NUCLEAR ENERGY INSTITUTE

David R. Kline
DIRECTOR, SECURITY
NUCLEAR GENERATION DIVISION

2/3/2011
76 FR 6086

(3)

August 2, 2011

Mr. Philip G. Brochman
Senior Program Manager
Division of Security Policy
Office of Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Industry Comments on 10 CFR Part 73 Proposed Rulemaking on Enhanced Weapons, Firearms Background Checks and Security Event Notifications (*Federal Register 76 FR 6200, 76 FR 6085, 76 FR 6086 and 76 FR 6087*) Docket ID NRC–2011–0018

Project Code: 689

Dear Mr. Brochman:

The Nuclear Energy Institute (NEI)[1] appreciates the opportunity to comment on the subject rulemaking, associated Draft Regulatory Guides (DG) and Draft Weapons Safety Assessment. We also appreciated the opportunity to interact with the staff, Federal Bureau of Investigation and Bureau of Alcohol, Tobacco, Firearms and Explosives in a public meeting on June 1, 2011. The meeting resulted in a clearer understanding of the staff's position and intent behind the proposed rule language and associated documents.

---

[1] NEI is the organization responsible for establishing unified nuclear industry policy on matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include all utilities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect/engineering firms, fuel fabrication facilities, materials licensees, and other organizations and individuals involved in the nuclear energy industry.

SUNSI Review Complete

E-RIDS = ADM-03

1776 I Street, NW | Suite 400 | Washington, DC | 20006-3708 | P: 202.739.8174 | F: 202.533.0139 | dk@nei.org | www.nei.org

Template = ADM-013

Cc'd = R. Carpenter (rgc1)
M. Cuke (mjc)
P. Brochman (pgb)

On behalf of the industry, NEI has attached comments on 10 CFR Part 73 Proposed Rulemaking on Enhanced Weapons, Firearms Background Checks and Security Event Notifications and Associated Documents: DG-5019, Revision 1 "Reporting and Recording Safeguards Events", DG-5020 "Applying for Enhanced Weapons Authority, Applying for Exemption Authority, and Performing Firearms Background Checks Under 10 CFR Part 73" and Weapons Safety Assessment, Volume 1-5.

The industry had a few comments on the rule and DG-5020 regarding Enhanced Weapons. The majority of the industry comments are related to Reporting and Recording Safeguards Events, due largely to the immediate, significant impacts that changes to the rule language and associated regulatory guide will have on current industry operations regarding event notifications, without a clear benefit. Comments on "Reporting and Recording Safeguards Events" are being submitted as part of Enhanced Weapons Rulemaking in accordance with the *Federal Register* notice. However, it is the industry's position that proposed changes to "Reporting and Recording Safeguards Events" and Proposed Rulemaking on Enhanced Weapons are two entirely separate areas. Thus, any rulemaking on "Reporting and Recording Safeguards Events" should be addressed separately, using a risk-informed graded approach that considers the differences between the facilities subject to the reporting requirements (e.g. reactors and fuel cycle facilities). The fact that proposed changes to "Reporting and Recording Safeguards Events" were issued under Proposed Rulemaking on Enhanced Weapons caused significant confusion throughout the industry.

If NRC decides to move forward to address these separate issues in the single rulemaking, the industry is providing comments that clarify the term "discovery" and suggest modifications to the reporting requirements defined within the proposed rule and DG-5019 that will improve the efficiency and effectiveness of event reporting and eliminate redundant requirements. Industry recognizes and appreciates the need for timely reporting of security events to the NRC. However, industry considers "discovery" to have occurred after the initial event has been observed, appropriate internal notifications made, and a licensee determination made that the event meets the applicable reporting requirements. We recognize that for many events and most conditions, the time of "discovery" begins when a cognizant individual such as a manager, supervisor for the security function has been notified. However, for some less obvious conditions, a thorough investigation and evaluation is necessary which may lead to the discovery of a potentially reportable event. Also, the licensee's evaluation should proceed on a time scale commensurate with the security significance of the issue to ensure that both the licensee and the NRC receive a complete and accurate report of the event or condition. Therefore, the industry believes that the time of "discovery" will vary because it is event driven and should not be considered to have occurred in each case at the time that the actual event occurred or condition is initially observed.

The following language was adopted by NRC in FCSS Interim Staff Guidance-12, Revision 0, 10 CFR Part 70, Appendix A - Reportable Safety Events, which industry believes can be applied to discovery of security events within the context of this rulemaking:

"The time of discovery begins when a cognizant individual observes, identifies, or is notified of a safety significant event or condition. A cognizant individual is anyone who, by position or experience, is expected to understand that the particular condition or event adversely impacts safety. For some conditions, such as the examples shown in Table 1 and Attachment B, an investigation and evaluation is necessary and may lead to the discovery of a potentially reportable situation. This evaluation should proceed on a time scale commensurate with the safety significance of the issue." Industry is willing to work with NRC to develop appropriate examples where investigation and evaluation is necessary.

A significant amount of the comments relate to the 15-minute and 4-hour reporting criteria, requirement to maintain a safeguards event log, and event reporting as it relates to cyber security. The proposed rule and DG-5019 require licensees to notify the NRC Headquarters Operations Center as soon as possible, but not later than 15-minutes after the discovery of an imminent or actual hostile action. The industry understands the objective to provide prompt notification to NRC for this type of event, but believes that the current notification time period of "approximately 15-minutes" for security based events contained in NRC Bulletin 2005-02 "Emergency Preparedness Response for Security-Based Events" meets that objective. The examples of security events provided by the proposed rule and DG that require 15-minute notification would promptly be reported to the station control room and the event classification accomplished in a very short time period. Adding an additional reporting requirement to ensure reporting "as soon as possible, but not later than 15-minutes of the discovery of..." would increase administrative burden and could potentially result in a negative impact on a licensee's response to the event. The potential minimal increased time to accomplish the notifications in conjunction with event classification would not inhibit the effectiveness of NRC in warning other licensees and/or other stakeholders of the event.

The proposed rule and DG also presents the addition of a 4-hour and 8-hour reporting requirement for suspicious activities. The industry understands the benefit of reporting suspicious activities to the NRC in a timely manner in light of the importance of detecting pre-operational surveillance activities. The criteria in the proposed rule and DG for determining the timeframe for event reporting within 4-hours appears to be events that 1) do not result in the interruption of facility operations and 2) could prevent the implementation of the protective strategy for protecting any target set; and notifications to and responses from LLEA. The examples provided that should be reported within 4-hours would have no immediate or short-term impact on protective strategies or law enforcement response. Therefore, we are proposing that all suspicious activities be reported in a timely manner but not later than 8-hours from discovery and that the 4-hour reporting requirement be eliminated.

The industry recommends eliminating the proposed requirement to maintain a separate Safeguards Event Log (SEL). This requirement, which was implemented in 1981, was a valuable tool for tracking and trending security failures, degradations and vulnerabilities. The need for this tool for that purpose has been eliminated by use of the Corrective Action Program (CAP) as required by the

current 10 CFR Part 73 rule requirements. All issues required to be entered into the SEL are captured in the CAP; therefore, this requirement has become redundant and an administrative burden, which provides no real value.

It would appear that the reportability requirements as applied to Physical Security were applied directly to cyber security. In addition, the licensee Cyber Security Plan does not specify what represents adequate compensatory measures for the different types of discovered vulnerabilities nor the timeframe to implement these compensatory measures. Therefore, an effective determination of what constitutes compensated or uncompensated is not currently an achievable objective from a reporting perspective. No guidance exists; therefore, it is not possible to differentiate which cyber security events are reportable versus which are recordable. Therefore, the industry Cyber Security Task Force has provided information, in addition to the comments, that offer an alternate approach for reporting criteria for cyber events.

The industry requests a follow-up meeting with your staff as soon as practical to discuss the comments and proposed wording to the regulatory draft guidance and proposed rule language. Due to the need to discuss specific security compensatory measures as they relate to security events, this meeting should be closed to the public, as Safeguards Information will be discussed. We believe that this meeting will help assure the language in the final rule and regulatory guidance documents provides clear direction to the industry without the need for interpretation.

If you have questions or require additional information, please contact me at (202) 739-8174; dk@nei.org or Jerud Hanson at (202) 739-8053; jeh@nei.org.

Sincerely,

David R. Kline

c: Mr. Richard M. Costa, Jr., NSIR/DSP/RSLB, NRC
NRC Document Control Desk

Attachments

~~SECURITY-RELATED INFORMATION – WITHOLD FROM PUBLIC DISCLOSURE~~

Industry Comments – Proposed Rulemaking on Enhanced Weapons and DG 5020

EW Document/Section/ Page Reference	Comment	Suggested Wording/Revision
General Comment	The NRC proposal to impose a requirement in §73.19 for periodic firearms background checks to be completed at least once every three years is unnecessarily administratively burdensome and costly for those licensees not subject to the NRC's access authorization program background check requirements. Instead, the periodic firearms background check periodicity should be changed to at least once every five years, consistent with Section 5 of the Firearms Guidelines, while allowing licensees the flexibility to conduct these checks more frequently than every five years. This would allow those licensees not subject to the NRC's access authorization program background check requirements to synchronize the firearms background checks with DOE security clearance reinvestigations, while at the same time allowing those licensees subject to the NRC's access authorization program background check requirements to synchronize the firearms background checks with the criminal history records checks. This would allow both classes of licensees to determine how to best reduce the administrative cost and burden.	N/A
General Comment	Recommend incorporating rule language into the regulatory guide similar to DG 5019.	

Industry Comments – Proposed Rulemaking on Enhanced Weapons and DG 5020

EW Document/Section/ Page Reference	Comment	Suggested Wording/Revision
Part 73.18, Section (m)(6)	The language of this paragraph requiring that, "Security personnel shall return enhanced weapons issued from armories to the custody of the licensee or certificate holder following the completion of their official duties" could be interpreted as preventing the turnover of an enhanced weapon from one authorized contract security officer to another authorized contract security officer during a security shift change, or during security officer rotation between posts in the course of a single shift. This requirement is unnecessarily burdensome, and would require licensees employing contractor security officers to procure and maintain significantly more enhanced weapons to support security shift changes and security officer post rotations, while providing no discernable benefit.	"(6) following the completion of their official duties, security personnel shall return enhanced weapons issued from armories to the custody of the licensee, certificate holder, or other security personnel authorized to use enhanced weapons who are assuming official duties."
Part 73.18 (o)(3)(vi)	The language in this paragraph specifying that, "The time interval from the previous monthly inventory shall not exceed 30 +/- 3 days" is unnecessarily restrictive by limiting how early a monthly inventory may be conducted following the previous inventory. Changing the requirement to a time interval not exceeding 30 +3 days from the previous monthly inventory would allow licensees to conduct an inventory earlier than 30 -3 days from the previous monthly inventory. This would cause no degradation in the effectiveness of the inventory, and would allow licensees the flexibility to manage when during the month the inventories occur by "resetting" the time	"(vi) The time interval from the previous monthly inventory shall not exceed 30 + 3 days."

Industry Comments – Proposed Rulemaking on Enhanced Weapons and DG 5020

EW Document/Section/ Page Reference	Comment	Suggested Wording/Revision
	during the month in which the inventory occurs by conducting an early inventory. Maintaining the 30 +3 days from the previous monthly inventory would continue to limit the maximum interval between monthly inventories, which appears to be the intent behind this paragraph of the regulation.	
Part 73.18 (o)(4)(iii)	The language in this paragraph specifying that, "The time interval from the previous semi-annual inventory shall not exceed 180 +/- 7 days" is unnecessarily restrictive by limiting how early a semi-annual inventory may be conducted following the previous inventory. Changing the requirement to a time interval not exceeding 180 + 7 days from the previous semi-annual inventory would allow licensees to conduct an inventory earlier than 180 - 7 days from the previous semi-annual inventory. This would cause no degradation in the effectiveness of the inventory, and would allow licensees the flexibility to manage when during the year the semi-annual inventories occur by "resetting" the time during the year in which the inventory occurs by conducting an early inventory. Maintaining the 180 + 7 days from the previous semi-annual inventory would continue to limit the maximum interval between semi-annual inventories, which appears to be the intent behind this paragraph of the regulation.	"(iii) The time interval from the previous semi-annual inventory shall not exceed 180 + 7 days."
Part 73.18 (o)(5)	"Licensees and certificate holders shall conduct monthly and semi-annual inventories of enhanced	Recommend using one person enrolled in a BOP to conduct the inventories.

Industry Comments – Proposed Rulemaking on Enhanced Weapons and DG 5020

EW Document/Section/ Page Reference	Comment	Suggested Wording/Revision
	weapons using a two-person team." Utilizing the behavioral observation program (BOP) would mitigate the manipulation of inventory results.	
Part 73.18 (f)(iv)(D)	In assessing potential safety impacts, licensees and certificate holders shall consider both accidental and deliberate discharges of these enhanced weapons. A deliberate discharge would only occur during an actual assault on the facility or during training and should not be considered when completing an assessment.	Recommend that when assessing potential safety impacts, the licensee shall only consider accidental discharges of enhanced weapons.
Part 73.18, Section IV. (b)(1)	This paragraph requires the licensees to report "A discovery that ammunition that is authorized by the licensee's security plan has been lost or uncontrolled inside a PA, VA, MAA or CAA. Blank cartridges used during force-on-force security exercises should be specifically excluded from this reporting requi4rement. The highly dynamic nature of force-on-force security exercises makes the occasional, incidental loss of blank cartridges a near certainty; however, because of the nature of a blank cartridge, the occasional, incidental loss of a blank cartridge inside a PA, VA, MAA or CAA poses essentially no security risk.	"(c) *Loss of control or protection of classified information.* A discovery that a loss of control over, or protection of, classified material containing National Security Information or Restricted Data has occurred, unless both of the following conditions are met – (1) There does not appear to be evidence of theft or compromise of the material, and (2) The material is recovered or secured within one hour of the loss of control or protection."
Part 73.19(b)(9)	The language of this paragraph requires "Security personnel who have completed a satisfactory firearms background check, but who have had a break in	Recommend clarification is provided regarding what constitutes a "break in service".

