

U.S. NUCLEAR REGULATORY COMMISSION



Annotated Public Comments on: Enhanced Weapons, Firearms Background Checks, and Security Event Notifications Rule and Supporting Regulatory Guidance Documents

**NRC-2011-0014, NRC-2011-0015, NRC-2011-0017,
NRC-2011-0018; RIN 3150-AI49**

U.S. Nuclear Regulatory Commission

Office of Nuclear Security and Incident Response
Office of Nuclear Material Safety and Safeguards
Office of Nuclear Reactor Regulation
Office of Nuclear Regulatory Research

March 2023

**Technical Lead: P. Brochman, NSIR
Project Manager: S. Schneider, NMSS**

ML22287A158

Introduction

On February 3, 2011, the NRC published for public comment a proposed rule, “Enhanced Weapons, Firearms Background Checks, and Security Event Notifications,” in the *Federal Register* (76 FR 6200). Subsequently on January 20, 2013, the NRC published in the *Federal Register* for public comment a first supplemental proposed rule (78 FR 2214) and on September 22, 2015, a second supplemental proposed rule (80 FR 57106). In conjunction with the publication of the proposed rule and supplemental proposed rules, the NRC also published for public comment the following supporting draft regulatory guidance documents.

DG-5019, Revision 1, “Reporting and Recording Safeguards Events” (February 3, 2011; 76 FR 6085) (NRC’s Agencywide Documents Access and Management System (ADAMS) Accession No. ML100830413).

DG-5020, Revision 0, “Applying for Enhanced Weapons Authority, Applying for Preemption Authority, and Accomplishing Firearms Background Checks under 10 CFR Part 73” (February 3, 2011; 76 FR 6086) (ML100321956).

Draft Weapons Safety Assessment (February 3, 2011; 76 FR 6087) (ML103190273).

DG-5020, Revision 1, “Applying for Enhanced Weapons Authority, Applying for Preemption Authority, and Accomplishing Firearms Background Checks under 10 CFR Part 73” (September 22, 2015; 80 FR 57106) (ML14322A847).

This document contains all the public comment submissions on the proposed rule, the supplemental proposed rules, and the supporting draft regulatory guidance documents. These individual comment submissions may also be found in ADAMS under their respective accession numbers as specified in Table 1 below. Additionally, these public comment submissions may also be found at the Federal e-Rulemaking Website at <https://www.regulations.gov/> under Docket ID Nos. NRC-2011-0014, NRC-2011-0015, NRC-2011-0017, and NRC-2011-0018.

The NRC reviewed and annotated the comment submissions to identify what the NRC concluded were separate comments within each submission. Accordingly, a single comment submission may have several individual comments associated with it. The NRC gave each individual comment within a submission a unique identifier.

The NRC’s responses to the public comments on the proposed and supplemental rules are found in ADAMS at ML16264A004. Separately, the NRC’s responses to public comment on the supporting draft regulatory guidance documents are found in ADAMS at ML17123A319. The NRC’s response to comments identify which individual comments are addressed by each comment response using a unique identifier comprised of the “Abbreviation” identified in Table 1 below coupled with an individual comment number in the respective annotated public comment submissions; for example, ANON-2, BY-3, or GE-8.

Table 1 – Comment Submissions on Enhanced Weapons, Firearms Background Checks, and Security Event Notifications Rule and Supporting Regulatory Guidance Documents

Comment Submission Number ¹	Commenter Name	Affiliation	Abbreviation	Contains Comments On ²		Identical Comment Submission ⁵	Date	ADAMS Accession No.
				Rule ³	Guidance ⁴			
1	Anonymous	Private Citizen	ANON	Proposed			04-03-11	ML110950656
2	Ryan M. Spahr	Private Citizen	RMS	Proposed			04-17-11	ML11109A002
3	Craig J. Renitsky	Private Citizen	CR	Proposed			04-18-11	ML11110A001
4	Mark Elliott	Nuclear Fuel Services	NFS	Proposed			05-04-11	ML11130A041
5	Robert E. Andrews	Congressman– U.S. House of Representatives	RA	Proposed			05-05-11	ML11130A112
6	Brian Yip	Private Citizen	BY	Proposed			07-14-11	ML11200A092
7	Barry Cole	Babcock & Wilcox Nuclear Operating Group	B&W	Proposed	DG-5019, Rev. 1 Weapons Safety Assessment		07-25-11	ML11208B451
8	Patricia L. Campbell	GE Hitachi Nuclear Energy	GE	Proposed	DG-5019, Rev. 1	76FR6085	07-29-11 07-29-11	ML11213A210 ML11214A217
9	Roberta J. Gray	Federal Bureau of Investigation	FBI	Proposed			07-29-11	ML11216A026
10	S. Hardin	Private Citizen	SH1	Proposed			08-02-11	ML11216A027
11	R.M. Krich	Tennessee Valley Authority	TVA	Proposed			08-02-11	ML11217A106
12	David R. Kline	Nuclear Energy Institute	NEI1	Proposed	DG-5019, Rev. 1 DG-5020, Rev. 0 Weapons Safety Assessment	76FR6085 76FR6086 76FR6087	08-02-11 08-02-11 08-02-11 08-02-11	ML11229A109 ML11242A127 ML11242A126 ML11242A128
13	Anonymous	Palo Verde Nuclear Power Plant	PV		DG-5019, Rev. 1		08-02-11	ML11216A139
14	Jerry W. Moore	Vogtle Nuclear Power Plant	JM		DG-5020, Rev. 0		08-04-11	ML11220A087
15	Anthony Dimitriadis	NRC Staff	AD		DG-5019, Rev. 1		08-05-11	ML11221A139

Table 1 – Comment Submissions on Enhanced Weapons, Firearms Background Checks, and Security Event Notifications Rule and Supporting Regulatory Guidance Documents (continued)

Comment Submission Number ¹	Commenter Name	Affiliation	Abbreviation	Contains Comments On ²		Identical Comment Submission ⁵	Date	ADAMS Accession No.
				Rule ³	Guidance ⁴			
16	Michael DeAngelo	Private Citizen	MD	2013 Supplemental Proposed			01-25-13	ML13031A142
17	David R. Kline	Nuclear Energy Institute	NEI2	2015 Supplemental Proposed			12-07-15	ML15341A278
18	S. Hardin	Private Citizen	SH2	2015 Supplemental Proposed			12-07-15	ML15348A372

Notes:

1. The comment submission number corresponds to the order in which the NRC received and docketed each comment submission.
2. Some comment submissions only contained comments on the proposed rule. Some comment submissions only contained comments on the draft supporting regulatory guidance documents. Others comment submissions contained comments on both the proposed rule and draft supporting regulatory guidance documents in a single submission.
3. Comments submitted on the 2011 proposed rule and 2013 and 2015 supplemental proposed rules are dispositioned in “Response to Public Comments: Enhanced Weapons, Firearms Background Checks, and Security Event Notifications Rule,” (ML16264A004).
4. Comments submitted on DG-5020, Revision 0; DG-5019, Revision 1; and the Weapons Safety Assessment are dispositioned in “Responses to Public Comments on the Regulatory Guidance Documents Supporting the Final Rule on Enhanced Weapons, Firearms Background Checks, and Security Event Notifications” (ML17123A319). No comments were submitted on DG-5020, Revision 1.
5. Two commenters submitted identical comments in response to the separate *Federal Register* notices for the proposed rule and draft regulatory guidance.

April 5, 2011 (9:15am)

Comment Submission No. 1
(ML110950656)

OFFICE OF SECRETARY
RULEMAKINGS AND
ADJUDICATIONS STAFF

PUBLIC SUBMISSION

As of: April 04, 2011
Received: April 03, 2011
Status: Pending_Post
Tracking No. 80c1a4a9
Comments Due: May 04, 2011
Submission Type: Web

Docket: NRC-2011-0018

Enhanced Weapons, Firearms Background Checks, and Security Event Notifications

Comment On: NRC-2011-0018-0001

Enhanced Weapons, Firearms Background Checks, and Security Event Notifications

Document: NRC-2011-0018-DRAFT-0013

Comment on FR Doc # 2011-01766

Submitter Information

Name: AI N/A **(Comment-Response Document Abbreviation: ANON)**

General Comment

As a concerned citizen with an interest in proper security of nuclear/power plant or critical infrastructures I am glad to hear that of the proposed rule changes.

It is my opinion that we shall do whatever is necessary to protect all critical and sensitive locations and prevent, and deter potential attacks or security breaches.

1 At the same time, as a gun owner and someone familiar with "enhanced" weapons, I would like to be assured that these weapons are closely monitored, adequately secured and disposed of properly (by sale, transfer or destruction).

2 In addition, I am very much concerned with the proper notification of theft of such weapons and accountability of facility or security personnel in-charge of the weapons.

3 I am also concerned about the infrequent background checks of personnel "every three years" after the initial background check. Three years is a long time to wait and it should be done bi-annually rather than once every three years.

The follow up background check does not have to be extensive and could only involve various database checks.

4 The proposed event notification, should include notification to local police agencies affected by the event. After all the local police agency may suffer the consequence of any adverse action.

In closing, I am in favor of any rule that would increase and upgrade security but when it is properly administrated.

Template = SECY-067

DS 10

Rulemaking Comments

From: Gallagher, Carol
Sent: Monday, April 04, 2011 9:55 AM
To: Rulemaking Comments
Subject: Comment on Proposed Rule - Enhanced Weapons, Firearms Background Checks, and Security Event Notifications
Attachments: NRC-2011-0018-0013.pdf

Van,

Attached for docketing is a comment on the above noted proposed rule (3150-AI49) that I received via the regulations.gov website on 4/03/11.

Thanks,
Carol

RE: Enhanced Weapons, Firearms Background Checks, and Security Event Notifications

Docket ID: NRC-2011-0018 Agency: NRC RIN: 3150-AI49

DOCKETED
USNRC

April 18, 2011 (10:15am)

Submitted by Ryan M Spahr

OFFICE OF SECRETARY
RULEMAKINGS AND
ADJUDICATIONS STAFF

(Comment-Response Document Abbreviation: RMS)

1. With one strong stipulation (see point 5 below) I, as a civilian member of the public, support this proposed rule.
- 1 2. Given the realities of modern stateless terrorism, as well as the growing threat of domestic terrorism, nuclear security has never been more important to the United States' national security. This rule provides a dynamic authorization for nuclear and related facilities to protect themselves with the appropriate tools.
- 2 3. Allowing affected security personnel access to "covered weapons," allows them to respond to security threats with appropriate veracity. In addition to standard civilian firearms, the rule allows access to machine guns and short barreled rifles. Weapons in these two classes represent those normally reserved to special response-type law enforcement (such as SWAT teams). It is plainly appropriate for personnel protecting nuclear sites to engage security threats with SWAT type firepower, rather than depend on the reactive arrival of such firepower to arrive after a security threat is detected. Any nuclear site worth protecting at all is worth keeping threats out in the first place, rather than calling the police after they are already present.
- 3 4. The rule provides dynamic guidance for background checks. Any person in the US who purchases a firearm from a dealer must pass a NICS background check. Extending this requirement to security personnel handling firearms at nuclear facilities passes the "common sense" test while also taking advantage of the existing and tried-and-true NICS system instead of creating a new, parallel background checking rubric. The rule also seems to recognize that the NICS system is not perfect. It is not unusual for checkees to be "delayed" only to be approved days later. Such an occurrence does not reflect negatively on the subject of the check and functionally is the same as an outright approval. The rule recognizes this by stating that those "delayed" and later approved may then be assigned the use of the covered firearms. Further, the rule allows those who receive a "denied" response on their NICS check opportunity to appeal and reverse the response. It is possible to be "denied" for a variety of reasons as harmless as incomplete or erroneous medical or residential records. Therefore it is appropriate for the rule to allow affected persons to "clear their name" and keep their jobs.
- 4 5. The proposed rule dangerously limits the affected facilities' ability to keep their firearms in good repair. The rule appropriately allows for the affected firearms to be taken off of the premises for the purposes of training at a gun range and to provide security for the transport (in or out) of sensitive nuclear and related material. However, the rule does not allow for covered weapons to be taken off

premises for repairs without a full-scale transfer in accordance with the National Firearms Act and other restrictions. The process governing the transfers for machineguns and short barreled rifles is extremely cumbersome and is generally accompanied by a series of long waits as various tax stamps are approved, mailed, and transfers and background checks are performed and approved. Such a process discourages preventative gun maintenance and creates the risk that affected facilities will be stuck without sufficient operable, safe weapons while they wait. Consider the following hypothetical:

Pursuant to the proposed rule, facility A legally acquires four M4 style machineguns and assigns them in shifts to security personnel who have passed their NICS and FBI background checks. After a passage of time, it is found that one of the M4s is not functioning properly. It is not reliably ejecting spent cases and causes the gun to jam. A visual inspection reveals a worn extractor in the bolt assembly. The parts needed for the repair are readily available, and the repair itself only takes minutes, but it requires the disassembly of the gun and test firing after the extractor is fitted. Gun ranges typically do not allow users to disassemble and work on guns on the premises, and the nuclear facility itself is no place for gunsmithing and test firing. Plus, the repair, while simple, should be done by a competent gun smith considering the importance of the firearm's function and the dangers of a botched repair.

Under the proposed rule, the facility's only recourse is a full scale transfer of the machinegun (the same process as if they were selling it off permanently). A long process which could take months to complete from the initial transfer, having the gun repaired, and then having it transferred back. Instead, the rule should be changed to allow covered firearms to be taken from the premises by authorized security personnel to a gunsmith for minor repairs and maintenance (things like broken and worn springs on machineguns are very common). This extension should be conditioned by requiring detailed records of such trips to be kept, and that the gunsmith utilized be the holder of a Federal Firearms License Type 1. This license ensures that the gunsmith himself has been subject to background checking and that he is legally able to perform gunsmithing services on machineguns. Further, the facility's security person should remain present while the repair services are rendered, such that the firearm never leaves his legal possession.

