if there are any additions or modifications to the initial notification.

2.4 Retraction of Notifications

2.4.1 Licensees desiring to retract a previous notification of a cybersecurity event that they have determined (through analysis or investigation) to be nonreportable (e.g., an event that does not meet the threshold for 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.

2.4.2 Cybersecurity 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 on documenting retractions in Section 3.3, "Retraction of Previous Written Security Follow-Up Reports" of this RG.

2.5 Declaration of Emergencies

2.5.1 A licensee reporting a cybersecurity event under 10 CFR 73.77 that also involves the declaration of an Emergency Classification (e.g., a Notification of Unusual Event (NOUE), Alert, Site Area Emergency, or General Emergency), in accordance with its NRC-approved emergency response plan, should follow the appropriate regulations for the declaration of an emergency.

2.5.1.1 In other words, emergency declarations have primacy over cybersecurity event notifications.

2.5.1.2 To reduce unnecessary burden and duplication, licensees should make a single report of any events that require both emergency response and cybersecurity event notifications.

2.5.1.3 The notification should indicate all of the applicable reporting requirements for the event.

2.5.1.4 However, a licensee may need to report additional information regarding a cybersecurity event that would not be included in an emergency response notification.

2.6 Elimination of Duplication

2.6.1 Licensees are not required to make separate notifications for cybersecurity events that also result in the declaration of an emergency.

2.6.1.1 In such circumstances, licensees should make the emergency notifications in accordance with existing regulations (e.g., 10 CFR 50.72).

2.6.2 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 the NRC's reporting regulations.

2.6.3 When making a notification, the licensee should indicate to the NRC that the notification is also to report a cybersecurity event under a specific paragraph of 10 CFR 73.77.

2.7 Content of Notifications

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

- caller name and callback number,

- facility name and location,
- emergency classification (if declared),
- current event status (e.g., in progress, recovered),
- event date and time (date and time of discovery of event, and of actual occurrence if known),
- event description, including the following information if available:
    - cybersecurity controls involved/affected (if any),
    - systems involved/affected (SSEP functions, BOP functions, CDAs, CSs),
    - method used to identify the event (e.g., security controls, audit, failed equipment),
    - what occurred during the event,
    - why the event occurred, if known, and
    - how the event occurred, if known,
- SSEP responses and corrective actions taken,
- offsite assistance (e.g., requested or not requested, arrived, status),
- media interest, if any, including licensee-issued press releases, and
- source of information (e.g., U.S. Computer Emergency Readiness Team, law enforcement); if a law enforcement agency, the contact telephone number should be provided.

2.8 Voluntary Notifications

2.8.1 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.

2.8.1.1 Assurance of safe operation of all plants depends on accurate and complete reporting by each licensee of all events having potential safety or security significance.

2.8.1.2 For example, a cyber-related event or condition affecting the licensee's corporate or business network, even if identified and mitigated with no impact on SSEP functions, may indicate a recently identified or known cyber threat.

2.8.1.3 Such activities should be voluntarily reported to the NRC to support Federal situational awareness activities.

2.8.2 Licensees may make voluntary ENS notifications about cyber-related events or conditions that the licensee believes might interest the NRC.

2.8.2.1 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.

2.8.2.2 If it is later determined that the event is reportable, the licensee can change the voluntary ENS notification to a required notification under the appropriate 10 CFR 73.77 reporting criterion without adverse consequences, as long as the voluntary report was submitted within the appropriate timeframe and provided the information necessary for the required notification.

2.8.2.3 Voluntary notifications do not require a written security follow-up report, unless the event is later determined to be reportable under 10 CFR 73.77 reporting criteria.

3 Written Security Follow-Up Reports

3.0.1 Telephonic notifications to the NRC Headquarters Operations Center for the cybersecurity events specified in 10 CFR 73.77(a)(1), (a)(2)(i), and (a)(2)(ii) 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, "Communications," when submitting a follow-up report.

- The NRC does not require licensees who have made a notification to the NRC Headquarters Operations Center for cybersecurity events specified in 10 CFR 73.77(a)(2)(iii) and (a)(3) to submit written security follow-up reports.

- In addition, cybersecurity events recorded in the site CAP under 10 CFR 73.77(b) do not require written security follow-up reports.

3.0.2 The format and quality of written security follow-up reports should allow for legible reproduction and processing.

- A written security follow-up report should contain sufficient detail, information, and analysis to enable a knowledgeable individual to understand what occurred during the event.