Industry Comments – Proposed Rulemaking on Enhanced Weapons and DG 5020

EW Document/Section/ Page Reference	Comment	Suggested Wording/Revision
	service with the licensee, certificate holder, or their security contractor of greater than on week subsequent to their most recent firearms background check... are required to complete a new satisfactory firearms background check." More clarification is needed regarding the definition of "break in service" as it relates to termination of employment, leaves of absence or active service in the Military Reserves or National Guard.	
DG-5020		
Page 9, Section 1.8.1	N/A	Recommend changing the definition in Part 73 section 73.2 of the Rule for "Covered Weapons" and define "covered weapons" as any enhanced Weapon or Standard Weapon as defined in 73.2." Also, delete the definition following "covered weapons."
Page 11, Section 2.5	At the beginning of the paragraph, "...certificate security personnel"; needs to be changed for consistency with other documents.	Recommend the term "certificate holder" be used rather than "certificate security personnel".
Page 16, Section 6.1	"Licensees or certificate holders must submit proposed modifications to their security plan to the NRC for review and approval prior to implementation."	Recommend clarifying specifically what documents are expected to be modified as part of the Security Plan (e.g., Defensive Strategy, Security Assessment for new reactors, PSP).
Page 21, Section 10.1	In the first paragraph of this section, "site of the facility" is used and defined in this section.	Recommend that the referenced term, "site of the facility" and "site boundary" be defined within the glossary.
Page 29, Section 15.1, sixth	"Security personnel who have completed a satisfactory	Recommend clarifying what the term "break in

Industry Comments – Proposed Rulemaking on Enhanced Weapons and DG 5020

EW Document/Section/ Page Reference	Comment	Suggested Wording/Revision
paragraph, first sentence	firearms background check, but who have had a break in service with the licensee, certificate holder, or their security contractor of greater than 1 week, or who have transferred from a different licensee or certificate holder, are required to complete a new satisfactory firearms background check."	service" as it applies to military duty, vacation, sick time, FMLA, short term disability and long term disability, etc.

~~SECURITY RELATED INFORMATION – WITHOLD FROM PUBLIC DISCLOSURE~~

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Reference Page/Section	Comment	Suggested Wording/Revision
General Comment	Proposed changes to Reporting and Recording Safeguards Events and Proposed Rulemaking on Enhanced Weapons are two entirely separate areas. Any rulemaking on Reporting and Recording Safeguards Events should be addressed separately, using a risk-informed graded approach that considers the differences between the facilities subject to the reporting requirements (e.g. reactors and fuel cycle facilities). The fact that proposed changes to Reporting and Recording Safeguards Events were issued under Proposed Rulemaking on Enhanced Weapons caused significant confusion throughout the industry.	Recommend issuing separate rulemaking for Reporting and Recording Safeguards Events and Enhanced Weapons.
General Comment	The proposed rule and DG-5019 require licensees to notify the NRC Headquarters Operations Center as soon as possible, but not later than 15-minutes after the discovery of an imminent or actual hostile action. The industry understands the objective to provide prompt notification to NRC for this type of event, but believes that the current notification time period of "approximately 15-minutes" for security based events contained in NRC Bulletin 2005-02 "Emergency Preparedness Response for Security-Based Events" meets that objective. The examples of security events provided by the proposed rule and DG that require 15-minute notification would promptly be reported to the station control room and the event classification accomplished in a very short time period. Adding an additional reporting requirement to ensure reporting	Recommend the requirement to notify NRC 15 minutes after the discovery of an imminent threat or hostile action be removed.

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Reference Page/Section	Comment	Suggested Wording/Revision
	"as soon as possible, but not later than 15-minutes of the discovery of..." would increase administrative burden and could potentially result in a negative impact on a licensee's response to the event. The potential minimal increased time to accomplish the notifications in conjunction with event classification would not inhibit the effectiveness of NRC in warning other licensees and/or other stakeholders of the event.	
General Comment	The proposed rule and DG present the addition of a 4-hour and 8-hour reporting requirement for suspicious activities. The industry understands the benefit of reporting suspicious activities to the NRC in a timely manner in light of the importance of detecting pre-operational surveillance activities. The criteria in the proposed rule and DG for determining the timeframe for event reporting within 4-hours appears to be events that 1) do not result in the interruption of facility operations and 2) could prevent the implementation of the protective strategy for protecting any target set; and notifications to and responses from LLEA. The examples provided that should be reported within 4-hours would have no immediate or short-term impact on protective strategies or law enforcement response.	Recommend that all suspicious activities be reported in a timely manner but not later than 8-hours from discovery and that the 4-hour reporting requirement be eliminated.
General Comment	10 CFR 73.55(b)(10) states "The licensee shall use the site Corrective Action Program to track, trend, correct and prevent recurrence of failures and deficiencies in the Physical Detection Program." 10 CFR 73.55(m)(4) states, "Findings from onsite Physical Protection Program reviews must be entered into the site	Based on the references provided, it is the industry's recommendation that the Safeguards Event Log be eliminated as an official record and that the station's Corrective Action Program be officially recognized as the primary data source and means to document failures, degradations, or

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Reference Page/Section	Comment	Suggested Wording/Revision
	Corrective Action Program." 10 CFR 73.55(n)(1)(iii) states "Identify in procedures the criteria for determining when problems, failures, deficiencies, and other findings are documented in the site Corrective Action Program for resolution." 10 CFR 73.55(n)(1)(iv) states, "Ensure that information documented in the site Corrective Action Program is written in a manner that does not constitute safeguards information as defined in 10 CFR 73.21." 10 CRF Part 73 Appendix B 3(i) "Findings, deficiencies and failures identified during tactical response drills and force-on-force exercises that adversely affect or decrease the effectiveness of the protective strategy and physical protection program shall be entered into the licensee's Corrective Action Program to ensure that timely corrections are made to the appropriate program areas." At it presently stands, the industry duplicates this process by recording events as Safeguards Event Logs as well as into the CAP. Approximately 20 years ago when this requirement was implemented, it was a valuable tool to track and trend security performance; however, as all stations have adopted the CAP as required above, the Safeguards Event Logs have become a duplicative administrative burden that is only being maintained as a code requirement and is no longer being used as a tool to track and trend security performance.	discovered vulnerabilities that could have allowed unauthorized or undetected access to any area if compensatory measures were not in place or implemented at the time of discovery.
General Comment	Industry recognizes and appreciates the need for timely reporting of security events to the NRC.	Recommend making modifications to the reporting requirements defined within the

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Reference Page/Section	Comment	Suggested Wording/Revision
	However, industry considers "discovery" to have occurred after the initial event has been observed, appropriate internal notifications made, and a licensee determination made that the event meets the applicable reporting requirements. Industry recognizes that for many events and most conditions, the time of "discovery" begins when a cognizant individual such as a manager, supervisor for the security function has been notified. However, for some less obvious conditions, a thorough investigation and evaluation is necessary which may lead to the discovery of a potentially reportable event. Also, the licensee's evaluation should proceed on a time scale commensurate with the security significance of the issue to ensure that both the licensee and the NRC receive a complete and accurate report of the event or condition. Therefore, industry believes that the time of "discovery" will vary because it is event driven and should not be considered to have occurred in each case at the time that the actual event occurred or condition is initially observed. The following language was adopted by NRC in FCSS Interim Staff Guidance-12, Revision 0, 10 CFR Part 70, Appendix A - Reportable Safety Events, which industry believes can be applied to discovery of security events within the context of this rulemaking: "The time of discovery begins when a cognizant individual observes, identifies, or is notified of a safety significant event or condition. A cognizant individual is anyone who, by position or experience, is expected to understand that the particular condition or event	proposed rule and DG 5019 that clarify "discovery", which will improve the efficiency and effectiveness of event reporting and eliminate redundant requirements.

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Reference Page/Section	Comment	Suggested Wording/Revision
	adversely impacts safety. For some conditions, such as the examples shown in Table 1 and Attachment B, an investigation and evaluation is necessary and may lead to the discovery of a potentially reportable situation. This evaluation should proceed on a time scale commensurate with the safety significance of the issue." Industry is willing to work with NRC to develop appropriate examples where investigation and evaluation is necessary.	
General Comment	It would appear that the reportability requirements within the proposed rule and DG 5019 as applied to Physical Security were applied directly to cyber security. In addition, the licensee Cyber Security Plan does not specify what represents adequate compensatory measures for the different types of discovered vulnerabilities, nor the timeframe to implement these compensatory measures. Therefore, an effective determination of what constitutes compensated or uncompensated is not currently an achievable objective from a reporting perspective. No guidance exists; therefore, it is not possible to differentiate which cyber security events are reportable versus which are recordable. In addition to the comments, the industry Cyber Security Task Force has provided information that offers an alternate approach for reporting criteria for cyber events.	Recommend providing an alternative approach for reporting criteria for cyber events.

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Reference Page/Section	Comment	Suggested Wording/Revision
General Comment	The use of words such as "could", "may" and "is likely to" in the draft rule and DG are not definitive; and therefore, require the licensee to use subjective reasoning to determine reportability and could cause excessive and unnecessary reporting.	
Appendix G, Section I *Events to be reported within one hour of discovery.* (d)(1), (f)(1), (f)(2), (h)(2), (k)(1), (k)(2) :	1.) General comment on 10 CFR 73.71(c) for Facility Security Events to Be Reported within 1 Hour. The NRC should reconsider the time requirements for some events to (1) simplify the requirements and (2) bring them more in line with reporting requirements for reactor safety issues that do not involve emergencies (10CFR50.72). It is understandable that certain issues that involve actual or potential threats to the facility should be reported in a more timely manner to assure the appropriate Federal and law enforcement agencies are notified, but other events do not require this urgency. In these cases, the licensee should be provided adequate time to collect the facts and evaluate the issues. The additional time would not interfere with the NRC or law enforcement agency goals to assess the "current threat environment". The rule 10 CFR73.71 (c) and Appendix G, Section I should not require 1 hour notifications for events not related to either a specific threat or attempted threat on the facility. This would be comparable to the 10CFR50.72 (b) (2) and (b) (3) and reporting requirements for non-emergency events. Certain	

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Reference Page/Section	Comment	Suggested Wording/Revision
	events may be significant from a security program implementation perspective; however, if there is no imminent threat then additional time should be afforded the licensee. The licensee should be given more time to collect the facts and evaluate issues such as (1) uncompensated failures or discovered vulnerabilities in security or cyber security systems (2) loss of SGI (3) an authorized standard weapon uncontrolled in PA/VA. These vulnerabilities where there is no actual threat is evident are no different than reactor safety issues such as being in an unanalyzed condition that significantly degrades plant safety. The reporting requirement for an unanalyzed condition is as soon as practical but no longer than **8 hours**.	
Part 73.71(a)(3)	15 minutes is an unrealistic timeframe to provide for a licensee to make a correct assessment of a situation/event and gather the necessary information that is required to be included within the notification.	Recommend the 15 minute timeframe be deleted from 73.71; other reporting requirement will result in notification within a similar timeframe.
Part 73.71(a)(2), p. 156	The wording provided in (2) would be redundant to (1) and only serves to cause confusion.	Delete (2).
Part 73.71(a)(6)(b), p. 157	The wording provided in (1) and (3) is redundant.	Delete (1) and (3).
Part 73.71, Appendix G, I.(b)(1), p. 169	Limiting this section to personnel with malevolent intent versus unintended acts adds clarity and intent to this requirement and is consistent with guidance in DG 5019.	Malevolent intent should be added to the end of the sentence.