This change is important in that it will allow relevant facilities to keep their weapons in good repair, and discourage them from stockpiling unneeded weapons out of the fear that they will be underarmed if one ever needs repaired. Importantly, the conditions listed in the previous paragraph should be sufficient to satisfy the ATF based on their opinion letter regarding transfers regarding moving the covered firearms to and from the facility, though another supplemental opinion letter should be sought to confirm this.

PUBLIC SUBMISSION

As of: April 18, 2011
Received: April 17, 2011
Status: Pending_Post
Tracking No. 80c2e769
Comments Due: May 04, 2011
Submission Type: Web

Docket: NRC-2011-0018

Enhanced Weapons, Firearms Background Checks, and Security Event Notifications

Comment On: NRC-2011-0018-0001

Enhanced Weapons, Firearms Background Checks, and Security Event Notifications

Document: NRC-2011-0018-DRAFT-0014

Comment on FR Doc # 2011-01766

Submitter Information

Name: Ryan Spahr

Address:

225 E North St.

Apt. 502

Indianapolis, IN, 46204

General Comment

Please see attachment for comment to rule.

Attachments

NRC-2011-0018-DRAFT-0014.1: Comment on FR Doc # 2011-01766

Rulemaking Comments

From: Gallagher, Carol
Sent: Monday, April 18, 2011 9:50 AM
To: Rulemaking Comments
Subject: Comment on Proposed Rule - Enhanced Weapons, Firearms Background Checks & Security Event Notifications
Attachments: NRC-2011-0018-DRAFT-0014.pdf

Van,

Attached for docketing is a comment from Ryan Spahr on the above noted proposed rule (3150-AI49; 76 FR 6200) that I received via the regulations.gov website on 4/17/11.

Thanks,
Carol

April 18, 2011

Comment Submission No. 3
(ML11110A001)

3

Secretary
U.S. Nuclear Regulatory Commission,
Attn: Rulemakings and Adjudications Staff
Washington, DC 20555-0001

DOCKETED
USNRC

April 19, 2011 (9:05 am)

OFFICE OF SECRETARY
RULEMAKINGS AND
ADJUDICATIONS STAFF

Comments of:

Craig Renitsky **(Comment-Response Document Abbreviation: CR)**
275 S. Bryn Mawr Ave. Apt. E-22
Bryn Mawr, PA 19010
CRenitsky@Law.Villanova.edu

**Re: Enhanced Weapons, Firearms Background Checks, and Security Event Notifications,
Docket ID NRC-2011-0018**

Dear Secretary of the U.S. Nuclear Regulatory Commission,

I. Introduction and Background

1. The Nuclear Regulatory Commission (NRC or Commission) has requested comment on the proposed regulations that would implement the NRC's authority under the new section 161A of the Atomic Energy Act of 1954 (AEA). I am pleased to submit these comments in response to this request and appreciate the Commission's effort to allow all interested parties voice their opinion on proposed regulations. Subsequently, I appreciate the time that the Commission will take in reviewing each submission. I submit these comments on my own behalf with an interest in energy and water development and not as an agent of any institution.

2. Evidenced by the NRC's previous request for comment in October of 2006 regarding its authority under section 161A of the AEA, I believe that the Commission is properly weighing all interests in dealing with the important and complicated risks of nuclear energy. The Commission must maintain a delicate yet proper balance of interests when implementing any rules regarding the security procedures of NRC licensees and certificate holders. It is my belief that, first and foremost, safety must be properly maintained when dealing with the protection of nuclear materials. This required safety I believe extends from the security personnel who employ covered weapons as part of their protective practice to the facilities of the NRC licensees and certificate holders and the general public at large. Enough flexibility must be given to security personnel and inventory agents to allow them to adequately perform their duties while keeping the facilities and the surrounding communities as safe as possible.

1

3. Economics must also be accounted for because there is not an endless supply of funding available to the NRC. The cost of fingerprint background checks and weapons inventorying is quite prohibitive. With the current level of funding expected to remain relatively constant, weekly performance of these practices is not economically feasible. Finally, any proposed rule requires clarity. I believe that all facilities personnel need to understand exactly what is required of them and what is forbidden to enable the NRC to create the most efficient and effective balance of these mentioned interests. The NRC has taken significant steps towards attaining the most desirable balance possible by its proposed solutions to various issues. As this comment details, however, I believe that there are some areas to which the proposal could use alteration. I use these self-created “balancing factors” as a main point of reference throughout the remainder of this comment.

4. The following paragraphs are in response to the issues raised and the solutions proposed in 76 Federal Register 6200 (February 3, 2011). The topic headings are presented here as they are presented in the register notice. Every reference to the “register notice” in the following paragraphs refers to the notice on February 3, 2011. I give reasons for why I support many of the proposal’s intentions and offer support for how I believe some measures can be improved. As a general starting position I believe that the Commission should be commended for taking into consideration the comments received from the October, 2006 request. This proposal significantly improves upon the prior in both safety and efficiency. I also offer these comments to the NRC, however, with the hope that the areas of concern that I have detailed will be taken into account and handled appropriately.

II. Differences Between the Firearms Guidelines and the October 2006 Proposed Rule

Issue #5

2 5. I strongly support the proposal in Section 5 of the Firearms Guidelines to require periodic firearms background checks after the initial firearms background check. The October, 2006 proposed rule indicating that no further or recurring firearms background checks would be required after the initial background check did not adequately take into account the safety of the licensee facilities and the surrounding communities. The risk was great that one “false positive” report would have allowed an unqualified licensee employee full access to covered weapons and never have to submit to another background check. Furthermore, although inconsistent with the Firearms Guidelines, a three year periodicity is appropriate for recurring firearms background checks for security personnel whose official duties require access to covered weapons. It is also appropriate to allow each licensee or certificate holder to perform these checks more frequently than every three years at their discretion.

April 18, 2011

6. Conducting firearms background checks every five years leaves too great a risk of security personnel slipping through the cracks of the system. Not only would this interval give personnel too great of an advantage to prepare for and possibly manipulate background checks, it would also raise administrative costs. Requiring a three year periodicity for recurring checks and allowing a licensee to conduct them more frequently at their discretion will greatly enhance the security at each facility. It would instantly become markedly more difficult for nonqualified security personnel to be granted access to covered weapons. If an error did occur it would be handled within three years or less, depending on the facilities' preferences.

3 7. Additionally, the marginal benefit for an employee who knows that she will not "satisfactorily pass" a firearms background check to attempt to gain access to covered weapons, or to continue with access granted through a false positive, decrease significantly. Requiring only an initial check with no recurring checks, or requiring one every five years as required by the Firearms Guidelines, may provide some incentive to attempt to gain access or continue with falsely granted access to covered weapons. A required check every three years however, with any number of random checks in between that time, would nearly eradicate that incentive.

4 8. Furthermore, criminal history checks are currently required every three years to grant access and personal security clearance. Syncing the firearms background checks with the criminal checks would significantly decrease administrative costs and labor time. Enabling each licensee and certificate holder to submit one set of fingerprints for each employee with weapons access for both firearms background checks and criminal history records would decrease the amount of time that security personnel would be away from their official duties. This would then have the advantage of allowing other licensee employees to not have their official duties interrupted for extended periods of time. For example, one or more employees must perform a supervisory position, one must dictate when each security employee will be fingerprinted, someone must actually perform the fingerprinting, and the fingerprints must be delivered to the FBI. If the time spent performing each of these functions can be decreased by syncing the two mentioned fingerprint requirements, then it is in the best interest of the NRC and each individual licensee or certificate holder to do it.

5 9. Additionally, the register notice does not clearly state whether security personnel would continue to be granted access while the results of their background checks are pending. It is clear that new applicants must have firearms background checks completed for all security personnel before they are granted access to covered weapons. Procedures are also clear regarding those who receive a response of "delayed" or "denied." In the interest of clarity, however, it would be helpful to note the restrictions, if any, placed on individuals awaiting their results. Facility efficiency and safety, more than any due process related concerns, would likely be the greatest disadvantage to restricting access during the period of waiting. If restrictions during this period were to be considered it would be best to alternate the security personnel of

various sectors of each facility to ensure that operations continued to run efficiently and with the least amount of interruption. Therefore, a three year periodicity is appropriate for recurring firearms background checks with the ability of the licensee to perform them more frequently at their discretion. It would also be appropriate, however, for the Commission to state any restrictions to access during the period where background check results are pending.

6 10. I would also like to note that requiring firearms background checks for all employees at Commission-designated facilities with access to covered weapons will likely result in a significant increase in applications for enhanced weapons authority. Requiring background checks only for access to enhanced weapons was a deterrent to applying for such weapons. Removing this deterrent by requiring the background checks regardless of the weapons' classification should therefore lead to an increase in applications. Additionally, with the expected increase in enhanced weapons, the amount of time spent inventorying these weapons can also be expected to increase in unison.

Issue #8

11. The requirement under Section 6 of the Firearms Guidelines for merely annual checks on accountability and inventory of enhanced weapons did not go far enough. I support the Commission's proposal for licensees and certificate holders to conduct two types of inventories but I do not agree with the periodicity set out by the NRC for the more stringent of the two inventories.

7 12. In direct response to *Question D* in the register notice, semi-annual accountability inventories are not an appropriate periodicity for inventories that would physically verify the serial number of each enhanced weapon possessed by a licensee or certificate holder. The Rules already require a monthly inventory to verify the number of enhanced weapons present at each licensed facility. Therefore, the resources and manpower to conduct more intensive serial number inventories are in place twelve times per year making it unacceptable to perform this task only twice annually. There are obvious drawbacks economically to conducting a serial number inventory each month, and effectively doing away with the "piece-count" inventory, and that is why a periodicity of every three months would be the ideal balance for serial count inventories of enhanced weapons.

13. As the Commission stated in the register notice it takes approximately two days from two individuals to conduct a serial number inventory, as opposed to one day for the piece-count inventory. Therefore, by adding two more serial number inventories per year, and thus eliminating the need for two scheduled piece-count inventories per year, each facility would only be losing two additional days per year. I realize that this is four times more than is required by the Firearms Guidelines but the NRC and subsequently each licensed facility must ensure that

stolen or lost weapons do not create an unacceptable security risk to the facility itself, local law enforcement, and the surrounding community. Two days of two individuals' manpower is a relatively small price to pay to verify the serial number of all enhanced weapons present at the licensee facility and increase the level of safety and security dramatically for those who may be affected by a lost or stolen weapon. As I mentioned in paragraph 10, however, with a likely increase in enhanced weapons applications, inventorying time may increase more than initially expected.

III. *Changes to Safeguard Event Notifications*

8 14. The requirements for reporting and recording security events should be consolidated into a single section of part 73 similar to Section 73.71 "**Reporting and recording of safeguards events.**" In Section 73.71 there are italicized headings, for example "*(a) 15-minute notifications—facilities*" that easily break up the different topics within the section. Section 73.71 expectedly covers the entirety of reporting and recording of safeguards events. These same italicized headings should be used within the consolidated single section of part 73 as follows: Section 73.71 "**Reporting and Recording Security Events: (a) Telephonic Communications, (b) Written Follow-up Reports, and (c) Safeguards Events Log.**"

15. The NRC's concerns about clarity if security event reporting and recording requirements continue to be located in separate portions of part 73 are well-founded. The entirety of each topic named in the corresponding topic heading in Section 73 is fully covered within that same section. This gives readers reason to believe that every option for reporting and recording security events will be covered under one consolidated section and not located in a series of three adjacent sections. Furthermore, having all three requirements for reporting and recording consolidated under one section would make the regulations easier to use. If it is clearer to the facilities what they must do in any given situation, then it follows that the regulations would be easier to implement. Reporters would thus be less likely to commit errors, overlook a regulation, or spend needless time searching for a regulation or requirement that is expected to be covered within a single section. Therefore, due to clarity and efficiency concerns, all requirements for reporting and recording security events should be consolidated into a single section of part 73.

IV. *Concluding Remarks*

16. Once again I would like to thank the Nuclear Regulatory Commission for the opportunity to comment on this rule proposal and for the efforts to properly deal with the complex issues that arise when dealing with nuclear energy. Many of the elements of the new rule proposal provide the framework for vastly safer and more efficient NRC licensees and certificate holders. I generally support the regulations that the NRC has proposed, but as I have

April 18, 2011

detailed above I do have concerns with certain areas. I would also like to thank the NRC for the time spent reviewing this comment. Please do not hesitate to contact me if any questions should arise.

Sincerely,

Craig Renitsky

Rulemaking Comments

From: Craig J. Renitsky [CRenitsky@law.villanova.edu]
Sent: Monday, April 18, 2011 4:07 PM
To: Rulemaking Comments
Subject: NRC-2011-0018
Attachments: NRC Comment to NRC.docx

Thank you for the time you spend reviewing my comment.

Craig Renitsky
CRenitsky@Law.Villanova.edu



NUCLEAR FUEL SERVICES, INC.
a subsidiary of The Babcock & Wilcox Company

■ 1205 banner hill road ■ erwin, tn 37650 ■ phone 423.743.9141
■ www.nuclearfuelservices.com

4

PR 73
(76FR06200)

Comment Submission No. 4
(ML11130A041)

Certified Mail
Return Receipt Required

DOCKETED
USNRC

24G-11-0009
GOV-01-55-10
ACF-11-0155

May 9, 2011 (2:45 pm)

OFFICE OF SECRETARY
RULEMAKINGS AND
ADJUDICATIONS STAFF

May 4, 2011

Secretary
U.S. Nuclear Regulatory Commission
Attn: Rulemakings and Adjudications Staff
Washington, DC 20555-0001

Reference: (1) Docket ID. NRC-2011-0018 **(Comment-Response Document Abbreviation: NFS)**

Subject: **Response to NRC Request for Comments Regarding 10 CFR Part 73
Enhanced Weapons, Firearms Background Checks, and Security Event
Notifications; Proposed Rule (U)**

Dear Sir:

Nuclear Fuel Services, Inc. (NFS) is providing the attached comments for your consideration to 10 CFR Part 73 Enhanced Weapons, Firearms Background Checks, and Security Event Notifications; Proposed Rule (Reference 1).