- For example, the report should specify whether any administrative or technical errors occurred, what equipment was involved, malfunctioned, or both; what CDAs, SSEP functions, or both were affected; whether the event involved the installation of new hardware or software (including patches and updates); and whether the event resulted from changes in system settings or configuration.

- Additionally, the licensee should indicate any immediate corrective actions that were taken (including 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 3 years or until the termination of the license, whichever comes first.

3.1 NRC Forms 366 and 366A

3.1.1 Nuclear power reactor licensees must prepare any written security follow-up reports required by 10 CFR 73.77 using NRC Form 366, "Licensee Event Report (LER)." They may use NRC Form 366A, "Licensee Event Report Continuation Sheet," if additional pages are needed.

3.1.2 Licensees using NRC Form 366 should complete items 1–15 as labeled (if known or applicable).

- For example, for item 1, the licensee should enter the name of the facility (e.g., Indian Point, Unit 1) at which the event occurred.

- For item 11, the licensee should check the block that indicates the appropriate requirement (e.g., 10 CFR 73.77(a)(1)).

- If submitting a voluntary LER, the licensee should check the "Other" block and indicate "voluntary report" in the space below.

- For item 16, "Abstract," the licensee should briefly describe the cyber event, including any failures or degradations that contributed to the event (e.g., user error, procedure violation, failures in cybersecurity controls), any affected CDAs and SSEP functions, and the extent to which these CDAs and SSEP functions were impacted. (For example, remote (digital) control of the protected area active vehicle barrier system was temporarily lost because of a bad firmware update; barriers were in the up position and were controlled manually until previous firmware was reloaded; no unauthorized access occurred during this event.)

3.1.3 NRC Form 366A should be used to provide additional details about the cybersecurity event, including the content requested in Section 3.6, "Content of Written Security Follow-Up Reports" of this RG.

3.1.4 Generally, the NRC will make licensee-submitted LERs publicly available.

3.1.4.1 However, information designated by the licensee as, for example, proprietary, safeguards, or classified information will be withheld (redacted) from the public, as appropriate.

3.1.4.2 Licensees should create, store, mark, label, handle, and transmit LERs in accordance with applicable NRC regulations (e.g., 10 CFR 2.390, "Public inspections, exemptions, requests for withholding" (Ref. 15); 10 CFR 73.21, "Protection of Safeguards Information: performance requirements"; 10 CFR 73.22, "Protection of Safeguards Information: specific requirements"; or 10 CFR Part 95, "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data" (Ref. 16)).

3.1.4.3 When providing designated information (e.g., proprietary, safeguards, or classified information) with the LER, licensees should enter it only in item 17, "Narrative," of NRC Form 366A, and not include it on NRC Form 366.

3.1.4.4 The text should clearly indicate what information is designated as proprietary, safeguards, classified, etc.

3.2 Significant Supplemental Information and Correction of Errors

3.2.1 Licensees that discover significant supplemental information after submitting a written security follow-up report to the NRC must submit a revised written report, following the same process as used to submit the initial written report.

3.2.2 Additionally, licensees that discover errors in a written report previously submitted to the NRC must submit a revised written report, following the same process as used to submit the initial written report.

3.2.3 A revised written report must replace the previous written report (i.e., the revised report must be complete and not be limited to only the supplementary or updated information).

3.2.4 The revised report should indicate the revision number, with revision bars, to assist the reader.

3.3 Retraction of Previous Written Security Follow-Up Reports

3.3.1 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.

3.3.2 However, if the licensee has already submitted a written security follow-up report to the NRC before retracting the notification, the licensee must then submit a revised written report to the NRC indicating that the initial event has been retracted and giving the basis for that retraction.

3.3.3 This supplemental written security follow-up report (retracting the notification) 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.

3.4 Written Security Follow-Up Reports Containing Safeguards Information

3.4.1 Licensees that submit written security follow-up reports to the NRC containing safeguards information must create, store, mark, label, handle, and transmit these written reports in accordance with the requirements in 10 CFR 73.21 and 10 CFR 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.

3.5 Written Security Follow-Up Reports Containing Classified Information

3.5.1 Licensees that submit written security follow-up reports to the NRC containing classified NSI or RD must 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."

3.5.2 Licensees should perform a derivative classification of such reports in accordance with the classification guide(s) applicable to their facility or activity.

3.5.3 Written security follow-up reports should be portion marked to indicate the classification level of the report's information.

3.5.4 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.