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Reference Page/Section	Comment	Suggested Wording/Revision
Appendix G to Part 73, Section I (d) (1) Appendix G, Paragraph III Events to be reported in 8 hours RE: Authorized weapon events.	Specific change to address a general comment above: The discovery that a standard weapon that is authorized by the licensee's security plan is uncontrolled within a PA, VA, MAA, or CAA but recovered should be an 8-hour report not a 1-hour report as long as there is no specific threat associated with the event. The licensee should be provided adequate time to collect the facts and evaluate the issue. The additional time would not interfere with the NRC or law enforcement agency goals to assess the "current threat environment". Add as an event to be reported within 8 hours.	***Revise*** *Appendix G to Part 73, Section I (d) (1)* ***to*** *state* *(d) Authorized weapon events.* *(1) The discovery that a standard weapon that is authorized by the licensee's security plan is lost* ~~***or uncontrolled***~~ *within a PA, VA, MAA, or CAA.* ***Add*** *to App G, Paragraph III Events to be reported in 8 hours* *Authorized weapon events.* *The discovery that a standard weapon that is authorized by the licensee's security plan is* ***uncontrolled*** *within a PA, VA, MAA, or CAA.*
Appendix G, Paragraph 1 (d)(2)	This is a definition of uncontrolled authorized weapon and belongs in the glossary – not here.	Delete.
Appendix G, Section I (f) App G, Section III Events to be reported in 8 hours	Uncompensated security events should be an 8 hour report not a 1 hour report IF there is no specific threat associated with the event. In particular, events related to inadequate compensation for degraded systems or vulnerabilities discovered that are not predictable and represent no immediate threat should not require immediate notification within 1 hour. These events have the potential to decrease the effectiveness of the security plans; however they do not represent an immediate threat. It should also be noted that the examples in App G, Paragraph I, sections (f)(1), f(2), and (f)(3) do not represent uncompensated events, but failures in the program that result in either a contraband event or	**Delete** *Appendix G to Part 73, Section I (f)* ~~*(f) Uncompensated security events. Any failure, degradation, or the discovered vulnerability in a safeguard system, for which compensatory measures have not been employed, that could allow unauthorized or undetected access of (1) Explosives or incendiaries beyond a vehicle barrier,*~~ **[Delete item 1 already covered under (e) Vehicle barrier system events]** ~~*(2) Personnel or contraband into a PA, VA, MAA, or CAA; or ;*~~ **[Delete item – already covered under (c) Contraband events.]** ~~*(3) Personnel or contraband into a vehicle transporting special nuclear material, spent*~~

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Reference Page/Section	Comment	Suggested Wording/Revision
	vehicle barrier event that are described separately in App G, Paragraph I, sections (c) and (e) respectively. Revise as suggested. Add as events to be reported within 8 hours.	~~*nuclear fuel, or high-level radioactive waste; or to the special nuclear material, spent nuclear fuel, or high-level radioactive waste itself.*~~ **[Delete item 3 – already covered under (c) Contraband events.]** ***Add*** *to App G, Paragraph III Events to be reported in 8 hours* *Uncompensated security events. Any failure, degradation, or the discovered vulnerability in a safeguard system, for which compensatory measures have not been employed, that could allow unauthorized or undetected access of a PA, VA, MAA, or CAA.*
Part 73.71, Appendix G, I.(e) & (f)(1)	Vehicle barrier systems are designed to defend against explosives above a specific amount based on site-specific analysis. Only introduction of contraband beyond a barrier and associated search process that is designed to prevent its introduction should be reportable. In this case, the barrier and associated search process is designed to prevent the introduction of a specific VBIED. This concept needs to be applied throughout the RG.	Delete "incendiaries" from both sections.
Part 73.71, Appendix G, I.(a)(5), II.(a)(1)(B) and III.(1,2,3)	Wording should be revised to clarify the need for deliberate and malevolent intent. This would rule out human error events such as mispositioning.	Recommend revising the wording as follows: The "malevolent" unauthorized operation, manipulation, or tampering...

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Reference Page/Section	Comment	Suggested Wording/Revision
Part 73.71, Appendix G, I.(a)(5)	N/A	*The unauthorized operation, manipulation, or tampering with any Category I strategic special nuclear material (SSNM) facility's controls or SSCs with malevolent intent that results in the interruption of normal operation of the facility.*
Appendix G, Section I (h)(2) Appendix G, Paragraph III Events to be reported in 8 hours	Uncompensated Cyber security events should be an 8 hour report not a 1 hour report as long as there is no specific threat associated with the event. In particular, events related to inadequate compensation for degraded systems or vulnerabilities discovered that are not predictable and represent no immediate threat should not require immediate notification within 1 hour. The licensee should be provided adequate time to collect the facts and evaluate the issue. The additional time would not interfere with the NRC or law enforcement agency goals to assess the "current threat environment" Events that would be reported in 1 hour would be reported under App G, Paragraph I, section (h) (1) *Cyber security events*	**Delete** *Appendix G to Part 73, Section I (h)(2) Cyber security events.* ~~*(2) Uncompensated cyber security events. Any failure, degradation, or the discovered vulnerability in systems, networks, and equipment that falls within the scope of § 73.54 of this part, for which compensatory measures have not been employed and that could allow unauthorized or undetected access into such systems, networks, or equipment*~~ ***Add*** *to App G, Paragraph III Events to be reported in 8 hours (f) Cyber security events.* ***(2) Uncompensated cyber security event. Any failure, degradation, or the discovered vulnerability in systems, networks, and equipment that falls within the scope of § 73.54 of this part, for which compensatory measures have not been employed and that could allow unauthorized or undetected access into such systems, networks, or equipment.***
Appendix G, Section I – Events to be reported in 1 hour (k)(1), (k)(2)	*Loss of Safeguards Information* should be an 8 hour report not a 1 hour report IF it does not involve theft AND there is no evidence of a specific threat	**Revise *Appendix G to Part 73, Section I*** *Events to be reported in 1hour (k)* ~~***Loss of***~~ *Theft of Safeguards Information. The discovery of the*

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Reference Page/Section	Comment	Suggested Wording/Revision
Appendix G, Section III, Events to be reported in 8 hours	associated with the event. The Regulatory Guide guidance is unclear as to when SGI loss or compromise rises to the level of significance (i.e., notification vs. recorded in a Safeguards Event Log) with regards to the SGI material in question. The requirements for reporting SGI theft, loss, or lack of controls in the current rule language suggest that an SGI control event is either a significant 1 hour notification or recorded within 24 hours, if identified by the licensee within 1 hour. It is understandable that for a loss of control of more significant SGI material, that the NRC would require a notification and a follow-up written report due to the vulnerability, however, without a threat it is not reasonable to require immediate notification within 1 hour. The additional time would not interfere with the NRC or law enforcement agency goals to assess the "current threat environment".	~~***loss or***~~ *theft of material (e.g., documents, drawings, analyses, or data) that contains Safeguards Information* ~~***— (1)***~~ *Provided that such material could substantially assist an adversary in* ***gaining undetected access to the facility PA or VAs or assist in significant damage to Safety Related SSCs.*** ~~*the circumvention of the facility or transport security or protective systems or strategies; or*~~ ~~*(2) Provided that such material is lost or stolen in a manner that could allow a significant opportunity for the compromise of the Safeguards Information.*~~ ***Add: Appendix G to Part 73, Section III*** *Events to be reported in 8 hours* ***Loss of Safeguards Information. The discovery of the loss of material (e.g., documents, drawings, analyses, or data) that contains Safeguards Information provided there does not appear to be evidence of theft or compromise of the material, and the material could significantly assist an adversary in (1) gaining undetected access to the facility PA or VAs or (2) assisting in significant damage to Safety Related SSCs or (3) significantly challenging the Licensee's ability to implement their protective strategy effectively.***
Appendix G, Paragraph II (c)(2)	Suggested change to reference additional applicable	*Appendix G, Paragraph II (c)(2) An event*

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Reference Page/Section	Comment	Suggested Wording/Revision
	regulations that require notification due to possible public or media inquiries.	*involving a law enforcement response to the facility that could reasonably be expected to result in public or media inquiries and that does not otherwise require a notification under paragraphs I, ~~or~~ the other provisions of paragraph II of this appendix,* ***or in other NRC's regulations such as 10CFR50.72(b)(2)(xi).***
Appendix G, Paragraph II, (d)(2)	The threshold for law enforcement agency response needs to be at a reasonable level. Many law enforcement agencies record any response in a ledger that is available to the public and routinely checked by media outlets. Reporting incidents absent a malevolent intent is an unnecessary burden.	Change to read, "An event involving a law enforcement response....of paragraph II of this appendix. (excluding response to minor incidents that may receive media attention, e.g., traffic accidents, trespass by individuals without malevolent intent)".
Part 73.71, Appendix G, IV.(a)(1)(i)	Vehicle barrier systems are designed to defend against explosives above a specific amount based on site-specific analysis.	Delete "incendiaries" from section.
Part 73.71, Appendix G, IV.(b)(1)	The lost or stolen ammunition does not rise to the level of a loggable incident due to the fact that small quantities of ammunition (authorized or unauthorized) do not constitute a significant vulnerability.	Recommend deleting this section.
Part 73.71, Appendix G, IV.(d)	This section refers to Safeguards Information as "classified" material.	Recommend replacing "classified" with "designated".
73.71(j)(8); 73.71(m)(13)(i)	10CFR73.71 guidance regarding retractions implies that the only reason you could retract the report is if the event was invalid. It is also possible to retract the call because it was determined it did not meet the	***73.71 (j) Notification process. (8)*** *Licensees and certificate holders desiring to retract a previous security event report that has been determined to be* ***not reportable in accordance***

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Reference Page/Section	Comment	Suggested Wording/Revision
	criteria for a notification or the event was determined to only rise to the level of an event to be recorded in the Safeguards Event Log in accordance with 73.71(k) and Appendix G, paragraph IV. While the characterization of the issue has changed, it would not be considered "invalid". The guidance should be revised.	***with 73.71(a) through (h) or*** *invalid shall telephonically notify the NRC Headquarters Operations Center in accordance with paragraph (j) of this section and shall indicate the report being retracted and basis for the retraction.* ***73.71(m) (13)(i)*** *If the licensee or certificate holder subsequently retracts a telephonic notification made under this section as* ***not reportable in accordance with 73.71(a) through (h) or*** *invalid and has not yet submitted a written report required by paragraph (m) of this section, then submission of a written report is not required.* *(ii) If the licensee or certificate holder subsequently retracts a telephonic notification made under this section* ***not reportable in accordance with 73.71(a) through (h) or*** *invalid, after it has submitted a written report required by paragraph (m) of this section, then the licensee or certificate holder shall submit a revised written report in accordance with paragraph (m) of this section.*
Definition of 'Credible Threat' within DG-5019, Glossary, p. 57	There appears to be inconsistency between the definition of "Credible threat" within the glossary of DG-5019 and information contained on p. 34 of 10 CFR 73 [NRC-2008-0465] RIN: 3150-A149.	N/A
Federal Register Vol 76, No. 23 **73.2 definitions** Page 6232	Covered Weapons should be defined as any enhanced Weapon or Standard Weapon as defined below. The proposed definition combines both of these definitions	Redefine "covered weapons".

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Reference Page/Section	Comment	Suggested Wording/Revision
	and makes it difficult to discern whether or not large capacity ammunition feeding device would constitute an enhanced weapon.	
Federal Register Vol 76, No. 23 **73.2 definitions** Page 6232		Standard Weapons Move statement. "3. In § 73.8, paragraphs (b) and (c) are revised to read as follows:" to precede the terms.
Federal Register Vol 76, No. 23 § 73.71 Pg. 6240	Written Follow-up Reports, and Page 45, Section 4.4 - The NRC indicates that Licensees subject to § 50.73 of this chapter shall prepare the written reports on NRC Form 366. NRC form 366 includes text location for an abstract and form 366 limits the abstract to 1400 characters including spaces. The NRC does not specify, either in the new rule (10CFR73.71, and 10CFR73, Appendix G) nor in Reg Guide DG-5019 the required content of the Abstract. Suggest clarifying the requirement or state that the content is at the Licensee's Discretion.	Suggest clarifying the requirement or state that the content is at the Licensee's Discretion.
Federal Register Vol 76, No. 23 § 73.71(a)(1) Page 6240	Wording Could be interpreted to imply that knowledge of an ongoing event at another covered facility (a non-Licensee Facility, through news media) would need to be reported by other Licensees. Suggest rewording to clarify that the intent is for Licensees to report events that affect their own facilities only.	Suggest rewording to clarify that the intent is for Licensees to report events that affect their own facilities only.
Federal Register Vol 76, No. 23 § 73.71(b) Page 6241	The phrase "or make provisions to notify" is unclear and subject to interpretation.	Suggest rewording to state: "or implement proceduralized actions to notify."