Should you have questions concerning this submittal, please contact Mr. Kris Weir, Security Section Manager, at (423) 743-1704. Please reference our unique document identification number, 24G-11-0009, regarding communications on this matter.

Sincerely,
Nuclear Fuel Services, Inc.

Mark Elliott/mpe

Mark Elliott
Quality, Safety and Safeguards Director

Attachment

Industry Comments – Enhanced Weapons Proposed Rulemaking

24G-11-0009
GOV-01-55-10

EW Document/Section/ Page Reference	Comment	Suggested Wording/Revision
<div data-bbox="37 480 153 611">1</div> Federal Register Vol. 76, No. 23, Part II, Section III.B.5, page 6204.	<p>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.</p> <p>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.</p> <p>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.</p>	

Industry Comments – Enhanced Weapons Proposed Rulemaking

24G-11-0009

GOV-01-55-10

EW Document/Section/ Page Reference	Comment	Suggested Wording/Revision
<div>2</div> <div>Federal Register Vol. 76, No. 23, Part II, Section III.I. page 6209.</div>	<p>In response to the NRC's question on the appropriate frequency for conducting firearms background checks, this licensee believes that it is appropriate to require a 5-year periodicity for recurring firearms background checks.</p> <p>By following the alternative approach outlined in this section and requiring firearms background checks at least once every five years, and letting licensees and certificate holders choose how they will coordinate and/or control these checks, each individual licensee can determine the most advantageous method and periodicity.</p> <p>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.</p>	
<div>3</div> <div>Federal Register Vol. 76, No. 23, Part II, Section III.I. page 6209.</div>	<p>This licensee believes that annual accountability inventories are an appropriate periodicity for inventories that physically verify the serial number of each enhanced weapon possessed by a licensee or certificate holder.</p>	

Industry Comments – Enhanced Weapons Proposed Rulemaking

24G-11-0009
GOV-01-55-10

EW Document/Section/ Page Reference	Comment	Suggested Wording/Revision
4 Federal Register Vol. 76, No. 23, Part II, Section III.I. page 6209.	The licensee believes that consolidating security event notification regulations into a single section would promote clarity and ease of use for these regulations.	
5 Federal Register Vol. 76, No. 23, Part 73, Section 73.18.(m).(6). page 6235.	<p>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.</p> <p>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.</p>	"(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."

Industry Comments – Enhanced Weapons Proposed Rulemaking

24G-11-0009

GOV-01-55-10

EW Document/Section/ Page Reference	Comment	Suggested Wording/Revision
Federal Register Vol. 76, No. 23, Part 73, Section 73.18.(o).(3).(vi). page 6235.	<p>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.</p> <p>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 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.</p>	"(vi) The time interval from the previous monthly inventory shall not exceed 30 +3 days."

6

Industry Comments – Enhanced Weapons Proposed Rulemaking

24G-11-0009

GOV-01-55-10

EW Document/Section/ Page Reference	Comment	Suggested Wording/Revision
Federal Register Vol. 76, No. 23, Part 73, Section 73.18.(o).(4).(iii). Page 6235.	<p>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.</p> <p>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 monthly inventory would continue to limit the maximum interval between semi-annual inventories, which appears to be the intent behind this paragraph of the regulation.</p>	"(iii) The time interval from the previous semi-annual inventory shall not exceed 180 +7 days."

7

Industry Comments – Enhanced Weapons Proposed Rulemaking

24G-11-0009
GOV-01-55-10

EW Document/Section/ Page Reference	Comment	Suggested Wording/Revision
Federal Register Vol. 76, No. 23, Part 73, Section 73.19.(b).(9). Page 6237.	<p>The language of this paragraph requires "Security personnel who have completed a satisfactory firearms background check, but who have had a break in service with the licensee, certificate holder, or their security contractor of greater than one week subsequent to their most recent firearms background check ... are required to complete a new satisfactory firearms background check."</p> <p>What is the definition of a "break in service"? This clearly applies to a termination of employment, but what about a leave of absence, active service with the Reserves or National Guard, etc.?</p>	

8

Industry Comments – Enhanced Weapons Proposed Rulemaking

24G-11-0009
GOV-01-55-10

EW Document/Section/ Page Reference	Comment	Suggested Wording/Revision
<p>Federal Register Vol. 76, No. 23, Part 73, Section 73.19.(f).(1), (2), and (3). Page 6238.</p>	<p>The language of these paragraphs require that, “(1) Licensees and certificate holders shall also complete firearms background checks at least once every three calendar years to continue the security personnel’s access to covered weapons. (2) Licensees and certificate holders may conduct these periodic firearms background checks at an interval of less than once every three calendar years, at their discretion. (3) (i) Licensees and certificate holders must submit the information specified in paragraph (f) of this section within three calendar years of the individual’s most recent satisfactory firearms background check.”</p> <p>As discussed in other comments, by following the alternative approach outlined by the NRC in the Federal Register (Vol. 76, No. 23, Part II, Section III.I. page 6209) and requiring firearms background checks at least once every five years, and letting licensees and certificate holders choose how they will coordinate and/or control these checks, each individual licensee can determine the most advantageous method and periodicity.</p> <p>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.</p>	<p>“(1) Licensees and certificate holders shall also complete firearms background checks at least once every five calendar years to continue the security personnel’s access to covered weapons. (2) Licensees and certificate holders may conduct these periodic firearms background checks at an interval of less than once every five calendar years, at their discretion. (3) (i) Licensees and certificate holders must submit the information specified in paragraph (f) of this section within five calendar years of the individual’s most recent satisfactory firearms background check.”</p>

Industry Comments – Enhanced Weapons Proposed Rulemaking

**24G-11-0009
GOV-01-55-10**

EW Document/Section/ Page Reference	Comment	Suggested Wording/Revision
<div data-bbox="35 422 102 485" style="border: 1px solid red; padding: 2px; display: inline-block;">10</div> <p>Federal Register Vol. 76, No. 23, Part 73, Section 73.71.(g).(1).(iii). Page 6241.</p>	<p>The language of this paragraph requires that notification to local law enforcement officials of lost or stolen enhanced weapons must be made by telephone. "These notifications must be made by telephone to the appropriate local law enforcement officials."</p> <p>The requirement that these 48-hour notifications must be made by telephone appears to be overly restrictive and rules out an in-person meeting with these officials to conduct the notification.</p>	
<div data-bbox="35 863 102 926" style="border: 1px solid red; padding: 2px; display: inline-block;">11</div> <p>Federal Register Vol. 76, No. 23, Appendix G to Part 73, Section I.(h).(1) and (2). Page 6244.</p>	<p>This paragraph requires the licensees to report cyber security events to "any systems, networks, or equipment that falls within the scope of §73.54 of this part"; however, only licensees currently licensed to operate a nuclear power plant under part 50 of this chapter are subject to §73.54.</p> <p>This paragraph should be revised to exclude this reporting requirement for licensees not subject to §73.54.</p>	<p>"(h) <i>Cyber security events</i>. Licensees subject to §73.54 shall report the following:"</p>
<div data-bbox="35 1133 102 1196" style="border: 1px solid red; padding: 2px; display: inline-block;">12</div> <p>Federal Register Vol. 76, No. 23, Appendix G to Part 73, Section II.(c).(1) and (2). Page 6244.</p>	<p>This paragraph requires the licensees to report suspicious cyber security events to any "systems, networks, or equipment that falls within the scope of §73.54 of this part"; however, only licensees currently licensed to operate a nuclear power plant under part 50 of this chapter are subject to §73.54.</p> <p>This paragraph should be revised to exclude this reporting requirement for licensees not subject to §73.54.</p>	<p>"(c) <i>Suspicious cyber security events</i>. Licensees subject to §73.54 shall report the following:"</p>

Industry Comments – Enhanced Weapons Proposed Rulemaking

24G-11-0009
GOV-01-55-10

EW Document/Section/ Page Reference	Comment	Suggested Wording/Revision
<div data-bbox="27 485 100 546" style="border: 1px solid red; padding: 2px; display: inline-block;">13</div> <p>Federal Register Vol. 76, No. 23, Appendix G to Part 73, Section IV.(b).(1). Page 6245.</p>	<p>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."</p> <p>Blank cartridges used during force-on-force security exercises should be specifically excluded from this reporting requirement. 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.</p>	<p>"(1) A discovery that ammunition, with the exception of blank cartridges used for security force training, that is authorized by the licensee's security plan has been lost or uncontrolled inside a PA, VA, MAA, or CAA."</p>
<div data-bbox="27 1020 100 1082" style="border: 1px solid red; padding: 2px; display: inline-block;">14</div> <p>Federal Register Vol. 76, No. 23, Appendix G to Part 73, Section IV.(c). Page 6245.</p>	<p>This paragraph requires the licensees to report in the Safeguards Event Log "A discovery that a loss of control over, or protection of, classified material containing National Security Information or Restricted Data has occurred, provided –</p> <ul style="list-style-type: none"> (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." <p>This appears to be overly restrictive, and does not appear to fit with the one, four and eight hour reporting criteria of sections I, II, and III of Appendix G to Part 73. Instead, it makes more sense to require reporting in the Safeguards Event Log when either or both of conditions (1) and (2) are not met, and to not require reporting when conditions (1) and (2) are met.</p>	<p>"(c) <i>Loss of control or protection of classified information.</i> 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 –</p> <ul style="list-style-type: none"> (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."

Industry Comments – Enhanced Weapons Proposed Rulemaking

24G-11-0009
GOV-01-55-10

EW Document/Section/ Page Reference	Comment	Suggested Wording/Revision
<div data-bbox="21 550 96 612" data-label="Text">15</div> <p>Federal Register Vol. 76, No. 23, Appendix G to Part 73, Section IV.(d). Page 6245.</p>	<p>This paragraph requires the licensees to report in the Safeguards Event Log "A discovery that a loss of control over, or protection of, classified material containing Safeguards Information has occurred, provided –</p> <ul style="list-style-type: none"> (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. (3) The material would not have allowed unauthorized or undetected access to facility or transport contingency response procedures or strategies." <p>This appears to be overly restrictive, and does not appear to fit with the one, four and eight hour reporting criteria of sections I, II, and III of Appendix G to Part 73. Instead, it makes more sense to require reporting in the Safeguards Event Log when the conditions of (1), (2), and (3) are not met, and to not require reporting when the conditions of (1), (2) and (3) are met.</p>	<p>"(c) <i>Loss of control or protection of Safeguards Information.</i> A discovery that a loss of control over, or protection of, classified material containing Safeguards Information has occurred, unless all of the following conditions are met –</p> <ul style="list-style-type: none"> (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. (3) The material would not have allowed unauthorized or undetected access to facility or transport contingency response procedures or strategies."

PR 73
(76FR06200)

DOCKETED
USNRC

5

May 9, 2011 (3:40 pm)

OFFICE OF SECRETARY
RULEMAKINGS AND
ADJUDICATIONS STAFF

Comment Submission No. 5
(ML11130A112)

PUBLIC SUBMISSION

As of: May 09, 2011 Received: May 06, 2011 Status: Pending_Post Tracking No. 80c414b7 Comments Due: August 02, 2011 Submission Type: Web

Docket: NRC-2011-0018

Enhanced Weapons, Firearms Background Checks, and Security Event Notifications

Comment On: NRC-2011-0018-0014

Enhanced Weapons, Firearms Background Checks, and Security Event Notifications

Document: NRC-2011-0018-DRAFT-0016

Comment on FR Doc # 2011-10163

Submitter Information

Name: Robert E. Andrews **(Comment-Response Document Abbreviation: RA)**

Address:

2265 Rayburn House Office Building
Washington, DC, 20515

Government Agency: United States House of Representatives

General Comment

Dear Ms. Bladey:

I write in strong support of Draft Rule, NRC-2011-0018, "Enhanced Weapons, Firearms Background Checks, and Security Event Notifications." Theft or sabotage of nuclear material is a serious threat, and all steps must be taken to ensure that this material is properly protected. By promulgating regulations that allow security guards at nuclear facilities to carry heavy weaponry, NRC can make our country safer.

At present, contract security personnel at NRC licensees are not permitted to carry the same weaponry as contract guards at similar DOE facilities throughout our government-owned nuclear complex. This lack of adequate weaponry represents a potential vulnerability to our homeland security. Although the potential consequence of a terrorist act varies by the type and quantity of nuclear material present, the recent accident at the Fukushima Daiichi site demonstrates the calamitous impact of malfunction, natural or deliberate, even with commercial nuclear operations. Ensuring that security personnel at all nuclear facilities have access to adequate weaponry is an important step in preventing a terrorist attack.

I also write to encourage further rulemaking on the use of deadly force by NRC licensees, especially at facilities where a weapons-grade quantities and types ("Category I") of Special Nuclear Material (SNM) is present. While DOE protective forces are authorized under the Atomic Energy Act of 1954, as amended, to use deadly force to protect Category I SNM, the authority of NRC licensee security forces to protect this nuclear material is ambiguous under current regulation. I support clarification within the federal code, with the NRC licensees being given the explicit authority to exercise deadly force to protect Category I SNM.

For further information, please contact Jonathan Golden (jonathan.golden@mail.house.gov) on my staff.