3.6 Content of Written Security Follow-Up Reports

*10 CFR 73.77(d)(5) states: "The written security follow-up report must include sufficient information for NRC analysis and evaluation."*

3.6.1 The NRC staff recommends that written security follow-up reports contain, at a minimum, the following information, as applicable:

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

3.6.1.2 date and time of notification to the NRC or local, State, or Federal agencies, or a combination of these,

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

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

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

3.6.1.6 CDAs, CSs, or both affected by the event (e.g., compromised, failed, degraded),

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

3.6.1.8 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),

3.6.1.9 method of discovery of the event or information, such as routine patrol or inspection, test, maintenance, alarm annunciation, audit, communicated threat, or unusual circumstances (include details),

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

3.6.1.11 description of media interest and press releases,

3.6.1.12 indications or records of previous similar events,

3.6.1.13 procedural or human errors or equipment failures, as applicable,

3.6.1.14 cause of the event, or licensee's analysis of the event (including a brief summary in

the report, with references to any ongoing or completed detailed investigations, assessments, analyses, or evaluations),

3.6.1.15 corrective actions taken or planned, including dates of completion, and

3.6.1.16 name and phone number of a licensee point of contact.

3.6.2 For failures, degradations, or discovered vulnerabilities of the cybersecurity program, licensees should provide the following information, as applicable, in addition to items 3.6.1.1 through 3.6.1.16 above:

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

3.6.2.2 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),

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

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

4 Training of Nonsecurity Staff on Reporting and Recording Requirements

4.1 Licensees should not limit the discovery or identification of reportable or recordable events to members of the licensee's security organization.

4.1.1 Employees, contractors, and vendors with physical or electronic access to digital computer and communication systems and networks within the scope of 10 CFR 73.54 should receive training on cybersecurity event notifications. Such training will foster awareness and help employees, contractors, and vendors understand their responsibility to immediately notify site security or management personnel of anomalies, failures, degradations, or vulnerabilities in the cybersecurity program, including activities that may indicate intelligence-gathering or preoperational planning related to cyberattacks.

4.2 Licensees may provide this training during general plant training and periodic refresher training.

4.3 Licensees may find 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 NRC staff may use this regulatory guide as a reference in its regulatory processes, such as licensing, inspection, or enforcement. However, the NRC staff does not intend to use the guidance in this regulatory guide to support NRC staff actions in a manner that would constitute backfitting as that term is defined in 10 CFR 50.109, "Backfitting," and as described in NRC Management Directive 8.4, "Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests," (Ref. 17), nor does the NRC staff intend to use the guidance to affect the issue finality of an approval under 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants."

The staff also does not intend to use the guidance to support NRC staff actions in a manner that constitutes forward fitting as that term is defined and described in Management Directive 8.4. If a licensee believes that the NRC is using this regulatory guide in a manner inconsistent with the discussion in this Implementation section, then the licensee may file a backfitting or forward fitting appeal with the NRC in accordance with the process in Management Directive 8.4.

# GLOSSARY

This glossary is intended to help the reader implement this guide to meet the requirements set forth in 10 CFR 73.77, "Cyber security event notifications." Definitions for certain security terms are also found in 10 CFR 73.2, "Definitions."

**access control** The control of entry to, or use of, all or part of any physical, functional, or logical component of a critical digital asset (CDA).

**adverse impact** A direct deleterious effect: on safety-related, important-to-safety, security, or emergency preparedness functions; on the operation of systems, networks, and associated equipment; or on the integrity and confidentiality of data and software. Examples include: loss or impairment of function; reduction in reliability; reduction in ability to detect, delay, assess, or respond to malevolent activities; reduction in the ability to call for or communicate with offsite assistance; or reduction in emergency response ability to implement appropriate protective measures in the event of a radiological emergency. If 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 does not result in radiological sabotage (i.e., if it causes the system to actuate properly in response to established parameters and thresholds), this is not considered an adverse impact, in accordance with 10 CFR 73.54(a)(2).

**compromise** A change to the state of a hardware, software, or firmware asset such that it performs outside of the intended functionality due to a loss of confidentiality, integrity, or availability of data, configuration, settings, or system function; alteration of existing functionality; or introduction of new functionality.

**credible** Describes information that either has been verified to be true, or has been received from a source determined to be reliable (e.g., law enforcement, a government agency, or the U.S. Computer Emergency Readiness Team). A threat or vulnerability can be verified to be true or considered credible when (1) evidence supporting the threat or vulnerability exists, (2) information independent from the actual threat message or vulnerability exists that supports the threat or vulnerability, or (3) a specific known group or organization claims responsibility for the threat or vulnerability.