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Reference Page/Section	Comment	Suggested Wording/Revision
Federal Register Vol 76, No. 23 Appendix G to Part 73 I. (a) Page 6243	N/A	Appendix G, paragraph "a" should be modified to change "threat" to "credible threat."
Federal Register Vol 76, No. 23 Appendix G to Part 73 I. (a)(4) Page 6243	As presently worded, this could include inadvertent manipulation of plant that interrupts plant operation. For example, authorized individuals working under authorized work instructions who inadvertently manipulate equipment on the "wrong unit" or "wrong component" could interrupt plant operation (e.g., cause a plant trip) and would be unauthorized manipulation if not covered by a specific approved work instruction. Such an event would require a report under this paragraph even though there was no security risk present.	Suggest rewording to clarify intent (e.g., "The unauthorized operation, or tampering with any nuclear reactors controls of with structures, systems and components (SSC's) with malevolent intent that results in the interruption of normal operation of the reactor;"
Federal Register Vol 76, No. 23 (e) Pg. 6244	N/A	Paragraph (e) should be clarified to indicate "explosives or incendiaries that are not intended for valid and authorized activities at the facility."
Federal Register Vol 76, No. 23 (f) (1) Pg. 6244	N/A	Section should be clarified to indicate "explosives or incendiaries that are not intended for valid and authorized activities at the facility."
Federal Register Vol 76, No. 23 (j) Pg. 6244	N/A	Paragraph (j): Restricted Data is not defined.
Federal Register Vol 76, No. 23 (II) (a)(1)(B)	N/A	"Elicitation of information from facility personnel relating to the security or safe operation of the

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Reference Page/Section	Comment	Suggested Wording/Revision
Page 6244		facility." This phrase is vague and subject to interpretation. As written, this could be interpreted to apply to legitimate inquiries from the public regarding how the licensee ensures the plant operates safely (operational defense in depth, protected trains status, vital equipment, etc.). Suggest rewording as follows: "Non Routine elicitation of information from facility personnel relating to the security or safe operation of the facility.
Federal Register Vol 76, No. 23 (III) (1)(2)&(3) Page 6244	N/A	Section 2.6.1, Appendix G, Paragraph III(1), (2), and (3) should all be modified such that reporting is not required unless the licensee has reason to believe the event was caused by malicious intent.
Federal Register Vol 76, No. 23 (IV) (a)(1) (i) Page 6244	N/A	Appendix G, Paragraph IV, (a)(1)(i) should be conditioned to require an SEL only for events involving requires licensees to record an SEL entry for "explosives or incendiaries that are not intended for valid and authorized activities at the facility."
Federal Register Vol 76, No. 23 (IV) (a)(2)(b) Page 6245	N/A	Based upon evaluation of Authorized Ammunition that has been lost or is uncontrolled within a PA it is recommended that Attachment 1 be discussed at the NEI conference currently Scheduled for 3/15/2011. The regulatory language is to broad. Reporting of events that would not equate to an actual threat to the

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Reference Page/Section	Comment	Suggested Wording/Revision
		Security Plan, should not be required to be recorded in the Safeguards Event Log.
Federal Register Vol 76, No. 23 (IV) (a)(2)(c) Page 6245	N/A	Please define Restricted Data.
DG-5019		
Section 2.1, p. 12	See suggested wording.	The first sentence of the third paragraph should be re-located to beginning of the section.
DG-5010, Section 2.1	There seems to be a conflict between two paragraphs within section 2.1. Paragraph 3 states that "this Reg. Guide does not apply to aircraft threats and attacks...;" however, on page 13, paragraph 5 states "Hostile actions include attacks by air....."	Delete "air" from 2.1 paragraph 5.
Section 2.1.2, c.	Section d. sets the threshold for 15 minute reporting involving weapons. Section c. does not meet the threshold established by d. and therefore does not meet the requirements for 15 minute reporting.	Delete c.
Section 2.1.2, j.	This example is redundant to examples a., d., e., and i.	Delete j.
Page 14, Section 2.1.2 (b)	Steam Generator Tube Sleeving is performed with explosive welding techniques.	Recommend adding clarifying verbiage to exclude explosive charges used for legitimate purposes; "malevolent detonation".
Page 14, Section 2.1.2 (h)	As written, it is unclear at what "believed theft"	Suggest rewording to clarify (e.g., "actual theft or

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Reference Page/Section	Comment	Suggested Wording/Revision
	means.	significant information causing a licensee reason to conclude that theft of SSNM or SNF has occurred").
Page 14, Section 2.1.2 (k)	Due to the formatting in this section, it is not clear whether this paragraph applies to Section k.	Recommend that the second paragraph be reformatted as a sub-bullet or indented under k.
Page 15, Section 2.2	See suggested wording.	The first sentence of the third paragraph should be re-located to beginning of the section.
Page 15, Section 2.2, Paragraph 4	The definition for "hostile action" needs to be consistent with the definition for "hostile action" contained in NEI 03-12 "Security Plan Template" and NEI 99-01 "Methodology for Development of Emergency Action Levels". Review definition in RG 5.76. There is no definition for "imminent" in the text or in the glossary sufficient for licensees to make consistent decisions.	Use the definition of "imminent" contained in NEI 03-12.
Page 15, Section 2.2, Paragraph 4	Phrase "to deliver destructive force" is overly broad and subject to interpretation.	Suggest deleting "to deliver destructive force."
Page 16, Section 2.2.2 (d)	The example does not appear to rise to the level of the 15 minute notification rule requirement 73.71(b).	Delete d.
Page 17, Section 2.3, 2nd paragraph	Wording should be revised to clarify the need for deliberate and malevolent intent. This would rule out human error events such as mispositioning.	Recommend rewording the paragraph as follows: Generally, these events relate to committed or attempted acts and credible threats involving theft

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Reference Page/Section	Comment	Suggested Wording/Revision
		or diversion of SSNM or SNM; significant physical damage to the facilities identified above; interruption of normal operation of a facility caused by **malevolent** unauthorized operation or by **malevolent** tampering with controls, safety related and non safety-related structures, systems, and components (SSCs); **malevolent** unauthorized entry of personnel into a PA, VA, MAA, or CAA; malevolent attempted entry of personnel into a PA, VA, MAA, or CAA; actual or attempted introduction of contraband into a PA, VA, MAA, or CAA; actual or attempted introduction of explosives or incendiaries beyond a vehicle barrier system; or an uncompensated vulnerability, failure, or degradation of security systems that could allow unauthorized access of personnel or contraband.
Page 17, Section 2.3, 4th paragraph	General Comment: Cyber attack reporting discussed in this section needs to be synchronized with NEI 08-09 "Cyber Security Plan Template" and RG 5.71 to ensure the final RG contains well defined reporting criteria and avoid conflicting guidance.	N/A
Page 18, Section 2.3, 7th paragraph	This paragraph discusses "the need to record other failures, degradations.....". Those types of events are located in section 5.1. Suggest eliminating this paragraph.	Eliminate paragraph

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Page 20, Section 2.3.2	A number of the examples in this section are not providing additional clarity. The examples seem to be written in a manner to encompass multiple scenarios, and in doing so, the clarity is reduced. Individual specific "real life" examples would be more helpful. A collegial review of historical data by industry and NRC representatives would provide "real life" specific examples that would help clarify NRC expectations.	Provide specific examples with granularity in the text.
Page 20, Section 2.3.2 (a)	Clarification should be provided consistent with 2.3.2, b, (1) that unauthorized entries to be reported are those with malicious intent.	Clarify (a) as follows: the successful, surreptitious penetration of a PA, VA, MAA, or CAA by unauthorized personnel with malevolent intent.
Page 20, Section 2.3.2 (c)	Clarification should be provided consistent with 2.3.2,b,(1) that attempted unauthorized entries to be reported are those with malicious intent.	(c) malicious entry attempts by unauthorized persons, vehicles, or material, meaning that reliable and substantive information indicates that (1) an effort to accomplish the entry, even though it has not yet occurred, is possible, or (2) the entry was not successful because it was interrupted or stopped before completion.
Page 20, Section 2.3.2 (d)	This is redundant to 2.3.2,c and should be deleted	Delete.
Page 20, Section 2.3.2 (f)	Paragraph is confusing. Mixing of "dismounted individuals and explosives and incendiary devices. Is the example related to dismounted personnel or the introduction of explosives or incendiary devices past the VBS? Paragraph "h" appears to address the explosives and incendiary devices. It is unclear why the VBS is the demarcation for reportability for other than VBIEDs. This issue appears in other areas of the draft rule and RG.	Recommend clarifying the entire paragraph; the intent is unclear.

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Page 21, Section 2.3.2 (h)	This section does not explain "Where" – is this section pertaining to OCA, PA, VA, etc. Provide clarification to where the "introduction of contraband material" occurs.	Change to "the actual or attempted introduction of contraband material into the PA, VA, MAA or CAA".
Page 21, Section 2.3.2 (h)	The information within the parenthesis is unnecessary, since the definition is in the glossary.	Delete (e.g., unauthorized weapons, explosives, or incendiaries).
Page 21, Section 2.3.2 (i)	This is redundant to (h).	Delete.
Page 21, Section 2.3.2 (j)	Unless it is determined that there is a malicious attempt to defeat the barrier, the event should not be reported. Damage that would impact on the ability of the barrier to perform its function would be compensated for. Failure to compensate degraded barriers is addressed in (k).	Delete.
Page 21, Section 2.3.2 (k)(1)	Uncompensated is defined in the glossary. The text in (k)(1) does not provide additional clarity and should be removed.	Delete.
Page 21, Section 2.3.2 (q)	It is not clear how the "within one hour" phrase relates to the rest of the example. As written, it appears to imply that if undetected access could not have occurred within one hour that the event need not be reported within one hour. Example also combines one hour reporting and 24 hour recording in the same example. The intent of this section is unclear. The text also seems to be in conflict with earlier criteria regarding actual malicious unauthorized entry.	Provide clarification or delete if the intent is not associated with an actual event, since the criteria then should be 24 hour loggable.

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Page 21, Section 2.3.2 (l), (m), and (n)	These are redundant to (k) and should be eliminated.	Delete.
Page 22, Section 2.3.2 (r)	73.71, App G, Para I (a)(4) refers to the interruption of normal operation of the reactor, not facility.	Change to read, "security events that involve an interruption of the normal operation of the licensee's reactor or certificate holder's facility...."
Page 22, Section 2.3.2 (r)(1)	Willful human error as defined by NRC Enforcement Manual, Section 6.1, includes issues of careless disregard where individuals do not bother to see if there is a requirement or restriction. This paragraph, then, would require one hour reporting of events where authorized work was planned and performed by authorized individuals, but did not know the security impacts of such work. This paragraph, therefore, would require one hour security reporting for inadequate planning or work control unrelated to actual tampering with plant structures, systems, or components.	Suggest removing the phrase "or related to willful human error". ~~and "reasonable mechanical failure".~~ Suggest moving the second half of this paragraph due to it being contradictory to the criteria described in (r), "They should report tampering that does not result in an interruption of normal operations under the 4-hour or 8-hour notification requirements. Licensees and certificate holders should report events that are suspicious in nature and where a general assessment cannot be made within 1 hour, under the 4-hour or 8-hour notification requirements."
Page 22, Section 2.3.2 (r)(2)	N/A	Suggest removing the word "may" from this sentence.
Page 22, Section 2.3.2 (r)(1,2,7)	In this section, statements 1, 2 and 7 are the only events that fit under the criteria described in 2.3.2 (r).	Suggest moving statements 3, 4, 5, 6 and 8 to another section.
Page 22, Section 2.3.2 (r)(3)	Unavailability of security personnel after implementation of recall procedures is addressed in (z), p. 23. Anticipated labor actions such as an actual or imminent strike are routinely communicated to NRC along with contingency planning. In addition, this	Recommend deleting this statement.

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

	statement does not fit within the criteria established in Appendix G to Part 73 for a 1-hour notification.	
Page 22, Section 2.3.2 (r)(4)	Defining a "Mass Demonstration" as five individuals or more appears to be arbitrary and too low. Differentiating one hour reporting based on whether or not the demonstrators have a permit also appears to be arbitrary and unrelated to the actual or potential security risk posed by a gathering of individuals outside the facility.	If there is no apparent threat or hostile action, then reporting should be made within eight hours.
Page 22, Section 2.3.2 (r)(5)	N/A	Recommend removing the word "near" and adding the words "without authorization" to the end of the sentence.
Page 22, Section 2.3.2 (r)(6)	Statement 6 conflicts with the Statement of Consideration (p. 34, 35). The Statement of Consideration states that determination of credibility should be made by law enforcement, whereas this section places that responsibility on the licensee.	Recommend statement 6 be revised as follows; Bomb or extortion threats are reportable if the licensee or certificate holder, with input from NRC, law enforcement or intelligence agency information, considers them credible and substantive (this includes the discovery of intent to commit such an act). In addition, the results of any bomb search should be reported within 1 hour of completion.
Page 22, Section 2.3.2 (s)	The phrase "or battery against a plant employee" would require licensees to report offsite incidents of domestic violence within one hour of discovery as a security event even when a security nexus is not present. Additionally, it is unclear how Licensees would be able to comply with the reporting example phrase "being a	Unless there is a specific, identified threat to the facility, recommend this be reported within 8 hours. Suggest rewording from "involving individuals" to "committed by individuals."

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

	member of a terrorist organization." Licensees would not be able to reliably separate rumors and unsubstantiated accusations from reality without extensive investigation. This could require Licensees to make security related one hour reports based on innuendo. The phrase "involving individuals" is also undefined and ambiguous.	
Page 23, Section 2.3.2 (t)	Access to controlled areas is too broad.	Replace "to controlled areas" with "to a PA, VA, MAA, or CAA".
Page 23, Section 2.3.2 (u)	Same comment as above.	Same as above.
Page 23, Section 2.3.2 (aa),(bb)	Duplicate events. Item (4) and (5) reference unsuccessful attacks, which are not a characteristic of (bb).	Recommend deleting (bb) and moving all text under (bb) to (aa). Recommend deleting (4) and (5) under (bb).
Page 29, Section 2.5.1 (a)(1)(B) & Appendix G, paragraph II	"Elicitation of information from facility personnel relating to the security or safe operation of the facility." This phrase is vague and subject to interpretation. As written, this could be interpreted to apply to legitimate inquiries from the public regarding how the licensee ensures the plant operates safely (operational defense in depth, protected trains status, vital equipment, etc.).	Suggest rewording as follows: "Non Routine and suspicious elicitation of information from facility personnel relating to the security or safe operation of the facility."
Page 30, Section 2.5.2 (b)	The use of Owner Controlled Property in this example is overly broad. Recommend changing "Owner Controlled Property" to "Owner Controlled Area." Existing wording could also imply a duty or obligation	Recommend replacing "Owner Controlled Property" with "Owner Controlled Area".