Sincerely,

Robert E. Andrews
Member of Congress

Template = SECY-067

DS 10

Attachments

NRC-2011-0018-DRAFT-0016.1: Comment on FR Doc # 2011-10163

ROBERT E. ANDREWS

FIRST DISTRICT, NEW JERSEY

COMMITTEES:

EDUCATION AND LABOR

CHAIRMAN, SUBCOMMITTEE ON
HEALTH, EMPLOYMENT, LABOR
AND PENSIONS (HELP)

MEMBER, SUBCOMMITTEE ON HIGHER EDUCATION
LIFELONG LEARNING AND COMPETITIVENESS

ARMED SERVICES

CHAIRMAN, PANEL ON DEFENSE ACQUISITION REFORM

MEMBER, SUBCOMMITTEE ON
STRATEGIC FORCES

MEMBER, SUBCOMMITTEE ON TERRORISM,
UNCONVENTIONAL THREATS AND CAPABILITIES

BUDGET COMMITTEE

Congress of the United States
House of Representatives
Washington, DC 20515-3001

May 5, 2011

PLEASE REPLY TO:

☒ 2265 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-6501

☐ 515 GROVE STREET
3RD FLOOR, SUITE 3C
HADDON HEIGHTS, NJ 08036
(856) 546-5100

☐ 63 NORTH BROAD STREET
WOODBURY, NJ 08096
(856) 546-5100

WEBSITE:

www.house.gov/andrews

Cindy Bladey

Chief, Rules, Announcements, and Directives Branch (RADB)

Division of Administrative Services, Offices of Administration

Mail Stop: TWB-05-B01M

U.S. Nuclear Regulatory Commission

Washington, DC 20555-0001

Dear Ms. Bladey:

1 I write in strong support of Draft Rule, NRC-2011-0018, "Enhanced Weapons, Firearms Background Checks, and Security Event Notifications." Theft or sabotage of nuclear material is a serious threat, and all steps must be taken to ensure that this material is properly protected. By promulgating regulations that allow security guards at nuclear facilities to carry heavy weaponry, NRC can make our country safer.

1 At present, contract security personnel at NRC licensees are not permitted to carry the same weaponry as contract guards at similar DOE facilities throughout our government-owned nuclear complex. This lack of adequate weaponry represents a potential vulnerability to our homeland security. Although the potential consequence of a terrorist act varies by the type and quantity of nuclear material present, the recent accident at the Fukushima Daiichi site demonstrates the calamitous impact of malfunction, natural or deliberate, even with commercial nuclear operations. Ensuring that security personnel at all nuclear facilities have access to adequate weaponry is an important step in preventing a terrorist attack.

2 I also write to encourage further rulemaking on the use of deadly force by NRC licensees, especially at facilities where a weapons-grade quantities and types ("Category I") of Special Nuclear Material (SNM) is present. While DOE protective forces are authorized under the Atomic Energy Act of 1954, as amended, to use deadly force to protect Category I SNM, the authority of NRC licensee security forces to protect this nuclear material is ambiguous under current regulation. I support clarification within the federal code, with the NRC licensees being given the explicit authority to exercise deadly force to protect Category I SNM.

For further information, please contact Jonathan Golden (jonathan.golden@mail.house.gov) on my staff

Sincerely,



Robert E. Andrews

Member of Congress

Rulemaking Comments

From: Gallagher, Carol
Sent: Monday, May 09, 2011 3:20 PM
To: Rulemaking Comments
Subject: Comment on Proposed Rule - Enhanced Weapons, Firearms Background Checks and Security Event Notifications
Attachments: NRC-2011-0018-DRAFT-0016.pdf

Van,

Attached for docketing is a comment from Robert Andrews on the above noted proposed rule (3150-AI49; 76 FR 6200) that I received via the regulations.gov website on 5/6/11.

Thanks,
Carol

PUBLIC SUBMISSION

As of: 7/29/11 12:14 PM
Tracking No. 80ec2dc5
Comments Due: August 02, 2011

Docket: [NRC-2011-0018](#)

Enhanced Weapons, Firearms Background Checks, and Security Event Notifications

Comment On: [NRC-2011-0018-0014](#)

Enhanced Weapons, Firearms Background Checks, and Security Event Notifications

Document: [NRC-2011-0018-0021](#)

2011/07/14-Comment (6) of Brian Yip on FR Doc # 2011-10163

Submitter Information

Name: Brian Yip (**Comment-Response Document Abbreviation: BY**)

General Comment

1

Several of the 1-hour reportable events in proposed 10 CFR Part 73 Appendix G make reference to an individual's malevolent intent (e.g., attempted introduction of contraband by a person with malevolent intent into a PA, VA, MAA, or CAA). A licensee's evaluation of malevolent intent should not be a factor in determining the reportability of an event. First, it is unlikely that a licensee would be able to make a determination as to an individual's intent within an hour of their attempt to introduce contraband. Additionally, just as the agency has stated that only the NRC, the intelligence community, and law enforcement can determine whether a threat is credible (76 FR 6208, February 3, 2011), the NRC should not rely upon licensees alone to determine whether an individual had malevolent intent. Within the NRC, the staff will generally not make a determination about an individual's willfulness without an determination by the Office of Investigations. It would be inconsistent with this position to provide licensees an opportunity to determine an individual's intent (willfulness), and impractical to provide that such a determination could be made within an hour.

2

Furthermore, because the event, if not malevolent, is only required to be logged if determined to be a decrease in security plan effectiveness (76 FR 6245), NRC would at most become aware of it through an annual review of the logs, if at all. Therefore, although willful attempted unauthorized introduction of contraband into a PA is now a federal crime, the reportability regulations place the agency's ability to investigate such potential crimes on whether licensees first determine the crime was committed, and report it. All attempts to introduce contraband should be reported to allow the agency to independently assess the threat, regardless of the licensee's determination of intent.



babcock & wilcox nuclear operations group

► p.o. box 785 ► lynchburg, va 24505-0785 usa ► phone 434.522.6000
► www.babcock.com

7

**Comment Submission No. 7
(ML11208B451)**

**PR 73
(76FR06200)**

July 25, 2011
11-057

Secretary
U.S. Nuclear Regulatory Commission
Attn: Rulemakings and Adjudications Staff
Washington, D.C. 20555-0001

DOCKETED
USNRC

July 26, 2011 (11:08 am)

OFFICE OF SECRETARY
RULEMAKINGS AND
ADJUDICATIONS STAFF

Reference: Docket 70-27 **(Comment-Response Document Abbreviation: CR)**

Subject: Response to NRC Request for Comments Regarding 10 CFR Part 73 Enhanced Weapons, Firearms Background Checks, and Security Event Notifications: Docket ID NRC-2011-0018

Dear Sir/Madam:

Babcock & Wilcox, Nuclear Operations Group is submitting the attached comments for your consideration to 10 CFR Part 73 Proposed Rule for Enhanced Weapons, Firearms Background Checks, and Security Event Notifications.

If there are any questions in this regard, please contact Jamie Grassano, NRC Security Compliance Manager, at (434) 522-5816.

Sincerely,

Barry Cole
Manager, Licensing & Safety Analysis

The below comments reference Federal Register / Vol. 76, No. 23 / Thursday, February 3, 2011 / Proposed Rules and are for proposed rule 10 CFR 73.18 Authorization for use of enhanced weapons and preemption of firearms.

(d) Application for stand-alone preemption authority

P. 6233 (3) (ii) "Alternatively, licensees and certificate holders shall indicate they have commenced firearms background checks for their security personnel whose official duties require access to covered weapons; and they shall subsequently supplement their application to indicate that a sufficient number of security personnel have completed satisfactory firearms background checks to meet the licensee's or certificate holder's security personnel minimum staffing and fatigue requirements, in accordance with 73.19."

- 1
- There is no reference to fatigue requirements in 73.19. Licensee suggests citing the referenced fatigue requirements from 73.19 in 73.18.

(f) Application for enhanced weapons authority additional information

P. 6233 (1) Licensees and certificate holders shall also submit to the NRC for prior review and written approval a new, or revised, physical security plan, security personnel training and qualification plan, safeguards contingency plan, and a weapons safety assessment incorporating the use of the specific enhanced weapons the licensee or certificate holder intends to use and a weapons safety assessment incorporating the use of the specific enhanced weapons the licensee or certificate holder intends to use."

- 2
- Licensee suggests submitting an addendum to the physical security plan and security personnel training and qualification plan instead of revising and submitting the entire plans during the application phase. If the licensee is approved for the enhanced weapons, then the submitted addendums would be attached to the plans. Licensee suggests not submitting the safeguards contingency plan if the addition of the enhanced weapon would not affect the content of the plan.

P. 6234 (2) (i) "For the physical security plan, identify the specific types or models, calibers, and numbers of enhanced weapons to be used;"

- 3
- Licensee suggests instead of using "numbers of enhanced weapons" to be used to "how many will normally be deployed." This would remain consistent with the wording in the Weapons Safety Assessment Volume 2 of 5 - Template under 2 -2: Desired Weapon.

- 4
- Would an enhanced weapon that has been modified to be used as a Multiple Integrated Laser Engagement System (MILES) still be considered and treated as an enhanced weapon? When modified, the MILES weapons support a blank fire only system not capable of nor easily returned to live fire.

P. 6234 (2) (iii) "For the safeguards contingency plan, address how these enhanced and any standard weapons will be employed by the licensee's or certificate holder's security personnel in meeting the NRC-required protective strategy, including tactical approaches and maneuvers;"

- 5
- The licensee suggests addressing how "the enhanced and any standard weapons will be employed by the licensee" in an addendum to be attached to the physical security plan upon approval of enhanced weapons and not require submission of the safeguards contingency plan if the addition of the enhanced weapon would not affect the content of the plan.

P. 6234 (D) In assessing potential safety impacts, licensees and certificate holders shall consider both accidental and deliberate discharges of these enhanced weapons.

Administrative Review
MW Sadson 7/22/11
Date

6

- Licensee suggests when assessing potential safety impacts, the licensee shall only consider accidental discharges of the 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 the assessment.

P. 6234 (3) "The licensee's or certificate holder's training and qualification plan for enhanced weapons must include information from applicable firearms standards developed by nationally-recognized firearms organizations or standard setting bodies or from standards developed by Federal agencies, such as the U.S. Department of Homeland Security's Federal Law Enforcement Training Center, the U.S. Department of Energy's National Training Center, and the U.S. Department of Defense."

7

- The licensee suggests adding standards developed by Local and State agencies as well as Department of Criminal Justice Services (DCJS) Training Academies to the list. Adding Local, State and DCJS agencies would provide licensees an opportunity to receive specialized/enhanced training from a number of qualified agencies.

(m) Transfer of enhanced weapons

P. 6235 (6) 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.

8

- Licensee suggests being able to secure enhanced weapons in same location(s) as covered weapons.

(o) Periodic inventories of enhanced weapons

P. 6235 (3) "Licensees and certificate holders possessing enhanced weapons under this section shall perform inventories of its enhanced weapons monthly" (vi) The time interval from the previous monthly inventory shall not exceed 30 ± 3 days.

9

- Licensee suggests requiring the inventory to be completed every 30 ± 7 days. The change from ± 3 to ± 7 provides consistency between the monthly inventory and semi-annual inventory.

P. 6236 (5) "Licensees and certificate holders shall conduct monthly and semi-annual inventories of enhanced weapons using a two-person team."

10

- The licensee suggests using one person who is enrolled in a behavioral observation program to conduct the inventories. The behavioral observation program would mitigate the manipulation of inventory results.

The below comments reference U.S. Army Corps of Engineers Protective Design Center Technical Report Draft, Rev. 2, October 2010 and are for Weapons Safety Assessment Volume 1 of 5 - Template Instructions

P.14 Enhanced and Specialized Training

The terminology currently states "training is normally (but not limited to) conducted by an outside agency approved and certified by the NRC or the U.S. department of Homeland Security."

11

WSA

- Licensee suggests using the same terminology from the 73.18 p. 6234 requirement that states "standards developed by nationally-recognized firearms organizations or standard setting bodies or from standards developed by Federal agencies, such as the U.S. Department of Homeland Security's Federal Law Enforcement Training Center, the U.S. Department of Energy's National Training

Center, and the U.S. Department of Defense." Licensee also suggests adding standards developed by Local, State and DCJS agencies as acceptable enhanced and specialized training. Adding Local, State and DCJS agencies would provide licensees an opportunity to receive specialized and enhanced training from a number of qualified agencies. In addition, a licensee's training personnel who receive and pass specialized instructor training (train the trainer) be qualified to conduct enhanced weapons training.

P. 24 1. Impact to Individuals - could be death (Tragic, consequence level 5)

12
WSA

- Licensee suggests revising the example for the administrative building and not including impact to individuals. When completing the input tables it is assumed all buildings are un-occupied and include people that would normally be in these buildings under the people line item.

The below comments reference U.S. Army Corps of Engineers Protective Design Center Technical Report Draft, Rev. 2, October 2010 and are for Weapons Safety Assessment Volume 2 of 5 - Template Instructions

P. 3 2-6: Initial Area Danger Ring

13
WSA

- Licensee suggests when creating the initial Area Danger Ring (ADR) instead of using the maximum range of ammunition licensees use the lethal distance of the bullet. The lethal distance of the bullet is based on the bullet's energy. To determine the bullet's lethal distance, the licensee records the bullet's velocity and then uses a ballistics program to determine the bullet's lethal range. Once a bullet has traveled a certain range the bullet loses energy and is considered non-lethal. A clear representation of the bullet's lethality would be provided by using the bullet's energy instead of the bullet's maximum range.

P. 11 Input Table 39. Key Facilities/Areas Inside the PA

14
WSA

- Need to add footnote 3 - "Assume all buildings are un-occupied and include people that would normally be in these buildings under the people line item" to the bottom of the table. This will provide consistency to input tables.

15
WSA

- On all input tables under "Likelihood of Strike" the pull down should allow the Licensee to select "Never" instead of "Rare" as an option. Licensees may have items considered to be at risk inside the ADR that are physically protected from possible strikes.

16
WSA

- On all input tables under "Consequence of Strike" the pull down should allow the Licensee to select "None" instead of "Insignificant" as an option. Licensee may have items considered to be at risk inside the ADR that are physically protected from consequence of strike.

17
WSA

- On all input tables under Risk Level "0" should be a factor when utilizing the above options. Currently the Licensee would be given a "1" for a "Rare" and "Insignificant" even though there was no likelihood or consequence of strike and thus elevating the overall risk factor unnecessarily.

The below comments reference U.S. Army Corps of Engineers Protective Design Center Technical Report Draft, Rev. 2, October 2010 and are for Weapons Safety Assessment Volume 3 of 5 - Template Instructions

Table 2-2.2 Suggested Weapon Hazard Ratings

- 18
WSA
- Licensee suggests categorizing select fire weapons with a Hazard Rating of 2 instead of a Hazard rating of 3. Select fire weapons are those that have the ability to select safe, semi-auto, or full auto/burst. Select fire weapons require the user to make a conscious decision and physically manipulate the weapon for the selected sustained rate of fire. Currently, the select fire weapons are categorized as full automatic machine guns.