**critical digital asset (CDA)** A digital computer, communication system, or network that is one of the following:

- a component of a critical system (this includes assets that perform safety, security, or emergency preparedness (SSEP) functions, or that support, protect, or provide a pathway to critical systems); or
- a support system asset whose failure or compromise as the result of a cyberattack would result in an adverse impact to an SSEP function.

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

| | |
|---|---|
| | with a safety-related, important-to-safety, security, or emergency preparedness function. |
| **cyberattack** | Any event in which there is reason to believe that an adversary has committed or caused, or has attempted to commit or cause, an adverse impact on a safety-related, important-to-safety, security, or emergency preparedness function. |
| **higher security level network** | A digital network that is air gapped or behind a data diode that contains one or more CDAs. |
| **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 be 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 standby mode but would need to operate if called upon in an abnormal or emergency situation. Section 236 of the Atomic Energy Act of 1954, as amended (42 USC 2284), treats as sabotage the knowing "interruption of normal operation of any [nuclear] facility through the unauthorized use of or tampering with the machinery, components, or controls of any such facility," or any attempt or conspiracy to do such an act. |
| **malware** | Malicious software designed for infiltrating or damaging a digital device, without a licensee's consent; software or firmware intended to perform an unauthorized process to adversely impact the confidentiality, integrity, or availability of a system or function; or a virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malware. |
| **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. |
| **recovery** | Steps taken to restore a system, function, or device to its original state of operation after a catastrophic or partial loss of functionality, or after a challenge to an original state of operation by either an event (such as a cyberattack) or an 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 by impersonating authorized functions or personnel. |
| **tampering (cyber)** | Altering, disabling, or damaging digital computer or communication systems or networks, or cybersecurity controls, for improper purposes or in an improper manner. |

# REFERENCES [1]


1 Nuclear Energy Institute (NEI), 15-09, "Cyber Security Event Notifications," Revision 1, Washington, DC, May 2022.

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

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

4 CFR, "Licenses, Certifications, and Approvals for Nuclear Power Plants," Part 52, Chapter I, Title 10, "Energy."

5 NRC, RG 5.71, "Cybersecurity Programs for Nuclear Power Reactors," Washington, DC.

6 NRC, NUREG-1379, "NRC Editorial Style Guide," Washington, DC.

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

8 Cybersecurity & Infrastructure Security Agency (CISA), Department of Homeland Security (DHS), "National Cyber Incident Response Plan (NCIRP)," December 2016, Washington, DC, can be found at https://www.cisa.gov/resources-tools/resources/national-cyber-incident-response-plan-ncirp.

9 CISA, DHS, "Terrorist Threats to the U.S. Homeland: Reporting Guide for Critical Infrastructure and Key Resource Owners and Operators," Washington, DC, January 24, 2005 (ML112280232).

10 NRC, "Nuclear Regulatory Commission International Policy Statement," *Federal Register*, Vol. 79, No. 132, July 10, 2014, pp. 39415–39418.

11 NRC, Management Directive 6.6, "Regulatory Guides," Washington, DC.


---

1 Publicly available NRC published documents are available electronically through the NRC Library on the NRC's public website 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 email pdr.resource@nrc.gov.

Publications from Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency are available at the CISA.gov website, or by contracting CISA, 245 Murray Lane, Washington DC, 20528 phone: 888-282-0870.

Publications from the Nuclear Energy Institute (NEI) are available at the NEI website, http://www.nei.org, or by contacting the headquarters at Nuclear Energy Institute, 1776 I Street NW, Washington DC 20006; phone: 202-739-800; fax: 202-785-4019.

Publications from International Atomic Energy Agency (IAEA) are available at the IAEA website, https://www.iaea.org/publications, or by contacting IAEA, PO Box 100, 1400 Vienna, Austria, (43-1) 2600-0.

12 IAEA Nuclear Security Series No. 42 G, "Computer Security for Nuclear Security," 2021, Vienna, Austria, can be found at https://www.iaea.org/publications/13629/computer-security-for-nuclear-security.

13 IAEA Non serial Publications, "Computer Security Incident Response Planning at Nuclear Facilities," 2016, Vienna, Austria, can be found at https://www.iaea.org/publications/10998/computer-security-incident-response-planning-at-nuclear-facilities.

14 Executive Order 13526, "Classified National Security Information," December 29, 2009, issued in *Federal Register*, Vol. 75, No. 2, January 5, 2010, pp. 707–731.

15 CFR, "Agency Rules of Practice and Procedure," Part 2, Chapter I, Title 10, "Energy," Section 390, "Public inspections, exemptions, requests for withholding."

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

17 NRC, Management Directive 8.4, "Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests," Washington, DC.