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

	to surveil "Owner Controlled Property" for such activities. Additionally, site policy may prohibit use of non-company equipment or company- or private cell phone cameras inside the owner controlled area. This example would require licensees with similar site policies to report to the NRC within four hours whenever a site employee violated site camera use policy regardless if policy violation had a nexus to security or security risks.	
Page 30, Section 2.5.2 (e)	The information provided in this statement is already covered in other examples under this section.	Recommend removing (e).
Page 30, Section 2.5.2 (g)	"Secretive sketching, making maps, or taking notes on the owner controlled area." This example could be applied to almost all activity involving site personnel taking notes during the course of normal business. This example could also apply to individuals making entries into personal diaries during lunch breaks and being unwilling to share that information with other site personnel.	Recommend adding "which would be indicative of potential pre-operational surveillance, reconnaissance, or intelligence-gathering activities directed against the facility" to the section.
Page 30, Section 2.5.2 (h)	"eliciting information from security or other site personnel regarding security systems or vulnerabilities." Existing wording is overly broad and could apply to routine inquiries about security systems.	Recommend modifying this example to state: "Non-routine and suspicious elicitation of information from security or other site personnel regarding security systems or vulnerabilities."
Page 31, Section 2.5.2 (j)		Delete out of this section and include in section 2.5.2 for impacts to cyber.
Page 31, Section 2.5.2 (m)	"boating activities conducted in unauthorized locations or attempts to loiter near facility restricted areas." The phrase "or attempts to loiter near" is undefined	Recommend deleting the phrase "or attempts to loiter near...". Add "within" before "restricted areas".

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

	and open to interpretation.	
Page 31, Section 2.5.2 (n)	"Unusual" in the step adds too much interpretation.	Change to read, "repeated attempts after requests have been denied by the same individual(s) to obtain....."
Page 31, Section 2.5.2 (o)	"discovery of Internet site postings that make violent threats related to specific licensed facilities or activities." As presently worded, this could require licensees to report occurrences related to facilities other than their own.	Suggest rewording to state: "discovery of Internet site postings that make violent threats related to a licensee's nuclear facilities or their licensed activities."
Page 31, Section 2.5.2 (p)	This statement is redundant and has been adequately covered throughout this section.	Recommend it be deleted.
Page 31, Section 2.5.2 (q)	This statement is redundant and has been adequately covered throughout this section.	Recommend it be deleted.
Page 31, Section 2.5.2 (r)	"unsubstantiated bomb or extortion threats that are considered to be related to harassment, including those representing tests of response capabilities or intelligence-gathering activities, or an attempt to disrupt facility operations (such events should be recorded in the safeguards log until a pattern is discovered). Example is unclear and self-contradictory. Section 2.5.2 provides example of events that should be reported within four hours of discovery. Example "r" states that "unsubstantiated bomb or extortion threats" should be reported. The parenthetical phrase at the end implies that such events would be reportable only after a pattern had been discovered. All events should be reported within 8 hours.	Suggest rewording to state: "unsubstantiated bomb or extortion threats that are considered to be related to harassment, including those representing tests of response capabilities or intelligence-gathering activities, or an attempt to disrupt facility operations."

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Page 31, Section 2.5.2 (s)	"fires or explosions of suspicious or unknown origin within an OCA, PA, VA, or MAA that have not been reported under the 15-minute or 1-hour notification requirements of 10 CFR 73.71 and do not represent an immediate or significant impact on the safe operation of the facility or disrupt its normal operations.	Recommend rewording to also exclude reporting of events already reported under 10 CFR 50.72(a)(1)(i) (Declaration of an Emergency Event). Also recommend removing the words "or unknown".
Page 31, Section 2.5.2 (t)	"Licensees or certificate holders should report to the NRC multiple sightings of the same commercial or general aviation aircraft, circling or loitering above or in close proximity to their facilities, or photographing the facilities or surrounding areas. Appendix A of this RG outlines additional guidance for reporting suspicious aircraft activity and recommendations for licensee or certificate holder pre-coordination efforts to reduce false positive (unnecessary) reports. The bolded phrase requires Licensees to report aircraft that are photographing the facility or surrounding areas. It is more likely that a licensee would not know if an aircraft was photographing the facility or surrounding areas. If such an event were to occur and the photos become known to the NRC and/or public, this guidance could leave licensees subject to NRC enforcement for not reporting a reportable event. It is unclear how citing a licensee for non-reporting would be able to alter Licensee performance and would serve no purpose.	Suggest eliminating the phrase "or photographing the facility or surrounding area" as unachievable.
Page 32, Section 2.5.2 (aa)	N/A	Recommend this item be taken out as a sub-bullet and be a stand-alone item.
Pages 32 and 33, Section 2.5.2	Examples bb through hh: Each of these examples	Recommend (bb) through (jj) be eliminated as

(bb) through (jj)	discusses unauthorized operation, manipulation, cutting of wires, damage to plant equipment, and or damage to non-plant equipment. Each example would require a report to the NRC within four hours. Each of the examples provided could be the result of procedure errors, errors in implementation of work instructions, or accidental damage to plant or non-plant equipment.	these events would not impact on the protective strategy and would be addressed in 1-hour or 8-hour reports based on the impact on normal operation of the reactor or facility.
Page 33, Section 2.5.2 (pp)	Example pp: Example states: the discovery of unsubstantiated cyber attack threats that are considered to be related to harassment, including threats that could also represent tests of response capabilities or intelligence-gathering activities, or an attempt to disrupt facility operations (to be recorded in the safeguards log until a pattern is discovered). The highlighted phrase is undefined and could be interpreted to include attempts to gain access to an e-mail account to harass an employee for reasons unrelated to plant operation or safety would need to be reported in accordance with this example. Example is also confusing as written.	Suggest rewriting as follows: "The discovery of a pattern of unsubstantiated cyber attack threats that ~~are considered to be related to harassment, including threats that) could~~ represent tests of response capabilities or intelligence-gathering activities, or an attempt to disrupt facility operations ~~to be recorded in the safeguards log until a pattern is discovered~~. A pattern exists after three or more such threats have been received within a short period of time (one calendar quarter).
Page 34, Section 2.6.1 (1), (2), and (3) & Appendix G, Paragraph III	Section 2.6.1, Appendix G, Paragraph III(1), (2), and (3) should all be modified such that reporting is not required unless the licensee has reason to believe the event was caused by malicious intent.	See comment.
Page 35, Section 2.6.2 (a) through (f)	Examples (a) through (g), each of these examples discusses unauthorized operation, manipulation, cutting of wires, damage to plant equipment, and or damage to non-plant equipment. Each example would require a report to the NRC within eight hours. Each	Recommend revising each of these examples to include only those events wherein the licensee has reason to believe that the event was caused by malicious intent.

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

	of the examples provided could be the result of procedure errors, errors in implementation of work instructions, or accidental damage to plant or non-plant equipment. Example (f) is not clear and requires further clarification.	
Page 35, Section 2.6.2 (g)	N/A	Recommend deleting example g., due to it having no relation or concern to plant security.
Page 35, Section 2.7.2	Consistent with overarching comment, with the exception of (d) to be reported within 1 hour, all items within this section should be reported within 8 hours.	See comment.
Page 42, Section 3.7, First Paragraph	Need a space between the last line of line of Section 3.7 and 3.8. The phrase "and received training as a communicator" is undefined and unnecessary. As currently drafted, this phrase could imply licensees need to implement a new training requirement for at least a subset of Operations, Security and Emergency Preparedness personnel and ensure that "Communicator-Trained" individual are always present on site.	Recommend deleting the phrase.
Page 43, Section 4.0	There does not seem to be any value in written follow-up reports to (e), (f) and (g) and creates an unnecessary administrative burden on licensees.	Recommend deleting (e) through (g) from both the guidance and the rule requirement.
Page 44, Section 4.1	Written Follow-up Reports, and Page 45, Section 4.4 - The NRC indicates that Licensees subject to § 50.73 of this chapter shall prepare the written reports on NRC Form 366. NRC form 366 includes text location for an abstract and form 366 limits the abstract to 1400 characters including spaces. The NRC does not specify, either in the new rule (10CFR73.71, and	Suggest clarifying the requirement or state that the content is at the Licensee's discretion.

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

	10CFR73, Appendix G) or in Reg Guide DG-5019 the required content of the abstract.	
Page 47, Section 5.0, 2nd paragraph, 1st sentence	The last three words of this paragraph, "whichever is greater" are not consistent with the rule language.	Recommend deleting the words "whichever is greater" from this sentence.
Page 49, Appendix G, Paragraph IV, (a)(1)(i)	Appendix G, Paragraph IV, (a)(1)(i) should be conditioned to require an SEL only for events involving "explosives or incendiaries that are not intended for valid and authorized activities at the facility."	See comment.
Page 50-51, Section 5.3 (c), (d), (h)	These examples would be loggable regardless of the timeframe and exceeding these timeframes would not change the reporting requirement.	Recommend deleting the timeframe examples.
Page 50, Section 5.3 (g)	This example is unclear and requires further clarification.	
Page 51, Section 5.3 (p)	Example as written is confusing; the status of the perimeter as long as properly compensated for does not change the reporting requirements for loss of lighting.	Recommend rewording sentence as "failure or degradation of lighting below security-plan requirements". Delete all other wording.
Page 51, Section 5.3 (q)	Example as written is confusing; the loss of full capability of an alarm station is loggable if properly compensated.	Recommend rewording sentence as "loss of capability of one alarm station (for facilities with two alarm stations)". Delete all other wording.
Page 51, Section 5.3 (r)	Loss of control of SGI is a loggable event in all cases where there is no evidence of theft or compromise. It is not dependant on a timeframe.	Recommend removing the 1-hour stipulation.
Page 52, Section 5.3 (u)	This example is identical to (s). If this was intended to refer to classified information, then it is a typo.	Recommend deleting or correcting (u).

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

Page 52, Section 5.3 (v)	Loss of control of a security weapon within a PA, VA, MAA or CAA is a loggable event regardless of timeframe and exceeding the 1-hour retrieval timeframe would not change reporting requirements.	Recommend deleting the reference to 1 hour.
Page 52, Section 5.3 (y)	This event should be moved to an 8-hour reporting requirement in accordance with 10 CFR 73.71(f).	
Page 52, Section 5.3 (aa)	Does this require missed checks that are not regulatory checks but are required by security procedure need to be logged? Are "security requirements" the same as regulatory requirements, or are "security requirements" the regulatory requirements and any additional requirements that a licensee directs Officers to perform within their specific site procedures and/or the licensing documents?	Recommend changing "Security Requirements" to "Security Plan Requirements".
Page 52, Section 5.3 (cc)	"discovery of contraband material outside the PA or inside a designated vehicle barrier or control point that does not constitute a threat or potential threat to the facility." The highlighted "or" should be changed to an "and." Consideration needs to be made regarding sites that allow the admittance of firearms/contraband onto site property.	Recommend replacing "or" with "and".
Page 52, Section 5.3 (ff)	"unplanned missed cyber vulnerability assessments." It is not clear what this example is attempting to convey. Is it (1) a planned cyber vulnerability assessment that is inadvertently missed or is it (2) a planned random cyber vulnerability assessment that is missed, or (3) a cyber vulnerability assessment that is	Please clarify.

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

	performed late?	
Page 53, Section 6.1 (c)	Ammunition is outside of the scope of the contraband definition; however, as it relates to logging events, ammunition is also outside of the criterion for not logging prohibited items.	Recommend rewording Section 6.1, c. as follows: "discovery of weapons/ammunition found during entrance searches to a facility, provided the licensee concludes the individual had no malevolent intent"
Page 53, Section 6.1 (c)	This would provide the NRC the opportunity to ensure that this activity is not indicative of a pattern of suspicious behavior and is isolated to the site reporting.	Recommend this example be moved to Section 2.6 to be reported within 8 hours in accordance with 10 CFR 73.71(f).
Page 54, Section 6.2	This section is not loggable and for continuity purposes, should follow the sections for not loggable; increase clarity for the end user.	Recommend Section 6.2 be moved to Section 5.4.
Page 54, Section 6.2 (c), (e)	If the event is not reportable, then the 1-hour determination does not apply.	Recommend deleting 1-hour determination criteria.
Page 55, Section 6.2 (k)	This example, if not reported, could serve to desensitize the diligence of the security force.	Recommend (k) be deleted.
DG-5019/ Page 56, "Implementation"		Recommend that NUREG-1304 be withdrawn until Revision 1 is available for issue, in order to avoid conflicting guidance following the issuance of RG 5.62, Revision 2.
General Comment on Glossary	All definitions contained in the Glossary should be synchronized with applicable with code requirements, RGs and other documents (e.g. RG 5.76, NEI 03-12,	N/A

Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019

	etc.).	
Glossary, Covered Weapons	The definition of Covered Weapons includes items not normally considered weapons, such as ammunition and feeding device.	Recommend rewording as follows: "--any handgun, rifle, shotgun, short-barreled shotgun, short-barreled rifle, semiautomatic assault weapon, machine gun. Covered weapons include both enhanced weapons and standard weapons."
Glossary, Contraband	The first sentence in the definition is not consistent with the discussion in Section 2.3, third paragraph.	Recommend deleting this sentence.