2-12 Review Information

- 19
WSA
- When determining the hazard ratings licensee suggests combining the ratings for weapon type and ammo types to get a combined hazard rating. Currently, the weapon and ammo hazard rating carry the same weight as the categories in the input tables. If a licensee selects a weapon type listed in the machine gun category with a hazard rating of 3 and an ammo type with a hazard rating of 4 their total hazard rating score prior to completing the input tables is a 7. The licensee suggests combining the hazard ratings for the weapon type and ammo types to get one hazard rating score. In this case the combined hazard rating score would be a 4 and carry the same weight as the hazard ratings for the input tables.

The below comments reference Federal Register / Vol. 76, No. 23 / Thursday, February 3, 2011 /Proposed Rules and are for proposed rule 10 CFR 73.19 Firearms background checks for armed security personnel.

(b) General Requirements

P. 6237 (iii) Not permit any security personnel access to covered weapons, unless the individual has completed a satisfactory firearms background check per this section.

- 20
- Does "any security personnel" include security management, security staff members and members of the security organization who maintains the lock controls to the approved weapons storage area(s) who normally do not have access to covered weapons, but at times may have access to an armory or observe firearms training on the firing range?

P. 6237 (6) Within the 180-day transition period specified in paragraph (b)(4) of this section, affected licensees and certificate holders that currently possess enhanced weapons under the authority other than 42 U.S.C. 2201a must remove any security personnel who receive a "delayed" NICS response from duties requiring access to enhance weapons.

- 21
- Licensee suggests individuals who received a delayed response be allowed access to covered weapons while the individual obtains additional information to resolve the delayed response. The Federal Bureau of Investigation (FBI) has stated it will attempt to resolve a delayed response for 30 days and then it will be the sole responsibility of the individual to provide additional information. If the individual is not allowed access to covered weapons while collecting additional information, it will place a burden on the licensee and may unfairly punish the individual.

P. 6237 (9) Security personnel who have completed a satisfactory firearms background check, but who have had a break in service with the licensee, certificate holder, or their security contractor of greater than one week subsequent to their most recent firearms background check, or who have transferred from a different licensee or certificates holder are required to complete a new satisfactory firearms background check.

22

- Licensee suggests clearly defining "a break in service" as termination of employment. Licensee suggests individuals returning from medical leave of more than 120 days or military deployment (Reserves or National Guard) be allowed to have access to covered weapons and within 30 days upon returning complete a satisfactory firearms background check.

(f) Periodic firearms background checks.

P. 6238 (1) Licensees and certificate holders shall also complete a satisfactory firearms background check at least every three calendar years to continue the security personnel's access to covered weapons.

23

- Licensee suggests requiring satisfactory firearms background checks at least once every five calendar years. This would allow licensees that currently conduct DOE security clearance reinvestigations every five years to align firearms background checks with reinvestigations. Licensees not subject to the NRC's access authorization program background check requirements would remain in alignment with the DOE security clearance re-investigations.

(p) Appeals and resolution of erroneous system information.

P. 6239 (1) Individuals who require a firearms background check under this section and who receive a "denied" or a "delayed" NICS response may not be assigned duties requiring access to covered weapons...

24

- Licensee suggests individuals who received a delayed response be allowed access to covered weapons while the individual obtains additional information to resolve the delayed response. The Federal Bureau of Investigation (FBI) has stated it will attempt to resolve a delayed response for 30 days and then it will be the sole responsibility of the individual to provide additional information. If the individual is not allowed access to covered weapons while collecting additional information, it will place a burden on the licensee and may unfairly punish the individual.

The below comments reference Draft Regulatory Guide DG-5019, Revision 1 (From US NRC Office of Nuclear Regulatory Research dated January 2011) and are for proposed rule 10 CFR 73.71 Reporting and recording of safeguards events.

4 Hour Reportables

P. 32 DG-5019 2.5.2 The following are examples of events involving the notification or unanticipated response of local, State or Federal law enforcement agencies that do not involve the licensee's implementation of its contingency response plan or protective strategy:

- x. Licensees should notify the NRC of law enforcement personnel onsite to arrest a felon or fugitive from justice or to execute a search warrant.
- y. Licensees should notify the NRC of law enforcement personnel's pursuit of subjects into the facility's OCA.
- z. Licensees should notify the NRC of requests for law enforcement response to the facility because a crime may have been committed (e.g. assault and battery or discovery of controlled substances or unauthorized weapons).

25

(DG)

- The Licensee interprets the above wording that these examples are "optional" reportable events. The Licensee suggests these types of incidents not be reportable so long as the Licensee does not implement its contingency response plan or protective strategy.

P. 33 DG-5019 2.5.2 Examples of Reportable Events (gg) The tampering with, or the destruction of equipment that does not affect plant operations (e.g. water coolers, office equipment, maintenance tools).

- 26
(DG)
- Licensee suggests these types of incidents be handled by the in house HR Department. The Licensee considers the requirement to report these incidents an unnecessary burden with no value added for the Commission.

8 Hour Reportables

P. 35 DG-5019 2.6.2 Examples of Reportable Events (g) The tampering with, or the destruction of equipment that does not affect plant operations or security (e.g. water coolers, office equipment, maintenance tools).

- 27
(DG)
- With the exception of this example adding the word "security" this proposed example mirrors 2.5.2 (gg) for 4 hour reportable. Licensee suggests these types of incidents be handled in house. The Licensee considers the requirement to report these incidents an unnecessary burden with no value added for the Commission.

Loggable Events

P. 51 DG-5019 5.3 (k) The licensee discovers authorized ammunition has been lost or is uncontrolled within a PA, VA, MAA or CAA.

- 28
(DG)
- Licensee suggests if 10 or more rounds of authorized ammunition has been lost or is uncontrolled within a PA, VA, MAA or CAA should be a loggable event. There are circumstances when an officer may lose a round while running to a response call or during their physical performance qualification standard (PPQS) run.

P. 58 DG-5019 Definitions Discovery (time of) - the specific time at which the licensee or certificate holder determines that a verified degradation of a security safeguards measure, contingency situation, or reportable event exists.

- 29
(DG)
- Licensee suggests "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.

Below comments reference Federal Register / Vol. 76, No. 23 / Thursday, February 3, 2011 / Proposed Rules and are for proposed rule 10 CFR 73.71 Reporting and recording of safeguards events.

P. 6244 II. Events to Be Reported Within Four Hours, Eight Hours and 24 Hours of Discovery

- 30
- Licensee suggests consolidating events that are proposed to be reported within four hours and eight hours to within 24 hours. By consolidating the reporting requirement, the Licensee would maintain consistency regarding event reporting and mitigate event reporting violations.



HITACHI

**Comment Submission No. 8
(ML11213A210)**

GE Hitachi Nuclear Energy

Patricia L. Campbell
Vice President, Washington Regulatory Affairs

1299 Pennsylvania Avenue, NW
Ninth Floor
Washington, DC 20004
USA

T 202-637-4239
patriciaL.campbell@ge.com

MFN 11-197

10 CFR Part 73
DG-5019

July 29, 2011 **(Comment-Response Document Abbreviation: GE)**

Via E-Mail

Secretary
U.S. Nuclear Regulatory Commission
ATTN: Rulemakings and Adjudications Staff
And Rule, Announcements, and Directives Branch,
Division of Administrative Service, Office of Administration
Washington, DC 20555-0001

Subject: Proposed Rule, Enhanced Weapons, Firearms Background Checks, and Security Event Notifications (76 Fed. Reg. 6200, February 3, 2011, NRC-2011-0018, RIN 3150-AI49); Draft Regulatory Guide (76 Fed. Reg. 6085, February 3, 2011, NRC-2011-0014, RIN 3150-AI149)

The U.S. Nuclear Regulatory Commission (NRC) published for comment the subject proposed rule regarding enhanced weapons, firearms background checks, and security event notifications. GE Hitachi Nuclear Energy ("GEH") provides comments below on the proposed rule provisions related to security event notifications. In addition, comments below address related guidance in DG-5019.

NRC Propose Rule, "Enhanced Weapons, Firearms Background Checks, and Security Event Notifications," Docket NRC-2011-0018

General Comments

The NRC states that it is proposing clarifying changes to security event notification regulations "to improve regulatory clarity and licensee implementation of the requirements" (76 Fed. Reg. 6202). GEH supports this goal. However, the organization and wording of the proposed changes to 10 CFR 73.71 and Appendix G to 10 CFR Part 73 create a requirement which could result in unnecessary disclosure of classified information-related security events to individuals without a need-to-know and also appears to introduce inconsistencies with other existing regulations, in particular 10CFR95.57.

2

With respect to question “E” at 76 Fed. Reg. 6209 (“Should the requirements for reporting and recording security events be consolidated into a single section of part 73?”), GEH generally supports consolidation of reporting of safeguards events, i.e., events involving materials and information which are the subject of 10 CFR Part 73, into a single section of Part 73 since this could reduce redundant (and thus potentially confusing or conflicting) language. However, GEH does not support the inclusion of reporting and recording of classified information-related security events into Part 73 for the reason that such consolidation of reports and records is in conflict with the general need-to-know requirements for access to security-related, safeguards, and classified information. In addition, for any such consolidation that would include classified information event reporting, the NRC would need to address requirements regarding classified information reporting currently set forth in 10 CFR 95.57.

Specific Comments

3

(1) The preamble of the proposed Appendix G is a differently organized restatement of the requirements of a portion of the proposed 10 CFR 73.71. Since it is both incomplete and redundant, GEH supports its deletion.

4

(2) The word “contraband” as used in the proposed Appendix G, Section I, paragraphs (c) and (f), is not defined in either the existing or proposed Part 73 except in the context of language such as 10 CFR 73.55(1)(ii)(B): “Search vehicles and materials for contraband or other items which could be used to commit radiological sabotage....” Licensees may have chosen to define for their facilities a set of items locally deemed contraband to include items, such as cell phones and cameras, which are not the subject of the intent of the NRC use of the word “contraband.” The NRC explains that some items are considered contraband when they are located at a nuclear facility, but not when they are away from the facility (e.g., guns and ammunition) (76 Fed. Reg. 6215). GEH recommends that the NRC consider adding a clarifying definition of “contraband,” for which the existing and proposed notification requirements are intended, in 10 CFR 73.2 or 73.71. A definition in the “Glossary” and a useful clarification are included in the NRC’s Draft Regulatory Guide, DG-5019, “Reporting and Recording of Safeguards Events”, Revision 1:

Contraband—materials banned from a protected area, vital area, material access area, or controlled access area. Contraband consists of unauthorized firearms, explosives, and incendiary devices that can be used to commit acts of sabotage as specified under Section 236 of the *Atomic Energy Act of 1954*, as amended (AEA) (42 U.S.C. § 2284). Contraband may be carried or concealed on personnel or in packages, materials or vehicles. [See pg. 57.]

The NRC staff considers contraband to be unauthorized weapons, explosives, or incendiaries. Licensees and certificate holders may also identify “prohibited items” under their facility procedures. The staff considers contraband items and prohibited items as separate

categories. Licensees and certificate holders are not required under these regulations to report attempted or actual introduction events involving prohibited items. In addition, items that are possessed by authorized persons for authorized purposes inside of the facility should not be considered contraband. For example, weapons possessed by the facility's security personnel as part of their official duties, weapons possessed by sworn law enforcement personnel visiting the facility, squib valves used in certain types of reactors, or explosives intended for authorized and controlled demolition or construction activities at the facility should not be considered contraband. [See Pg. 17.]

- 5 (3) The proposed Appendix G, Section I, paragraph (j), *Loss or theft of classified information*, as worded, is inconsistent with a similar existing requirement in 10 CFR 95.57(a) and (b). In particular, the proposed Appendix G, I(j) text imposes a one-hour notification for **loss** of classified information on certain licensees whereas 10 CFR 95.57(b) requires that such an event of a **loss** of classified information only be recorded in a written log by the facility clearance holder, with a copy of the log provided to the NRC on a monthly basis. In addition, certain holders of facility security clearances may not necessarily be subject to the provisions of 10 CFR Part 73 cited in the proposed 10 CFR 73.71(c) and (d) and the preamble to the proposed Appendix G to Part 73.

In a public meeting held June 1, 2011, the NRC stated it did not intend that the proposed rule result in duplicative requirements and, if Part 95 applies, then reporting requirements of 10 CFR 73.71 are not applicable. However, it appears that the proposed rule imposes additional requirements. Section 73.1, "Purpose and Scope," provides that Part 73 requirements are in addition to other requirements and obligations, such as those in Part 95:

10 CFR 73.1(a)(4) Special nuclear material subject to this part may also be protected pursuant to security procedures prescribed by the Commission or another Government agency for the protection of classified materials. The provisions and requirements of this part are in addition to, and not in substitution for, any such security procedures. Compliance with the requirements of this part does not relieve any licensee from any requirement or obligation to protect special nuclear material pursuant to security procedures prescribed by the Commission or other Government agency for the protection of classified materials. [Emphasis added.]

If it is not the intent of the NRC to impose additional and more restrictive reporting requirements related to a loss of classified information, then the NRC should delete or reconsider certain language in the proposed rule. GEH recommends the following:

- requirements for notifications to the NRC of classified information security events be solely identified in 10CFR Part 95, as it is a more appropriate location for such requirements and such location improves regulatory clarity, and

- the proposed Appendix G, Section I, paragraph (j) not be included in the final Part 73 rule.