~~SECURITY RELATED INFORMATION – WITHOLD FROM PUBLIC DISCLOSURE~~

Access Authorization/PADS Advisory Task Force Comments to DG-5019

Document/Section/ Page Reference	Comment	Suggested Wording/Revision
Page 7, Section C, 1st paragraph	First paragraph states: The NRC requires licensees and certificate holders to provide timely reports of security events. As soon as a security event is recognized, it becomes reportable within the timeframe specified. The time to report the event is based on the licensee's or certificate holder's "time of discovery," as opposed to the time a licensee or certificate holder concludes that a reportable event has occurred. A licensee's or certificate holder's initial analysis of an event could take several days to reach a conclusion on the reportability of a specific event. Therefore, the time period for reporting an event starts at the time of discovery. Many of the physical security events would definitely warrant this immediate reporting, but the Access Authorization type of issues are typically not time sensitive and believe would cause numerous unnecessary burden on licensees, certificate holders, and the NRC by immediate reporting and then subsequent retractions if there is not time to evaluate what the situation is. NRC requirements require us to evaluate intent and this process does not allow the access authorization group to make that evaluation or take this into consideration. NEI 03-01, revision 3, endorsed by Regulatory Guide 5.66 revision 1 section 6.1.b.4 states: **4.The reason for inconsistencies detected through review of collected**	The NRC requires licensees and certificate holders to provide timely reports of security events. As soon as a security event requiring 15 minute reporting is recognized and other 1 hour, 4 hour and 8 hour **(excluding unescorted access authorization process potentially reportable issues)** events, it becomes reportable within the timeframe specified. The time to report the event is based on the licensee's or certificate holder's "time of discovery," as opposed to the time a licensee or certificate holder concludes that a reportable event has occurred. A licensee's or certificate holder's initial analysis of an event could take several days to reach a conclusion on the reportability of a specific event. Therefore, the time period for reporting an event starts at the time of discovery.

Access Authorization/PADS Advisory Task Force Comments to DG-5019

Document/Section/ Page Reference	Comment	Suggested Wording/Revision
	information, i.e., intentional, innocent, or an oversight. Willful or intentional acts of omission or untruthfulness would be grounds for denial of UAA/UA. Only after this review has been completed would we then know if a report is warranted due to a denial situation. Typically upon discovery the individual's unescorted access is immediately placed on a hold status and the potential threat is no longer an issue and then the investigation is conducted for reportability. In addition there are several references that include a timeframe that if determined are not suspicious, need not to be reported, contradicts this.	
Page 17, Section 2.3, 2nd paragraph	Second paragraph states: Generally, these events relate to committed or attempted acts and credible threats involving theft or diversion of SSNM or SNM; significant physical damage to the facilities identified above; interruption of normal operation of a facility caused by unauthorized operation or by tampering with controls, safety related and non-safety-related structures, systems, and components (SSCs); unauthorized entry of personnel into a PA, VA, MAA, or CAA; malevolent attempted entry of personnel into a PA, VA, MAA, or CAA; actual or attempted introduction of contraband into a PA, VA, MAA, or CAA; actual or attempted introduction of explosives or incendiaries beyond a vehicle barrier system; or an uncompensated vulnerability, failure, or degradation of security systems that could allow unauthorized access of	Recommend rewording as follows: "unauthorized entry of personnel (ie., intruder or a person under escort (e.g., visitor) who intentionally gets separated from their escort) into a PA, VA, MAA, or CCA.

Access Authorization/PADS Advisory Task Force Comments to DG-5019

Document/Section/ Page Reference	Comment	Suggested Wording/Revision
	personnel or contraband. The only challenge in this section is the comment of "unauthorized entry of personnel into a PA, VA, MAA or CCA". The term "unauthorized" is being mis-interpreted and is not an individual who has been authorized unescorted access and then subsequently fails to meet a qualification required to maintain that status. Unauthorized has always meant that an individual with intent to circumvent the process, similar to an intruder or a person under escort (e.g., visitor) who intentionally gets separated from their escort.	
Page 23, Section 2.3.2 (w)	Section states: incomplete or inaccurate preauthorization screening that could have resulted in unescorted access authorization, had the screening been complete and accurate (involving either the authorization or the granting of unescorted access) The term pre-authorization does not exist. It should be pre-access, but also if the incomplete or inaccurate pre-access screening did not "could have" resulted in unescorted access or unescorted access authorization there is no issue and do not understand the vulnerability since the event did not result in the interruption of facilities operation. The proposed language is what was proposed by the NRC for licensee guidance prior to issuance RG 5.62	incomplete or inaccurate pre-access screening events involving licensee program failure that did result in unescorted access authorization (UAA) or unescorted access (UA), had the screening been complete and accurate the individual would have been denied UAA/UA (involving either the authorization or the granting of unescorted access). A failure to perform an appropriate evaluation *or* background investigation so that information relevant to the access determination was not obtained or considered and as a result a person, who would have been denied access by the licensee if the required investigation or evaluation had been performed.
Page 47, Section 5, last paragraph	Last paragraph states: Events recorded in the safeguards event log include failures, degradations, or discovered	Events recorded in the safeguards event log include failures, degradations, or discovered vulnerabilities that could have allowed

Access Authorization/PADS Advisory Task Force Comments to DG-5019

Document/Section/ Page Reference	Comment	Suggested Wording/Revision
	vulnerabilities that could have allowed unauthorized or undetected access to any area (e.g., **OCA**, PA, VA, MAA, or CAA) if compensatory measures were not in place or implemented at the time of discovery. There is no requirement to restrict access and account for unauthorized or undetected OCA access.	unauthorized or undetected access to any area (e.g., PA, VA, MAA, or CAA) if compensatory measures were not in place or implemented at the time of discovery.
Page 50, Section 5.1 (g)	Section states: an individual who is incorrectly (i.e., through an error not amounting to falsification) authorized unescorted access to a controlled area but was not actually granted access through the issuance of control media (e.g., badge, key, key card) This seems to imply 1) that if there is falsification than it would be considered a 1 hour report, but there is nothing in the 1 hour reporting that addresses falsification. Believe that the NRC guidance currently established for these types of events has been successfully capturing the events with the appropriate level of NRC notification. A licensee cannot prevent a person from falsification of information so as long as the there is no licensee program failure and completed all required activities, this should be considered a 24 hour loggable event. Also prior to the examples it references that this example would fall under the category for failure of a security system that could have allowed for unauthorized or undetected access, had compensatory measures not been established.	Incomplete or inaccurate pre-access screening events involving licensee program failure that did result in unescorted access authorization (UAA) or unescorted access (UA), had the screening been complete and accurate the individual would not have been denied UAA/UA (involving either the authorization or the granting of unescorted access). A failure to perform an appropriate evaluation *or* background investigation so that information relevant to the access determination was not obtained or considered and as a result a person, who would not have been denied access by the licensee if the required investigation or evaluation had been performed.
N/A	New wording to be added to section 5.1 under 24 hour loggable event since there is no clear guidance for this	For cases of deliberate falsifications where the licensee denies access either because of the

Access Authorization/PADS Advisory Task Force Comments to DG-5019

Document/Section/ Page Reference	Comment	Suggested Wording/Revision
	as stated above.	fa1sified information or because of the falsification itself and the case involves: a) deliberate falsification to gain UAA/UA on this occurrence or repeated occurrences. e.g., has falsified information at other sites, b) the individual has stated that he will falsify information in the future. e.g., shows no remorse, c) the individual falsifies his identity.
N/A	New wording to be added under section 6.2 since there is no clear guidance for this as stated above.	For cases of deliberate falsifications where the licensee would have granted access regardless of the falsified information.
Page 52, Section 5.3 (bb)	Section states: termination of personnel whose job duties and responsibilities actively support the licensee's or certificate holder's insider mitigation program On page 51 between 5.3.o and 5.3.p are the following words that apply to section 5.3.bb: The following are examples of other threatened, attempted, or committed acts not previously defined in Appendix G that should be recorded in the licensee's or certificate holder's safeguards event log and that reduced or could have reduced the effectiveness of the physical protection program or cyber security program below that described in the licensee's or certificate holder's NRC-approved physical security plans or cyber security plans. Why is termination of person whose job duties and responsibilities actively support the insider mitigation	Delete; no basis for this unless the individual attempted to tamper or sabotage and then it is already covered under another reporting requirement.

Access Authorization/PADS Advisory Task Force Comments to DG-5019

Document/Section/ Page Reference	Comment	Suggested Wording/Revision
	program an example of threatened, attempted or a committed act that would need to be a 24 hour loggable event?	
N/A	Add to Glossary on page 57 the definition for "authorized unescorted access"	Authorized Unescorted Access- status in the access authorization process that the individual satisfactorily completed all required elements for unescorted access which were evaluated by a licensee reviewing official who then made a favorable determination relative to the individuals trustworthiness and reliability and was then granted access based on a licensee authorizing the access.
Page 60-61 Glossary Definition for Unauthorized Person	**Unauthorized Person**—any person who gains unescorted access to any area for which the person has not been authorized access. This includes otherwise authorized persons gaining access in an DG-5019, Page 61 unauthorized manner, such as circumventing established access-control procedures by tailgating behind an authorized person. Expand definition to unauthorized since the whole document references unauthorized persons, vehicles items and only unauthorized person was addressed.	Unauthorized – any person, vehicle or item that gains access to any area, item or system for which the person, vehicle or item has not been authorized access through the unescorted access process or by a cognizant individual with the authority to allow access into or use of the area, system or item. This does not include when an individual fails an element that is required to maintain the authorization status where there is no malevolent intent.
N/A	Add to Glossary on page 57 the definition for "authorized". There is no reference of what authorized means for an individual, vehicle or item into an area, or system and is referenced numerous times throughout the whole document.	Authorized – Approval by a cognizant individual with the authority to grant approval to allow a person, vehicle or item with the appropriate credentials, need and/or screening to have access to an item or be allowed into an area or system.

~~SECURITY RELATED INFORMATION – WITHOLD FROM PUBLIC DISCLOSURE~~

Access Authorization/PADS Advisory Task Force Comments to DG-5019

Document/Section/ Page Reference	Comment	Suggested Wording/Revision

~~OFFICIAL USE ONLY - SECURITY-RELATED INFORMATION~~

Industry Cyber Security Comments on Part 73 Rulemaking on Event Notifications and DG 5019

Document Section/Page Reference	Comment	Suggested Wording or Markup
General comment	The application of compensatory measures as criteria for determining the level of reportability for cyber attacks does not appear to be a workable solution. There are no compensatory measures delineated in the Cyber Security Plan. The definition for "uncompensated" in the Cyber Security Plan is related to cyber measures that have not been employed. Therefore, use of compensatory measures to determine reportability of cyber security events does not work. The industry Cyber Security Task Force is providing an alternate proposal for reporting criteria for cyber events.	See attachment 1 to this document.
Cyber Security Plans/ RG 5.71	General Comment: The Physical Security Plan contains criteria to provide licensees guidance to differentiate which events are reportable or recordable. The Cyber Security Plan Templates, NEI 08-09 R. 6 or RG 5.71 do not contain guidance therefore reportability or recordable event criteria is not included in the licensee Cyber Security Plans.	The licensee Cyber Security Plan does not specify what represents adequate compensatory measures for the different types of discovered vulnerabilities nor the time frame to implement these compensatory measures. Therefore, an effective determination of what constitutes compensated or uncompensated is not currently an achievable objective, from a reporting perspective. No guidance exists therefore; it is not possible to differentiate which cyber security events are reportable ~~or~~ versus which are recordable.
10 CFR 73.73 and 10CFR 73 Appendix G	General comment: Neither 10CFR 73.71 nor Part 73 Appendix G indicates a date of effectiveness for cyber security.	The licensee Cyber Security Plan Implementation Schedule establishes the date the licensee has committed to have a Cyber Security Program in place. Prior to that date the licensee will be establishing and implementing the Program and aspects of some security

Industry Cyber Security Comments on Part 73 Rulemaking on Event Notifications and DG 5019

Document Section/Page Reference	Comment	Suggested Wording or Markup
		controls may not be fully addressed. Because these security controls may not be fully addressed, some CDAs may be subject to the reporting or recording requirements in Appendix G. This could result in reporting or recording conditions in a manner that is not intended. The reporting and recording requirements for cyber security should align with the date the Cyber Security Program is in effect.
General Comment	CDAs that are not part of the target set should not have the same sensitivity as those that make up part of a target set.	Where referencing one hour reports relative to CDAs – change to CDAs that are part of a target set.
Appendix G I. (h)(1)	Recommend rewriting as follows: Any event in which there is reason to believe that a person has committed or caused~~, or attempted to cause~~, or has made a **credible** threat to commit or cause, a~~n~~ **malicious** act to modify, destroy, or compromise any systems, networks, or equipment that falls within the scope of § 73.54 of this part **where a compromise of these plant systems has resulted or could result in radiological sabotage (i.e. significant core damage) and therefore has the potential to adversely impact the public health and safety.**	The expression, "or attempted to cause" has been removed. There is no direct corollary between an "attempt" in physical security and cyber security. A broad interpretation of "attempt" could include network probes that can occur thousands of times per day. The Regulatory Analysis in DG-5019 articulates that, "The intrusions, which require a one hour notification time, are assumed by the NRC staff to occur on average once every 2 years, or at a rate of 0.5 per year." The proposed modification is consistent with the intent of the rule and with the regulatory analysis - to report cyber attacks that have a direct impact to plant operations. Attempted cyber attacks would be reported in other reporting or recording categories. The clarification to tie the threat's impact to radiological sabotage is proposed to maintain alignment with the intent of §