6

(4) Similarly, proposed 10 CFR 73.71(k) and proposed Appendix G, Section IV, paragraph (c), *Loss of control or protection of classified information*, as worded, are inconsistent with existing requirements in 10CFR95.57(b). Further, the requirement in the proposed 10CFR73.71(k) and the proposed Appendix G, IV(c) for recording in the licensee's safeguards event log and the resulting commingling of information related to Part 73 safeguards events and Part 95 classified information-related security events is inconsistent with the general requirement for need-to-know access to information regarding classified information security events. The proposed rule should not increase visibility to the NRC of classified information and is better controlled by existing Part 95 requirements. GEH recommends the following:

- requirements for recording of classified information security events be solely identified in 10CFR Part 95, as it is a more appropriate location for such requirements and such location improves regulatory clarity, and
- the proposed Appendix G, Section IV, paragraph (c), not be included in the final Part 73 rule.

7

(5) The purpose of the three (3) words "classified material containing" in the proposed Appendix G, Section IV, paragraph (d), *Loss of control or protection of Safeguards Information*, is unclear. GEH recommends that those three (3) words be deleted from the final paragraph (d).

GEH Comments re Draft Regulatory Guide, DG-5019, "Reporting and Recording of Safeguards Events", Revision 1, January 2011, NRC-2011-0014

General Comments

8

Sections of the proposed revision to the Regulatory Guide (RG) which quote requirements contained in 10 CFR Part 73 are generally redundant. The value of including the text of the regulations directly within the text of the guidance is not clear. As an alternative, the applicable regulations could be provided in an appendix to the RG.

Specific Comments

9

(1) Above, GEH provides several comments to the NRC regarding the changes to 10 CFR Part 73. These comments included the recommendation that reporting and recording of classified information-related security events not be commingled with the reporting and recording of safeguards events, which are security events related to the primary

requirements of 10 CFR Part 73, for the protection of nuclear facilities and materials. Consistent with this recommendation, GEH recommends that the final Revision 2 to RG 5.62, section 2.3.1 and section 2.4.1 (both of which simply quote portions of the proposed rule), not include their respective paragraph (j), *Loss or theft of classified information*. Similarly, the proposed paragraph 2.3.2.x should be deleted.

10 (2) In section 2.5.2 of DG-5019, Rev. 1, the proposed examples of events characterized as requiring notification to the NRC under 10 CFR 73.71(e) and paragraph II of Appendix G, include attempts to gather classified information in sub-paragraph d. GEH recommends that classified information-related security events be addressed within 10 CFR Part 95 and its associated guidance and not commingled with safeguards events reporting. GEH thus recommends deleting "classified information," from 2.5.2.d.

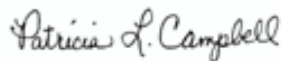
11 (3) In section 5.1 of DG-5019, Rev. 1, consistent with comments above, GEH recommends that the final Revision 2 of RG 5.62 in §5.1 not include sub-paragraph (c), *Loss of control or protection of classified information*.

12 (4) In section 5.1 of DG-5019, Rev. 1, GEH recommends the deletion of the three (3) words "classified information containing" in the proposed sub-paragraph (d), *Loss of control or protection of Safeguards Information*.

13 (5) In section 5.3 of DG-5019, Rev. 1, consistent with comments (1), (2), and (3) above, GEH recommends that the final Revision 2 of RG 5.62 in §5.3 not include sub-paragraph (t), "loss of control or protection over classified information...".

Please contact me if you have any questions regarding these comments.

Sincerely,



Patricia L. Campbell

CC: R. Beall (NRC)
P. Brochman (NRC)
L. Engle (GEH)

Rulemaking Comments**PR 73
(76FR06200)****Comment Submission No. 9
(ML11216A026)****9**

USNRC

From: Gray, Roberta J. [Roberta.Gray@ic.fbi.gov]
Sent: Tuesday, August 02, 2011 5:21 PM
To: Rulemaking Comments
Subject: Docket ID NRC-2011-0018
Attachments: FBI COMMENTS ON NRC NPRM 08022011.xlsx

August 3, 2011 (10:28 am)

OFFICE OF SECRETARY
RULEMAKINGS AND
ADJUDICATIONS STAFF

Please see attached Excel Spreadsheet for comments from the FBI's National Instant Criminal Background Check System (NICS) Section. Thank you.

Roberta J. Gray (Comment-Response Document Abbreviation: FBI)

*Management and Program Analyst**FBI National Instant Criminal Background Check System (NICS) Section**(304) 625-7394**roberta.gray@ic.fbi.gov*

Template = SECY-067

DS10

National Instant Criminal Background Check System (NICS) Section Comments on
Nuclear Regulatory Commission Notice of Proposed Rulemaking

DOCUMENT	PAGE / SLIDE	NUMBER/ FIGURE	PARA / BULLET	LINE	AS WRITTEN	COMMENT
FED REG 76 #23	6200	II	A.	last sentence	"Federal National Instant Background Check System (NICS)"	Should be "National Instant Criminal Background Check System (NICS)"
FED REG 76 #23	6202	III	A, third column	4th paragraph from bottom	"... Provisions in the NRC Form are appropriately consistent with the ATF form."	Should say "... Provisions in the NRC Form are appropriately consistent with the ATF Form 4473."
FED REG 76 #23	6203	B	third column	11 lines from bottom	Individuals who have been removed from duties requiring access to covered weapons and who subsequently complete a satisfactory firearms background check would be permitted to be returned to duties...	Should say "... requiring access to covered weapons and who successfully appeal would be permitted to be returned to duties."
FED REG 76 #23	6204	4	1st column Under "Solution"	6th line from bottom	incorrect "delayed" or "denied" NICS responses	Should be "extended delays and erroneous denials." Delays are not necessarily incorrect.
FED REG 76 #23	6204	4	2nd Column	9	incorrect "delayed" or "denied" NICS responses	Should be "extended delays and erroneous denials." Delays are not necessarily incorrect.
FED REG 76 #23	6204	4	Solution	10 lines from bottom	... individuals can apply to the FBI to check their status under the NICS databases.	Individuals should not apply to the VAF to check their status. Change to state " individuals can request the NICS Section to maintain specific information about them for use in subsequent background checks to determine their eligibility to receive firearms."
FED REG 76 #23	6205	third column	11	3rd and 5th lines from bottom	ATF FFL	Should be FFL (delete ATF)
FED REG 76 #23	6206	13	1st column	last line of paragraph	... Firearms background check, NICS check, NICS response, and Satisfactory firearms background check.	... Firearm background check, NICS check, NICS response, and Proceed firearm background check.
FED REG 76 #23	6209	I	A, B, C	All	Is it appropriate to require a 3 year ...?	We should make sure the re-checks are spaced out and do not come in one large quantity all at one time.
FED REG 76 #23	6209	I	A	C	If not 3 years or 5 years, what is an appropriate periodicity for recurring firearms background checks, keeping in mind that the Firearms Guidelines require no less than 5 years?	We recommend yearly recurrence; initiate the background checks in accordance with the employees' general security background checks, not via batchload, in order to spread the background checks out over time so they are not sent in a large quantity all at one time.

1
2
3
4
5
6
7
8
9
10

National Instant Criminal Background Check System (NICS) Section Comments on
Nuclear Regulatory Commission Notice of Proposed Rulemaking

DOCUMENT	PAGE / SLIDE	NUMBER/ FIGURE	PARA / BULLET	LINE	AS WRITTEN	COMMENT	
FED REG 76 #23	6220	3rd column	4th para	2nd line from bottom	... To conduct a firearms background check and would specify a retention period for this information.	Should state the retention period information, which is "On proceed transactions, all personally identifiable information is purged within 24 hours of notification to the licensee/certificate holder; the FFL number and state of residence are purged within 90 days from the creation date; and the NTN and creation date are retained indefinitely. On denied transfers, all information is retained for 110 years after the subject's date of birth or 110 years after the creation date of the transaction, whichever is sooner. For cancelled requests, all information is purged within 90 days from the creation date."	11
FED REG 76 #23	6221	E	3rd column, 1st paragraph	5th line from bottom of paragraph	Except for VAF records, the FBI purges the results of all NICS checks after 30 days...	Statement is incorrect; should state, "Except for VAF records, all personally identifying information is purged within 24 hours of notification to the licensee/certificate holder of an allowed transfer; the FFL number and state of residence are purged within 90 days from the creation date; and the NTN and creation date are retained indefinitely. On denied transfers, all information is retained for 110 years after the subject's date of birth or 110 years after the creation date of the transaction, whichever is sooner. For cancelled requests, all information is purged within 90 days from the creation date."	12
FED REG 76 #23	6237	§73.19	(6)	2nd line from bottom of para	...must remove any security personnel who receive a "delayed" NICS response from duties requiring access to enhanced weapons.	Should specify the time of the delay. Would they be removed if the check is immediately delayed, within three business days, or within 30 days? We would recommend three business days as that is what is applicable to Brady background checks.	13
FED REG 76 #23	6238	73.19 (g)	2nd column, g	Whole paragraph	Notification of removal	Question: If NRC finds a person has been removed from their job due to a disqualifying event, will you notify NICS in case they are in VAF or if we need to change a status?	14
FED REG 76 #23	6239	2nd Column	4 instances	4 instances	NICS Transaction Number is used 4 times in this column.	NICS Transaction Number is used 4 times in the whole document---all in this column. The acronym NTN is never established. It should be established and used.	15
FED REG 76 #23	6240	1st column	(9)	middle of paragraph	... Maintain information about himself or herself in a Voluntary Appeal File to be established by the FBI and checked ...	Should be "... Maintain information about himself or herself in a VAF established by the FBI and checked ..."	16
FED REG 76 #23	through out	throughout	throughout	throughout	"firearms background checks"	Change to "firearm background checks"	17
FED REG 76 #23	through out	throughout	throughout	throughout	"... NICS check response. ..."	Should say "... NICS response. ..."	18

PR 73
(76FR06200)

Comment Submission No. 10
(ML11216A027)

10

As of: August 03, 2011
Received: August 02, 2011
Status: Pending_Post
Tracking No. 80ed3fed
Comments Due: August 02, 2011
Submission Type: Web

PUBLIC SUBMISSION

Docket: NRC-2011-0018
Enhanced Weapons, Firearms Background Checks, and Security Event Notifications

DOCKETED
USNRC

Comment On: NRC-2011-0018-0014
Enhanced Weapons, Firearms Background Checks, and Security Event Notifications

August 3, 2011 (11:15 am)

Document: NRC-2011-0018-DRAFT-0021
Comment on FR Doc # 2011-10163

OFFICE OF SECRETARY
RULEMAKINGS AND
ADJUDICATIONS STAFF

Submitter Information

Name: S. Hardin (Comment-Response Document Abbreviation: SH1)
Address:
Box 1776
Mt Airy, MD,

General Comment

See attached file(s)

Attachments

Comments on Event Notifications, 8-2-11

Template = SECY-067

DS 10

Comments on Proposed Rule on Enhanced Weapons, Firearms Background Checks, and Security Event Notifications [NRC-2011-0018]

August 2, 2011

Overall, I support the proposed rule and associated regulatory and urge the NRC to issue a final rule and regulatory guidance in an expeditious manner.

Specific comments:

1. § 73.71(a)(3)(ii) – the use of a spoken authentication code to validate messages from facilities regarding imminent or actual hostile actions is operationally complex and burdensome. With the secure communications capabilities currently available to the NRC, the use of verbal authentication codes is antiquated and is a workaround. Ten years after 9/11, the NRC should be able to transition to a secure communications methodology providing built-in authentication and non-repudiation capabilities to validate such messages. Moreover, the NRC has not proposed authentication requirements for transportation imminent or actual hostile actions in the proposed § 73.71(b)(3), nor explained the basis for this disparate treatment. **Recommendation:** The NRC should remove the verbal authentication requirement for facility-based notifications to achieve consistency with transportation-based notifications; or the NRC should use a hardware-based solution that is effective, but transparent to the user, and thus reduces operational and regulatory burdens while achieving the important notification and communication purposes.
2. Appendix G, Paragraph II(a), “Suspicious events” – while I am supportive of a requirement for licensees to notify the NRC of suspicious events, the NRC has not articulated a rationale or basis for the proposed 4-hour timeliness requirement (either for internal NRC purposes or for purposes of forwarding this suspicious information to the law-enforcement or intelligence communities). **Recommendation:** Absent an articulated rationale or basis for the 4-hour timeliness, the NRC should require that suspicious events should be reported within 24 hours or the next business day. See also Comment 3, which may address the timeliness need.
3. § 73.71(j) – The notification process for reporting suspicious events does not include a requirement for licensees to notify their local FBI joint terrorism task force (JTTF). This direction has been contained in previous NRC and existing FBI guidance (See appendix to DG-5019 for relevant guidance documents). Additionally, the proposed rule does not require a licensee to establish a point of contact and notification protocol with their local JTTF. A requirement for licensees to notify their local JTTF of suspicious events (in accordance with FBI guidance) would appear to obviate the need for rapid notification to the NRC and would speed up the processing of the information by the intelligence and law-enforcement communities. Secondly, the need for NRC licensees to report suspicious events to their local JTTF is a reporting burden under the Paperwork Reduction Act and should be evaluated in a final rule. **Recommendation:** The final rule should be revised to require licensees to report suspicious activities to their local JTTF consistent with existing FBI direction. The NRC should consider whether reporting such events to the local FBI JTTF

obviates the need for an NRC reporting requirement, or just reduces the NRC's timeliness need to a next business day approach. The burden of such reports to the FBI should be addressed in the final rule as well.

Response to Specific Questions in Section III(l) of the FRN.

- 4 4. Questions A, B, and C – a five year reinvestigation periodicity for firearms background checks is most appropriate, given other licensee background check, fitness for duty, behavioral observation, and insider mitigation programs.
- 5 5. Question D – annual inventories for enhanced weapons are adequate given the close controls over such weapons at NRC-regulated facilities.
- 6 6. Questions E and F – the security event notifications should be consolidated from the separated § 73.71 and Appendix G into a series of three contiguous sections as suggested by the NRC under Question F.

S. Hardin
Mt. Airy, MD

Rulemaking Comments

From: Gallagher, Carol
Sent: Wednesday, August 03, 2011 11:04 AM
To: Rulemaking Comments
Subject: Comment letter on Enhanced Weapons, Firearms Background Checks, and Security Event Notifications
Attachments: NRC-2011-0018-DRAFT-0021.pdf

Van,

Attached for docketing is a comment letter from S. Hardin on the above noted proposed rule (76 FR 23515; 3150-AI49) that I received via the regulations.gov website on 8/2/11.

Thanks,
Carol



R. M. Krich
Vice President
Nuclear Licensing

DOCKETED
USNRC

August 5, 2011 (9:25 am)

OFFICE OF SECRETARY
RULEMAKINGS AND
ADJUDICATIONS STAFF

Tennessee Valley Authority
1101 Market Street, LP 3R
Chattanooga, Tennessee 37402-2801

August 2, 2011

(Comment-Response Document Abbreviation: TVA)

Secretary, U.S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001
ATTN: Rulemakings and Adjudications Staff

Subject: Enhanced Weapons, Firearms Background Checks, and Security Event Notifications (NRC-2011-0018)

Reference: Letter from David R. Kline (NEI) to Philip G. Brochman (NRC), Senior Program Manager, "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," dated August 2, 2011

The U.S. Nuclear Regulatory Commission (NRC) published proposed regulations that would implement the NRC's authority under the new section 161A of the Atomic Energy Act of 1954, as amended, and revise existing regulations governing security event notifications in the *Federal Register* on February 3, 2011 (76 FR 6200). In the *Federal Register* Notice, the NRC solicited comments on the proposed regulations. In a *Federal Register* Notice dated April 27, 2011 (76 FR 23515), the NRC extended the deadline for comments until August 2, 2011.

1

The Tennessee Valley Authority (TVA) has reviewed the proposed regulations and provides comments specific to TVA in the Enclosure. In addition, TVA endorses the Nuclear Energy Institute's comments provided in the referenced letter. If you have any questions regarding this letter, please contact Joe Shea at 423-751-6887.

Respectfully,

R. M. Krich

Enclosure: TVA Comments Regarding Enhanced Weapons, Firearms Background Checks, and Security Event Notifications (NRC-2011-0018)

TVA Comments Regarding Enhanced Weapons, Firearms Background Checks, and Security Event Notifications (NRC-2011-0018)

Document/Section/ Page Reference	Comment	Suggested Wording/Revision
<div data-bbox="54 728 132 819" style="border: 1px solid red; width: 37px; height: 55px; display: flex; align-items: center; justify-content: center; margin-bottom: 10px;">2</div> <p>76 FR 6200, "Nuclear Regulatory Commission, 10 CFR Part 73, [NRC-2011-0018], RIN: 3150-A149, Enhanced Weapons, Firearms Background Checks, and Security Event Notifications"</p> <p>§ 73.19 Firearms background checks for armed security personnel (e) Firearms background check submittals, and (f) Periodic firearms background checks. Ip. 6238</p>	<p>Tennessee Valley Authority (TVA) is a Federal agency established pursuant to the Tennessee Valley Authority Act of 1933, <i>as amended</i>, 16 U.S.C. §§ 831-831ee (2006 & Supp. III 2009), with the capacity to conduct firearms background checks without processing through the NRC as prescribed in the proposed rule. TVA Nuclear Security currently completes firearms background checks of all security personnel with access to covered weapons, which includes a check of the individual's fingerprints against the Federal Bureau of Investigation's (FBI's) fingerprint system and a check of the individual's identifying information against the FBI's National Instant Criminal Background Check System (NICS). Additionally, TVA currently processes criminal history checks in accordance with current regulatory requirements, specifically 10 CFR § 73.57 (b)(2)(iii), which states in-part; "Any licensee currently processing criminal history requests through the FBI pursuant to Executive Order 10450 need not also submit such requests to the NRC under this section; and" . . .</p> <p>Requiring TVA to process these checks through the NRC would not be of benefit to either agency, would be an unnecessary administrative and cost burden to all agencies involved.</p>	<p>Recommend adding a section to the subject rule and associated Regulatory Guidance document(s) with similar wording to that of 10 CFR § 73.57 (b)(2)(iii) that would recognize TVA's ability to continue processing firearms background checks without submitting such requests through the NRC under § 73.19.</p>

Enclosure

TVA Comments Regarding Enhanced Weapons, Firearms Background Checks, and Security Event Notifications (NRC-2011-0018)

3

Document/Section/ Page Reference	Comment	Suggested Wording/Revision
<p>76 FR 6200, "Nuclear Regulatory Commission, 10 CFR Part 73, [NRC-2011-0018], RIN: 3150-A149, Enhanced Weapons, Firearms Background Checks, and Security Event Notifications"</p> <p>§ 73.18 Authorization for use of enhanced weapons and preemption of firearms laws (d) <i>Application for stand-alone preemption authority</i>, (e) <i>Application for combined enhanced-weapons authority and preemption authority</i>, (f) <i>Application for enhanced-weapons authority additional information</i>, and (g) <i>Conditions of approval</i>. lpgs. 6233-6234</p>	<p>Tennessee Valley Authority (TVA) is a Federal agency with the capacity to obtain, possess, and implement the use of enhanced weapons under current Federal Laws and therefore should not be required to submit application to the NRC for stand-alone preemption authority and/or enhanced weapons authority as prescribed in the proposed rule.</p>	<p>Recommend adding a section to the subject rule and associated Regulatory Guidance document(s) that would recognize TVA's ability to obtain, possess, and implement the use of enhanced weapons without processing application through the NRC.</p>



Enclosure

Rulemaking Comments

From: Perdue, Barbara Ann [baperdue@tva.gov]
Sent: Thursday, August 04, 2011 6:21 PM
To: Rulemaking Comments
Cc: Perdue, Barbara Ann
Subject: Enhanced Weapons, Firearms Background Checks, and Security Event Notification (NRC-2011-0018)
Attachments: TVA_NRC_Enhanced Weapons, Firearms Background Checks, and Security Event Notifications_080211.pdf

Attached is TVA's comments.

Barbara A. Perdue

Senior Management Assistant to Rod Krich
Vice President, Nuclear Licensing
TVA Nuclear Power Group
1101 Market Street, LP 3R
Chattanooga, TN 37402-2801
423-751-4039  423-751-4904 

Industry Comments – Proposed Rulemaking on Enhanced Weapons and DG 5020

EW Document/Section/ Page Reference	Comment	Suggested Wording/Revision
	<p>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."</p> <p>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.</p>	
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.



NUCLEAR ENERGY INSTITUTE

David R. Kline
DIRECTOR, SECURITY
NUCLEAR GENERATION DIVISION

**DOCKETED
USNRC**

August 2, 2011 **(Comment-Response Document Abbreviation: NEI)**

August 15, 2011 (4:30 pm)

**OFFICE OF SECRETARY
RULEMAKINGS AND
ADJUDICATIONS STAFF**

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.

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.

3 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.

5 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

Mr. Philip G. Brochman

August 2, 2011

Page 4

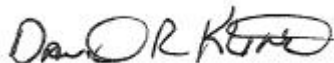
current 10 CFR Part 73 rule requirements. All issues required to be entered into the SEL are captured in the CAP; therefore, this requirement has become redundant and an administrative burden, which provides no real value.

6 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
<div data-bbox="44 451 121 521">1</div> <p data-bbox="132 354 365 383">General Comment</p>	<p data-bbox="583 354 1293 597">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.</p> <p data-bbox="583 638 1293 846">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.</p> <p data-bbox="583 886 1293 1268">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.</p>	<p data-bbox="1325 354 1373 383">N/A</p>
<div data-bbox="44 1312 121 1382">2</div> <p data-bbox="132 1304 365 1333">General Comment</p>	<p data-bbox="583 1304 1220 1377">Recommend incorporating rule language into the regulatory guide similar to DG 5019.</p>	

Industry Comments – Proposed Rulemaking on Enhanced Weapons and DG 5020

EW Document/Section/ Page Reference	Comment	Suggested Wording/Revision
3 Part 73.18, Section (m)(6)	<p>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.</p> <p>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.</p>	<p>"(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."</p>
4 Part 73.18 (o)(3)(vi)	<p>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.</p> <p>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</p>	<p>"(vi) The time interval from the previous monthly inventory shall not exceed 30 + 3 days."</p>

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)	<p>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.</p> <p>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.</p>	"(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.	
7 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.
8 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 requirement. 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) <i>Loss of control or protection of classified information.</i> 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.”
9 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
	<p>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."</p> <p>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.</p>	
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 – WITHHOLD FROM PUBLIC DISCLOSURE~~**Industry Comments – Proposed Rulemaking on Event Notifications and DG-5019**

Reference Page/Section	Comment	Suggested Wording/Revision
<div data-bbox="79 467 163 537">1</div> General Comment	<p>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.</p>	<p>Recommend issuing separate rulemaking for Reporting and Recording Safeguards Events and Enhanced Weapons.</p>
<div data-bbox="65 911 149 980">2</div> General Comment	<p>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</p>	<p>Recommend the requirement to notify NRC 15 minutes after the discovery of an imminent threat or hostile action be removed.</p>

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.	
3 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.
4 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
	<p>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.”</p> <p>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.</p>	<p>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.</p>
5 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
	<p>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.</p> <p>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:</p> <p>“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</p>	<p>proposed rule and DG 5019 that clarify “discovery”, which will improve the efficiency and effectiveness of event reporting and eliminate redundant requirements.</p>

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

Reference Page/Section	Comment	Suggested Wording/Revision
	<p>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.”</p> <p>Industry is willing to work with NRC to develop appropriate examples where investigation and evaluation is necessary.</p>	
General Comment	<p>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.</p> <p>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.</p>	Recommend providing an alternative approach for reporting criteria for cyber events.

6

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

Reference Page/Section	Comment	Suggested Wording/Revision
7 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.	
8 Appendix G, Section I <i>Events to be reported within one hour of discovery.</i> (d)(1), (f)(1), (f)(2), (h)(2), (k)(1), (k)(2) :	<p>1.) General comment on 10 CFR 73.71(c) for Facility Security Events to Be Reported within 1 Hour.</p> <p>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".</p> <p>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</p>	

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 .	
9 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.
10 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).
11 Part 73.71(a)(6)(b), p. 157	The wording provided in (1) and (3) is redundant.	Delete (1) and (3).
12 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.
16 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.
17 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
18	Part 73.71, Appendix G, I.(a)(5)	N/A	<i>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.</i>
19	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) <i>Cyber security events</i>	Delete Appendix G to Part 73, Section I (h)(2) <i>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</i> Add to App G, Paragraph III Events to be reported in 8 hours (f) <i>Cyber security events. (2) <u>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.</u></i>
20	Appendix G, Section I – Events to be reported in 1 hour (k)(1), (k)(2)	<i>Loss of Safeguards Information</i> should be an 8 hour report not a 1 hour report <u>IF</u> 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 or 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
<div>21</div> <p>Appendix G, Section III, Events to be reported in 8 hours</p>	<p>associated with the event.</p> <p>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”.</p>	<p>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</p> <p>(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.</p> <p>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.</p>
<div>22</div> <p>Appendix G, Paragraph II (c)(2)</p>	<p>Suggested change to reference additional applicable</p>	<p><i>Appendix G, Paragraph II (c)(2) An event</i></p>

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.	<i>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).</i>
23	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)".
24	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.
25	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.
26	Part 73.71, Appendix G, IV.(d)	This section refers to Safeguards Information as "classified" material.	Recommend replacing "classified" with "designated".
27	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	<i>73.71 (j) Notification process. (8) Licensees and certificate holders desiring to retract a previous security event report that has been determined to be <u>not reportable in accordance</u></i>

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.	<p><u>with 73.71(a) through (h) or</u> <i>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.</i></p> <p>73.71(m) (13)(i) <i>If the licensee or certificate holder subsequently retracts a telephonic notification made under this section as <u>not reportable in accordance with 73.71(a) through (h) or</u> 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.</i></p> <p><i>(ii) If the licensee or certificate holder subsequently retracts a telephonic notification made under this section <u>not reportable in accordance with 73.71(a) through (h) or</u> 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.</i></p>
28 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
29 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.	
30 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.
31 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.
32 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.
33 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
34	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."
35	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;")
36	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."
37	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."
38	Federal Register Vol 76, No. 23 (j) Pg. 6244	N/A	Paragraph (j): Restricted Data is not defined.
39	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.
40 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.
41 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."
42 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.
43	Federal Register Vol 76, No. 23 (IV) (a)(2)(c) Page 6245	N/A	Please define Restricted Data.
	DG-5019		
44	Section 2.1, p. 12	See suggested wording.	The first sentence of the third paragraph should be re-located to beginning of the section.
45	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.
46	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.
47	Section 2.1.2, j.	This example is redundant to examples a., d., e., and i.	Delete j.
48	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".
49	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”).
50	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.
51	Page 15, Section 2.2	See suggested wording.	The first sentence of the third paragraph should be re-located to beginning of the section.
52	Page 15, Section 2.2, Paragraph 4	<p>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.</p> <p>There is no definition for “imminent” in the text or in the glossary sufficient for licensees to make consistent decisions.</p>	Use the definition of “imminent” contained in NEI 03-12.
53	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.”
54	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.
55	Page 17, Section 2.3, 2 nd paragraph	Wording should be revised to clarify the need for deliberate and malevolent intent. This would rule out human error events such as mispositioning.	<p>Recommend rewording the paragraph as follows:</p> <p>Generally, these events relate to committed or attempted acts and credible threats involving theft</p>

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.
56 Page 17, Section 2.3, 4 th 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
57 Page 18, Section 2.3, 7 th 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

58	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.
59	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.
60	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.
61	Page 20, Section 2.3.2 (d)	This is redundant to 2.3.2,c and should be deleted	Delete.
62	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

63	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".
64	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).
65	Page 21, Section 2.3.2 (i)	This is redundant to (h).	Delete.
66	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.
67	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.
68	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

69	Page 21, Section 2.3.2 (l), (m), and (n)	These are redundant to (k) and should be eliminated.	Delete.
70	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...."
71	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.	<p>Suggest removing the phrase "or related to willful human error". and "reasonable mechanical failure".</p> <p>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."</p>
72	Page 22, Section 2.3.2 (r)(2)	N/A	Suggest removing the word "may" from this sentence.
73	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.
74	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.	
75	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.
76	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.
77	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.
78	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