Industry Cyber Security Comments on Part 73 Rulemaking on Event Notifications and DG 5019

Document Section/Page Reference	Comment	Suggested Wording or Markup
		73.54 and is consistency with RG 5.71, Section 3.1.3, "Identification of Critical Digital Assets."
Appendix G I. (h)(2)	Recommend rewriting as follows: Uncompensated cyber security events. Any failure, degradation, or the discovered vulnerability in ~~systems, networks, and equipment that falls within the scope of § 73.54 of this part~~ **the defense-in depth protective strategies implemented in accordance with § 73.54 (c)(2)**, for which compensatory measures have not been employed and that ~~could~~ **would** allow unauthorized or undetected access into such systems, networks, or equipment **that fall within the scope of §73.54**.	The expression, "systems, networks, and equipment that falls within the scope of § 73.54 of this part" is not corollary with the use of the expression "safeguards systems" with respect to physical security reporting. The clarification to "the defense-in depth protective strategies implemented in accordance with § 73.54 (c)(2)" maintains alignment with the Cyber Security Rule and is consistent with the use of the term "safeguards systems" for reporting of uncompensated physical security events. The term "could" changed to "would" to maintain alignment with 10 CFR 73.54 (a)(2). The expression "that fall within the scope of § 73.54" added for clarity.
Appendix G I. (c)(1)	Recommend rewriting as follows: Any information received or collected by the licensee or certificate holder of suspicious **or surveillance** activity ~~that may be indicative of tampering, malicious or unauthorized access, use, operation, manipulation, modification, potential destruction, or compromise~~ **or attempts at access** of the systems, networks, and equipment that falls within the scope of § 73.54 of this part, or the security measures that could weaken or disable the protection for such systems, networks, or equipment.	The words "or surveillance" added to maintain alignment with the intent of four hour reportable physical security events. The expression, "that may be indicative of tampering, malicious or unauthorized access, use, operation, manipulation, modification, potential destruction, or compromise" has been removed. This is illustrative text that is confusing, and does not add clarity. Added the words, "or attempts at access" to eliminate the need for the draft Section (c)(2).

Industry Cyber Security Comments on Part 73 Rulemaking on Event Notifications and DG 5019

Document Section/Page Reference	Comment	Suggested Wording or Markup
Appendix G I. (c)(2)	~~An attempted but unsuccessful cyber attack or event that could have caused significant degradation to any system, network, or equipment that falls within the scope of § 73.54 of this part.~~	Paragraph II, Section (c)(2) appears to be unnecessary. This section clarifies Paragraph I, Section (h)(1) and Paragraph II Section (c)(1). In our comments, we have proposed modifications to Paragraph I, Section (h)(1) and Paragraph II Section (c)(1) that eliminate the need for this Section (c)(2).
10 CFR 73.71(f)	Recommend rewriting as follows: Each licensee subject to the provisions of §§73.20, 73.45, 73.46, 73.50, 73.51~~,~~ ~~73.54~~, 73.55, 73.60, or 73.67 shall notify the NRC Headquarters Operations Center, as soon as possible but not later than eight hours after discovery of the safeguards events described in paragraph III of Appendix G to this part.	Industry proposes to incorporate the cyber security-related four hour reportable events into the eight hour reportable events. This proposed revision to 10 CFR 73.71(f) is a conforming change, as no cyber security events would remain in the four hour reporting requirements in Appendix G to Part 73.
Appendix G III. (3)	Recommend rewriting as follows: The tampering **with**, malicious or unauthorized access, use, operation, manipulation, or modification of any **cyber** security ~~measures associated with systems, networks, and equipment~~ **controls used to protect the assets** that falls within the scope of § 73.54 of this part, that does not result in the interruption of the normal operation of such systems, networks, or equipment.	The proposed clarification ensures alignment with the requirements of 10 CFR 73.54 (c)(1), "Implement security controls to protect the assets identified by paragraph (b)(1) of this section from cyber attacks." ~~These events can be incorporated with the events identified for eight hour reporting. It is unnecessarily confusing to separate suspicious events from tampering events with respect to cyber security. The proposed Paragraph III, Section (3) may be incorporated as a replacement to Paragraph II, Section (c)(2).~~
Appendix G IV. (a)(2)	Recommend rewriting as follows: Degrade the effectiveness of the	The words "that would" have been added to maintain alignment with Paragraph I,

Industry Cyber Security Comments on Part 73 Rulemaking on Event Notifications and DG 5019

Document Section/Page Reference	Comment	Suggested Wording or Markup
	licensee's or certificate holder's cyber security program ~~or~~ **that would** allow unauthorized or undetected access to any systems, networks, or equipment that fall within the scope of § 73.54 of this part. ~~Decreases in the effectiveness of the cyber security program include any other threatened, attempted, or committed act not previously defined in this appendix that has resulted in or has the potential for decreasing the effectiveness of the cyber security program in a licensee's or certificate holder's NRC-approved cyber security plan.~~	Section (h)(2). The second sentence is struck as a duplication of Paragraph IV, Section (e).
App G / DG-5019/ 19, 27 I(h)(2)	The use of the word "uncompensated" is not clear as it relates to cyber security.	Physical security interprets "uncompensated" to mean a temporary measure was not applied in the event of a cyber attack. Cyber security interprets "uncompensated" to mean one or more security control(s) were not applied, or not properly applied.
App G / DG-5019/ 19, 27 I(h)(2)	The use of the word "compensatory" is not clear as it relates to cyber security.	Physical security interprets "compensatory" to mean a temporary measure was applied in the event of a cyber attack. Cyber security interpretation is unclear as "compensatory" could mean one or more security control(s) were not applied, or not properly applied.
DG-5019	Remove terms such as "could," "likelihood," or "likely to".	Paragraph 4 of Section 2.3 states "Reports made under this provision apply to power reactor facilities ...regarding the discovery that a cyber attack has occurred or has been attempted..." Use of words such as "could," "likelihood," or "likely to" are not

Industry Cyber Security Comments on Part 73 Rulemaking on Event Notifications and DG 5019

Document Section/Page Reference	Comment	Suggested Wording or Markup
		consistent with guidance in section 2.3 paragraph 4.
App G/ DG-5019/ 27, 30 I(h)	Change "Cyber security events." to "Significant Cyber Events".	Align with Physical Security in 10CFR73 App G I(a).
App. G / DG-5019/ 19, 27 I(h)(2)	Change "...could allow unauthorized access..." to "...would allow unauthorized access..."	10CFR73.54(a)(2) states "... protect [SSEP] systems and networks ... from cyber attacks that would: [adversely impact operation of SSEP]. The regulation is definitive in the use of the word "would." The word "could" is not definitive therefore would required constant reporting of potential unauthorized access resulting in a burden to the NRC and the licensee.
App. G / DG-5019/ 19, 27 II(c)(2)/ 2.5.2.(2)(c)(2)	Remove.	Duplicate of I(h)(1) which addresses "attempted" threats. If II(c)(2) remains, there is conflicting regulation regarding attempted attacks or events.
DG-5019/19 2.3.1 (h)(2)	Change "...have not been employed and that could allow..." to "... have not been employed and that allowed a cyber attack to be promulgated as a result of unauthorized..."	10CFR73.54(a)(2) states "... protect [SSEP] systems and networks ... from cyber attacks that would: [adversely impact operation of SSEP]. The regulation is definitive in the use of the word "would." The word "could" is not definitive therefore would required constant reporting of potential unauthorized access.
DG-5019/22 2.3.2.r.(2)	Rewrite as follows: Confirmed cyber attacks on computer systems that ~~may~~ adversely affect**ed** safety, security, and emergency preparedness systems are reportable.	Maintain alignment with r, "security events that involve an interruption of the normal operation".

Industry Cyber Security Comments on Part 73 Rulemaking on Event Notifications and DG 5019

Document Section/Page Reference	Comment	Suggested Wording or Markup
DG-5019/23 2.3.2.aa	...~~the successful, surreptitious penetration or compromise of a critical digital asset (CDA) by unauthorized personnel~~	Remove – redundant to 2.3.2.r.(2).
DG-5019/23 2.3.2.bb.(2)	Rewrite as follows: Licensees and certificate holders should report actual entries that are the result of an intentional act or breakdown of the **cyber** security program or **cyber** security measures.	Added "cyber" for clarity.
DG-5019/23 2.3.2.bb.(3)	Rewrite as follows: If the licensee or certificate holder concludes that the actions of the individual were inadvertent and did not threaten facility security, it may record this event in the safeguards event log. However, ~~if the event represents an uncompensated degradation or vulnerability that could allow intentional undetected or unauthorized access to SSEP functions, the licensee or certificate holder should make a 1-hour notification.~~**events related to failures and degradations causing an adverse impact to a CDA SSEP function subsequently determined to be a result of a cyber attack as described in 10CFR 73 Appendix G Paragraph I.(h)(1) are to be reported within one hour of discovery**.	Struck text is clarified by proposed new text.
DG-5019/23 2.3.2.bb.(4)	~~Attempts by unauthorized persons means that reliable and substantive information indicates that (1) an effort to accomplish the cyber attack, even though it has not yet occurred, is~~	Covered by four-hour reporting and suggest moving to eight hours, including 2.5.2.kk.

Industry Cyber Security Comments on Part 73 Rulemaking on Event Notifications and DG 5019

Document Section/Page Reference	Comment	Suggested Wording or Markup
	~~possible, or (2) the cyber attack was not successful because it was interrupted or stopped before completion.~~	
DG-5019/24 2.3.2.bb.(5)	~~Licensees or certificate holders should report a cyber attack that was thwarted by responders or other security system elements if a successful attack would have had an adverse impact on SSEP functions.~~	Covered by four-hour reporting and suggest moving to eight hours.
DG-5019/24 2.3.2.cc	Rewrite as follows: ...the discovery of malware~~, unauthorized software, or firmware~~ installed on a CDA	Struck language is redundant.
DG-5019/24 2.3.2.dd	Rewrite as follows: ...failures, degradations, or discovered vulnerabilities of CD As or security measures that protect CDAs that would ~~be likely to~~ allow unauthorized or undetected access to those CDAS ~~or~~ that ~~could~~ **would** result in ~~compromising the CDA or~~ an **adverse impact to** SSEP function when compensatory measures have not been employed (i.e., uncompensated)	Changes proposed to clarify example and maintain alignment with 10 CFR 73.54(a)(2).
DG-5019/24 2.3.2.ee	...~~the theft of sensitive cyber security data~~	There are no NRC regulations covering "sensitive cyber security data".
DG-5019/24 2.3.2.ff	Rewrite as follows: ...the loss of cyber intrusion detection capability ~~that is uncompensated in accordance with the facility's NRC-approved cyber security plan~~ **that would allow unauthorized or undetected access to a CDA**	For clarity; what is cyber intrusion detection system?

Industry Cyber Security Comments on Part 73 Rulemaking on Event Notifications and DG 5019

Document Section/Page Reference	Comment	Suggested Wording or Markup
DG-5019/24 2.3.2.gg	...~~the failure to adequately compensate, in a timely manner, for an event or identified failure, degradation, or vulnerability that could allow undetected or unauthorized access or modification to a CDA~~	Redundant to 2.3.2.hh
DG-5019/24 2.3.2.hh	Rewrite as follows: ...~~an uncompensated~~ a design flaw or vulnerability in a cyber protection system that ~~could have~~ **would** allowed unauthorized access to CDAs or ~~could have~~ substantively eliminated or significantly reduced the licensee's response capabilities	Maintain consistency with 10 CFR 73.54(a)(2).
DG-5019/24 2.3.2.ii	...~~cyber security events that could allow undetected or unauthorized access or modifications to CDAs within 1 hour, that usually affect multiple layers of cyber security systems or an individual, critical, single failure of a program element that would allow undetected or unauthorized access to CDAs~~	Redundant to 2.3.2.hh.
DG-5019/24 2.3.2.jj	...~~the discovery of falsified identification badges, key cards, or other access-control devices that could allow unauthorized individuals access to CDAs~~	Moved to 2.5.2, below.
DG-5019/24 2.3.2.kk	...the discovery of improper control over access-control equipment (e.g., badge fabrication, access-control computers, key cards, passwords, cipher codes), if the event results in the actual or attempted use of the equipment or media where an unauthorized individual ~~could~~ **would** or did gain entry to a CDA	Maintain alignment with 10 CFR 73.54(a)(2).
DG-5019/24 2.3.2.ll	...~~the uncompensated loss of all ac power to security systems that could~~	Redundant to 2.3.2.hh.

Industry Cyber Security Comments on Part 73 Rulemaking on Event Notifications and DG 5019

Document Section/Page Reference	Comment	Suggested Wording or Markup
	~~allow unauthorized or undetected access to a CDA~~	
DG-5019/24 2.3.2 mm	Remove.	Duplicate of 2.3.2.y. Safeguards reporting requirements have been established in previous section of the DG; this is a redundant sentence and should be deleted.
DG-5019/24 2.3.2.nn	...~~the unavailability of the minimum number of cyber security response personnel after implementation of the appropriate recall procedures~~	There are no NRC regulations to maintain staffing levels for "cyber security response personnel".
DG-5019/24 2.3.2 oo	Change "...could increase the likelihood of an attempted attack..." to "... would result in an attack..."	10CFR73.54(a)(2) states "... protect [SSEP] systems and networks ... from cyber attacks that would: [adversely impact operation of SSEP]. The words "increase the likelihood" is not definitive therefore would require constant reporting of potential likelihood of attempted attack.
DG-5019/30 2.5.2.## (new)	...the discovery of unauthorized user ids, the unexplained absence of event log, the unauthorized configuration change of a cyber control element (e.g. firewall port opening, account lockout threshold)	Moved from 2.3.2.jj.
DG-5019/30 2.5.2. ## (new)	Rewrite as follows: ...unauthorized attempts to probe or gain access ~~to the licensee's or certificate holders business secrets or other sensitive information or~~ to control CDAs including the use of social engineering techniques (e.g. impersonating authorized users)	Derived from 2.5.2.j to represent the cyber threat.
DG-5019/33 2.5.2.kk	Rewrite as follows: ...the discovery of individuals with	To add clarity.

Industry Cyber Security Comments on Part 73 Rulemaking on Event Notifications and DG 5019

Document Section/Page Reference	Comment	Suggested Wording or Markup
	uncommon interests or inquiries related to the facility's cyber security measures, personnel, or **cyber** security controls	
DG-5019/33 2.5.2.mm	Rewrite as follows: ...~~the discovery of individuals eliciting or attempting to elicit information from security or other facility personnel regarding CDAs, security measures, or vulnerabilities for SSEP functions~~	Redundant to 2.5.2.kk.
DG-5019/33 2.5.2.oo	Rewrite as follows: ...the discovery of the use of forged, stolen, or fabricated smart cards, tokens or other "two factor" authentication devices used to support access control to **Level 3 or Level 4** CDAs or authorization activities	To add clarity consistent with definition of CDA in the Glossary.
DG-5019/33 2.5.2.pp	Rewrite as follows: ~~the discovery of unsubstantiated cyber attack threats that are considered to be related to harassment, including threats that could also represent tests of response capabilities or intelligence-gathering activities, or an attempt to disrupt facility operations (to be recorded in the safeguards log until a pattern is discovered)~~ ...the discovery of a pattern of activity in the ~~safeguards event log~~ CAP that may be indicative of a cyber attack	A review of the CAP would reveal this pattern.
DG-5019/33 2.5.2.qq	Rewrite to "discovery of an active attack on a network adjacent that is capable of adversely affecting CDAs or SSEP functions", or consider deleting altogether.	Networks that have security barriers in place (such as the networks for CDAs which are deterministically segregated) are secure from virus or worm as well as an attack on the lower security level, un-

Industry Cyber Security Comments on Part 73 Rulemaking on Event Notifications and DG 5019

Document Section/Page Reference	Comment	Suggested Wording or Markup
		trusted network where the attack could be occurring. Computer systems and networks subject to 73.54 with security controls in place, are protected from malware that may be on adjacent networks in a lower security level. Reporting the high number of malware attempts on these lower security level networks that do not have the degree of protection afforded CDAs would be burdensome for the regulator and licensee. By focusing on networks not subject to 73.54, the licensee's focus on reporting instead of focusing on practical security measures could distract personnel from their core mission of protection.
DG-5019/33 2.5.2.rr	Rewrite as follows: Information that a compromise of ~~cyber systems~~ **a CDA** has occurred but without the licensee or certificate holder experiencing any degradation of SSEP functions ~~(although recommending that the licensee or certificate holder investigate the extent of the compromise to discover if any CDAs or SSEP functions have been affected)~~	"Cyber systems" clarified to "CDA" for clarity. Parenthetical encompasses a staff recommendation inconsistent with the intent of this proposed RG.
DG-5019/34 2.5.2.SS	Remove "...15 minute or..."	15-minute notification is not specified in 10CR73.71(a) for 10CFR73.54.
DG-5019/35 2.6.2.h	Remove.	The introductory paragraph states "...unauthorized operation or manipulation of or tampering with networks or equipment within scope of 10CR73.54..." The discovery of a "...vulnerability in a

Industry Cyber Security Comments on Part 73 Rulemaking on Event Notifications and DG 5019

Document Section/Page Reference	Comment	Suggested Wording or Markup
		CDA or security measures, but with compensatory measures in place..." does not indicate unauthorized activity. If unauthorized activity were involved the compensatory measures would have been compromised too. The section is generally confusing and should be deleted.
DG-5019/35 2.6.2.i	Change "...is disabled or has failed..." To "...is disabled ..."	There are many reasons why a CDA could be in a failed state such as equipment obsolescence, environmental issues, or inadvertent, non-malicious human performance for example. It is burdensome on the NRC and the licensee to report equipment degradation as a facility security event unless there is an indication that unauthorized activity was the cause. The condition for "failed" is addressed in 5.3.n.
DG-5019/51 5.3.n	Rewrite - "The discovery that a CDA has failed but does not degrade an SSEP function".	By removing the term "compensated" which is not clear when discussing cyber security, the re-write clarifies that CDA failures that do not adversely impact SSEP functions are recordable.
DG-5019/51 5.3.o	Rewrite as follows: "An individual who was inappropriately granted access to a CDA or who was incorrectly authorized access to a CDA but who could not actually access the CDA".	This is difficult to understand as written; the rewrite suggested may not completely clarify the intent.
App. G, DG-5019/51 5.3.m, n, and o	In the Cyber Security Plan there is no commitment or requirement to record cyber events in a safeguards event log. In section 4.9.4, the Cyber Security Plan describes how the Corrective Action	Is it possible to use the CAP as the safeguards event log through the use of trend codes assigned to non-conformances associated with conditions noted in DG-5019?

Industry Cyber Security Comments on Part 73 Rulemaking on Event Notifications and DG 5019

Document Section/Page Reference	Comment	Suggested Wording or Markup
	Program is used.	
DG-5019/50 5.3. ## (new)	Compensated cyber security event.	Capture events that are compensated, as required by Appendix G, Paragraph IV, Section (a).
DG-5019/57 Glossary	Add definition for Cyber Attack: Any event in which there is reason to believe that an adversary has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause malicious exploitation of a CDA.	This is the definition found acceptable by the NRC as documented in a USNRC letter from Richard P. Correia to Christopher E. Earls, *Nuclear Energy Institute 08-09, "Cyber Security Plan Template, Rev. 6,"* dated June 7, 2010. This definition is included in the industry Cyber Security Plans and is different than the definition in RG 5.71.
DG-5019/57 Glossary	Critical Digital Asset; change the definition to the following: Digital computer or communications systems or networks that fall within the scope of 10CFR73.54 (i.e. within the Level 3 or 4 boundaries described in Regulatory Guide 5.71). Such digital computer or communications systems or networks have the ability to compromise the facility's safety, security, or emergency response (SSEP) functions.	"Electronic systems" go well beyond the scope of 10CFR73.54 and could include plant equipment that does not have digital characteristics. As stated, the text aligns with 10CFR73.54(a).

Industry Cyber Security Comments on Part 73 Rulemaking on Event Notifications and DG 5019

ATTACHMENT 1

White Paper on Proposed Reporting of Cyber Security Events

1 REPORTING OF CONFIRMED CYBER SECURITY ATTACKS

10CFR 73.71 and 10CFR73 Appendix G address both physical and cyber security. Proposals contained within this document are limited to cyber security. Any physical security comments will be provided by the Nuclear Energy Institute and licensees separately.

10 CFR 73.71 has been revised to require reporting and recording of cyber security events. The proposed language in §73.71 requires licensees to report cyber security events to the NRC Headquarters Operations Center within one hour, four hours, or eight hours of discovery as described in 10CFR73, Appendix G. Any decrease in effectiveness in the cyber security program is recordable as described in 1CFR73 Appendix G.

2 ONE-HOUR REPORTING REQUIREMENTS

10CFR 73 Appendix G Paragraph I.(h)(1) and I.(h)(2) establish criteria for one hour reportability.

Consistent with the DG-5019 Glossary, the industry proposes the one hour reportability requirement be established for cyber attacks that adversely impact SSEP functions for CDAs that reside in cyber security Level 3 or Level 4. Industry proposes Cyber attacks are defined in §73 Appendix G Paragraph I.(h)(1) with the following modification:

*Any event in which there is reason to believe that a person has committed or caused, or attempted to cause, or has made a **credible** threat to commit or cause, a **malicious** act to modify, destroy, or compromise any systems, networks or equipment that falls within the scope of §73.54 of this part.*

Industry proposes that 10CFR 73 Appendix G Paragraph I.(h)(2) be rewritten for the reasons cited below:

1. Using the term "Uncompensated" in the cyber security context introduces uncertainty. "Uncompensated" in the physical security context means a temporary measure was not applied. Cyber security interprets "uncompensated" to mean one or more security controls were not applied or were not properly applied.
2. The term "failure" is not synonymous with attack, but in the context of this paragraph is used in as a synonym. "Failure" should be regarded as a maintenance issue initially, then, if investigation warrants, it can be declared a

suspected malicious act and reported/recorded as such.

Industry recommends that 10CFR 73 Appendix G Paragraph I.(h)(2) be rewritten to state:

Events related to failures and degradations which initially may present as a mechanical or electrical problem causing an adverse impact to a CDA SSEP function and subsequently determined to be a result of a cyber attack as described in 10CFR 73 Appendix G Paragraph I.(h)(1) be reported within one hour of discovery.

Confirmed cyber attacks are reported in accordance with existing notification procedures and actions are taken to stabilize the plant in accordance with emergency operations and imminent threat procedures. If a licensee encounters a situation in which multiple threat notification sources (e.g., FAA, NORAD, and NRC Headquarters Operations Center) are providing the same threat information, the licensee would only be required to maintain continuous communication with the NRC Headquarters Operations Center. See Table 1 for examples of One-Hour Reportable Cyber Security Events.

2 FOUR HOUR REPORTING REQUIREMENTS

3 EIGHT HOUR REPORTING REQUIREMENTS

4 RECORDABLE REQUIREMENTS

Industry Cyber Security Comments on Part 73 Rulemaking on Event Notifications and DG 5019

TABLE 1

ONE HOUR REPORTABLE CYBER SECURITY EVENT EXAMPLES

The following is the criteria for reporting confirmed cyber attacks in accordance with site procedures:

Reporting Criteria	Example
Part 73, Appendix G, paragraph I.(h)(1): *"Any event in which there is reason to believe that a person has committed or caused, or attempted to cause, or has made a* ***credible*** *threat to commit or cause, a* ***malicious*** *act to modify, destroy, or compromise any systems, networks or equipment that falls within the scope of §73.54 of this part."*	r.(2) Confirmed cyber attacks on **CDAs** that may adversely affect safety, security, and emergency preparedness **functions** are reportable. aa. [**Remove**] bb. an actual penetration or compromise of a CDA, where a person who is not authorized access circumvents the control measures (1) The regulation for reporting this type of event is not intended to suggest that simple mistakes or other inadvertent entries should be reported within 1 hour. (2) Licensees and certificate holders should report actual entries that are the result of an intentional act or breakdown of the **cyber** security program or **cyber** security measures.
Part 73, Appendix G, paragraph I.(h)(2): *Events related to failures and degradations which initially may present as a mechanical or electrical problem causing an adverse impact to a CDA SSEP function and subsequently determined to be a result of a cyber attack as described in 10CFR 73 Appendix G*	(3) If the licensee or certificate holder concludes that the actions of the individual were inadvertent and did not threaten facility security, it may record this event in the ~~safeguards~~ event log. However, *Events related to failures and degradations which initially may present as a mechanical or electrical problem causing an adverse impact to a CDA SSEP function and subsequently determined to be a result of a cyber attack as described in 10CFR 73 Appendix G Paragraph I.(h)(1) be reported within one hour of discovery.*

Industry Cyber Security Comments on Part 73 Rulemaking on Event Notifications and DG 5019

Reporting Criteria	Example
Paragraph I.(h)(1) be reported within one hour of discovery.	(4) [**Remove**] (5) [**Remove**] cc. the discovery of malware installed on a CDA dd. [**Remove**] ee. the theft of sensitive cyber security data ff. the loss of cyber intrusion detection or intrusion prevention capability that is uncompensated in accordance with the facility's NRC-approved cyber security plan gg. the failure to adequately compensate, in a timely manner, for an event or identified failure, degradation, or vulnerability that could allow ~~undetected~~ or unauthorized access or modification to a CDA [Remove or define timely??] hh. an uncompensated design flaw or vulnerability in a cyber protection system that **would allow** unauthorized access to CDAs or **would** ~~substantively~~ eliminated or **would** ~~significantly~~ reduce the licensee's response capabilities ii. cyber security events that would allow ~~undetected or~~ unauthorized access ~~or modifications~~ to CDAs within 1 hour, that usually affect multiple layers of cyber security systems or an individual, critical, single failure of a program element that would allow ~~undetected or~~ unauthorized access to CDAs [Remove???] jj. [**Remove** duplicate of 2.3.2.t] kk. [**Remove** – duplicate of 2.3.2.u] ll. [**Remove** – duplicate of 2.3.2.v] mm. [**Remove** – duplicate of 2.3.2.y]

Industry Cyber Security Comments on Part 73 Rulemaking on Event Notifications and DG 5019

Reporting Criteria	Example
	nn. [**Remove**] oo. uncompensated failures, degradations, or discovered vulnerabilities with a CDA, personnel responses, communications, monitoring, or oversight that **would result in** an attack on any CDA [Remove]