		<p>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.</p> <p>The phrase "involving individuals" is also undefined and ambiguous.</p>	
79	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".
80	Page 23, Section 2.3.2 (u)	Same comment as above.	Same as above.
81	Page 23, Section 2.3.2 (aa),(bb)	<p>Duplicate events.</p> <p>Item (4) and (5) reference unsuccessful attacks, which are not a characteristic of (bb).</p>	<p>Recommend deleting (bb) and moving all text under (bb) to (aa).</p> <p>Recommend deleting (4) and (5) under (bb).</p>
82	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."
83	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.	
84	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).
85	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.
86	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."
87	Page 31, Section 2.5.2 (j)		Delete out of this section and include in section 2.5.2 for impacts to cyber.
88	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.	
89	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....."
90	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."
91	Page 31, Section 2.5.2 (p)	This statement is redundant and has been adequately covered throughout this section. Recommend it be deleted.
92	Page 31, Section 2.5.2 (q)	This statement is redundant and has been adequately covered throughout this section. Recommend it be deleted.
94	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

95	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".
96	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.
97	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.
98	Pages 32 and 33, Section 2.5.2	Examples bb through hh: Each of these examples	Recommend (bb) through (jj) be eliminated as

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

	(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.
99	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).
100	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.
101	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.	
102	Page 35, Section 2.6.2 (g)	N/A	Recommend deleting example g., due to it having no relation or concern to plant security.
103	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.
104	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.
105	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.
106	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.	
107	Page 47, Section 5.0, 2 nd paragraph, 1 st 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.
108	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.
109	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.
110	Page 50, Section 5.3 (g)	This example is unclear and requires further clarification.	
111	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.
112	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.
113	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.
114	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

115	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.
116	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).	
117	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".
118	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".
119	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?	
120	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"
121	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).
122	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.
123	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.
124	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.
125	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.
126	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.).	
127 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."
128 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 – WITHHOLD FROM PUBLIC DISCLOSURE~~

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

Document/Section/ Page Reference	Comment	Suggested Wording/Revision
<div style="border: 1px solid red; padding: 2px; width: 20px; display: inline-block; text-align: center;">1</div> Page 7, Section C, 1 st paragraph	<p>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.</p> <p>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:</p> <p style="text-align: center;"><u>4.The reason for inconsistencies detected through review of collected</u></p>	<p>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 <u>(excluding unescorted access authorization process potentially reportable issues)</u> 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.</p>

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

Document/Section/ Page Reference	Comment	Suggested Wording/Revision
	<p><u>information, i.e., intentional, innocent, or an oversight. Willful or intentional acts of omission or untruthfulness would be grounds for denial of UAA/UA.</u></p> <p>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.</p>	
Page 17, Section 2.3, 2 nd paragraph	<p>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</p>	<p>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.</p>

2

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

Document/Section/ Page Reference	Comment	Suggested Wording/Revision
	<p>personnel or contraband.</p> <p>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 misinterpreted 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.</p>	
3 Page 23, Section 2.3.2 (w)	<p>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)</p> <p>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</p>	<p>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 <i>or</i> 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.</p>
4 Page 47, Section 5, last paragraph	<p>Last paragraph states: Events recorded in the safeguards event log include failures, degradations, or discovered</p>	<p>Events recorded in the safeguards event log include failures, degradations, or discovered vulnerabilities that could have allowed</p>

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

Document/Section/ Page Reference	Comment	Suggested Wording/Revision
	<p>vulnerabilities that could have allowed unauthorized or undetected access to any area (e.g., <u>OCA</u>, PA, VA, MAA, or CAA) if compensatory measures were not in place or implemented at the time of discovery.</p> <p>There is no requirement to restrict access and account for unauthorized or undetected OCA access.</p>	<p>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.</p>
5 Page 50, Section 5.1 (g)	<p>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)</p> <p>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.</p>	<p>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 <i>or</i> 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.</p>
6 N/A	<p>New wording to be added to section 5.1 under 24 hour loggable event since there is no clear guidance for this</p>	<p>For cases of deliberate falsifications where the licensee denies access either because of the</p>

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)	<p>Section states: termination of personnel whose job duties and responsibilities actively support the licensee's or certificate holder's insider mitigation program</p> <p>On page 51 between 5.3.o and 5.3.p are the following words that apply to section 5.3.bb:</p> <p>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</p>	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.
9		
Page 60-61 Glossary Definition for Unauthorized Person	<p>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.</p> <p>Expand definition to unauthorized since the whole document references unauthorized persons, vehicles items and only unauthorized person was addressed.</p>	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.
10		
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.
11		

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
1 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.
2 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.
3 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
		<p>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.</p> <p>The reporting and recording requirements for cyber security should align with the date the Cyber Security Program is in effect.</p>
4 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.
5 Appendix G I. (h)(1)	<p>Recommend rewriting as follows:</p> <p>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, an 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.</p>	<p>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.</p> <p>The clarification to tie the threat’s impact to radiological sabotage is proposed to maintain alignment with the intent of §</p>

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."
6 Appendix G I. (h)(2)	<p>Recommend rewriting as follows:</p> <p>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.</p>	<p>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.</p> <p>The term "could" changed to "would" to maintain alignment with 10 CFR 73.54 (a)(2).</p> <p>The expression "that fall within the scope of § 73.54" added for clarity.</p>
7 Appendix G I. (c)(1)	<p>Recommend rewriting as follows:</p> <p>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.</p>	<p>The words "or surveillance" added to maintain alignment with the intent of four hour reportable physical security events.</p> <p>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.</p> <p>Added the words, "or attempts at access" to eliminate the need for the draft Section (c)(2).</p>

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

Document Section/Page Reference	Comment	Suggested Wording or Markup
8 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).
9 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.
10 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).
11 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).
12 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.
13 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.
14 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.
15 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).
16 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.
17 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.
18 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.
19 DG-5019/22 2.3.2.r.(2)	Rewrite as follows: Confirmed cyber attacks on computer systems that may adversely affected 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
19 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).
20 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.
21 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.
22 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.	
23 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.
24 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.
25 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).
26 DG-5019/24 2.3.2.ee	...the theft of sensitive cyber security data	There are no NRC regulations covering "sensitive cyber security data".
27 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
28 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
29 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).
30 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.
31 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.
32 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).
33 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	
34 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.
35 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".
36 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.
37 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.
38 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.
39 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	
40 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.
41 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.
42 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 sa safeguards event log CAP that may be indicative of a cyber attack	A review of the CAP would reveal this pattern.
43 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
		<p>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.</p> <p>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.</p> <p>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.</p>
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.
44 DG-5019/34 2.5.2.SS	Remove "...15 minute or..."	15-minute notification is not specified in 10CR73.71(a) for 10CFR73.54.
45 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
46		

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.
47 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.
48 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.
49 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.
50 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.	
51 DG-5019/50 5.3. ## (new)	Compensated cyber security event.	Capture events that are compensated, as required by Appendix G, Paragraph IV, Section (a).
52 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, <i>Nuclear Energy Institute 08-09, "Cyber Security Plan Template, Rev. 6,"</i> dated June 7, 2010. This definition is included in the industry Cyber Security Plans and is different than the definition in RG 5.71.
53 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 10CFR73 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.*

54

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

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

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
<p>Part 73, Appendix G, paragraph I.(h)(1):</p> <p><i>"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."</i></p> <p>Part 73, Appendix G, paragraph I.(h)(2):</p> <p><i>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</i></p>	<p>r.(2) Confirmed cyber attacks on CDAs that may adversely affect safety, security, and emergency preparedness functions are reportable.</p> <p>aa. [Remove]</p> <p>bb. an actual penetration or compromise of a CDA, where a person who is not authorized access circumvents the control measures</p> <p>(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.</p> <p>(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.</p> <p>(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, <i>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.</i></p>

55

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

56

Reporting Criteria	Example
<i>Paragraph I.(h)(1) be reported within one hour of discovery.</i>	<p>(4) [Remove]</p> <p>(5) [Remove]</p> <p>cc. the discovery of malware installed on a CDA</p> <p>dd. [Remove]</p> <p>ee. the theft of sensitive cyber security data</p> <p>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</p> <p>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??]</p> <p>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</p> <p>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??]</p> <p>jj. [Remove duplicate of 2.3.2.t]</p> <p>kk. [Remove – duplicate of 2.3.2.u]</p> <p>ll. [Remove – duplicate of 2.3.2.v]</p> <p>mm. [Remove – duplicate of 2.3.2.y]</p>

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

Reporting Criteria	Example
	<p>nn. [Remove]</p> <p>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]</p>



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

Comment Submission No. 13
(ML11216A139)

(Comment-Response Document Abbreviation: PV)

2/3/2011
76 FR 6085

(3)

RECEIVED

FEB 02 2011 AM 9:56

REGULATORY SERVICES
FEB 02 2011

From fals Verde, NPP - via NET

SUNSI Review Complete
Template = ADM-013

FRDS = ADM-03

Add = R. Carpenter (vge2)
m. Case (m5c)
P. Brachman (pgb)



DRAFT REGULATORY GUIDE

Contact: P. Brochman
(301) 415-6557

DRAFT REGULATORY GUIDE DG-5019, Revision 1

(Proposed Revision 2 of Regulatory Guide 5.62, dated November 1987)

REPORTING AND RECORDING SAFEGUARDS EVENTS

A. INTRODUCTION

This draft regulatory guide (DG) describes methods that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable for licensees and certificate holders to report and record safeguards (i.e., security) events. This guide applies to a range of facilities and activities licensed or certified by the NRC. These facilities and activities include reactor facilities; special nuclear material (SNM) production, use, and storage facilities; spent nuclear fuel (SNF) and high-level radioactive waste (HLW) storage and disposal facilities; and the transportation of SNM, SNF, and HLW to or from such facilities.

Title 10 of the *Code of Federal Regulations* (10 CFR) 73.71, "Reporting and Recording of Safeguards Events," requires licensees and certificate holders to report certain safeguards events to the NRC Headquarters Operations Center and to record certain security events in a safeguards event log. Appendix G, "Reportable and Recordable Safeguards Events," to 10 CFR Part 73, "Protection of Plants and Materials," (Ref. 1) provides additional detail on the specific security events to be reported or recorded. In support of 10 CFR 73.71, Appendix A to 10 CFR Part 73, "U.S. Nuclear Regulatory Commission Offices and Classified Mailing Addresses," contains contact information for the NRC Headquarters Operations Center and directions on communicating ~~classified~~ security events to the NRC.

Comment [z1]: The term "classified" used here could be confused with events described in 10CFR50.47.

This guide provides examples of security events that represent actual or potential threats, suspicious activities, challenges to security systems or processes, or internal tampering with equipment that threatens or affects the safe operation or the security of facilities and transportation activities. This guide also provides examples of security events that adversely impact the effectiveness of security systems, components, and procedures required by the NRC's security regulations under 10 CFR Part 73 or the licensee's or certificate holder's NRC-approved security plans. Finally, this guide provides examples of events that are indicative of ~~security conditions imminent or actual~~ hostile actions against reactor facilities, Category I strategic special nuclear material (SSNM) facilities, and the transportation of SSNM, SNF, and

Formatted: Font color: Blue

This regulatory guide is being issued in draft form to involve the public in the early stages of the development of a regulatory position in this area. It has not received final staff review or approval and does not represent an official NRC final staff position. Public comments are being solicited on this draft guide (including any implementation schedule) and its associated regulatory analysis or value/impact statement. Comments should be accompanied by appropriate supporting data. Written comments may be submitted to the Rules, Announcements, and Directives Branch, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001; submitted through the NRC's interactive rulemaking Web page at <http://www.nrc.gov>; or faxed to (301) 492-3446. Copies of comments received may be examined at the NRC's Public Document Room, 11555 Rockville Pike, Rockville, MD. Comments will be most helpful if received by May 4, 2011.

Electronic copies of this draft regulatory guide are available through the NRC's interactive rulemaking Web page (see above); the NRC's public Web site under Draft Regulatory Guides in the Regulatory Guides document collection of the NRC's Electronic Reading Room at <http://www.nrc.gov/reading-rm/doc-collections/>; and the NRC's Agencywide Documents Access and Management System (ADAMS) at <http://www.nrc.gov/reading-rm/adams.html>, under Accession No. ML10100690087. The regulatory analysis may be found in ADAMS under Accession No. ML10100157.

HLW. This guide also describes required reports to the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) and local law enforcement agencies (LLEAs) regarding lost or stolen enhanced weapons.

Licensees and certificate holders should consider obtaining access to the NRC's protected Web server (PWS) to obtain routine threat bulletins and analyses the NRC receives from the Federal Bureau of Investigation (FBI) and the U.S. Department of Homeland Security (DHS) on critical national infrastructure and key resources. Licensees and certificate holders desiring access to the NRC's PWS should make their request through the security staff in their applicable NRC regional office.

This guide provides acceptable methods and examples for use by licensees and certificate holders to determine whether to report or record security events. The NRC staff does not consider the examples provided in this guide to be all inclusive. If a licensee or certificate holder has questions regarding the reporting or recording of a specific security event, they may, if time permits, discuss this matter with the NRC security staff in their applicable regional office or the staff from the Office of Nuclear Security and Incident Response in NRC Headquarters. Otherwise, the licensee or certificate holder should report the event and then discuss it with appropriate NRC staff. Licensees and certificate holders may subsequently withdraw a report of an invalid security event, without prejudice.

A licensee or certificate holder should not consider security events reported under this guide as indicative of performance failures. Rather, the NRC considers timely and comprehensive communication of matters relating to threats, attacks, or suspicious activities a vital component of its efforts to assess the current threat environment. Since our Nation's enemies have demonstrated the ability to attack multiple independent targets, timely reporting of non-threatening but suspicious activities is important to the NRC, law enforcement agencies, and the intelligence community in order to integrate potential adversary plans, intentions, and suspicious event reports into the ongoing assessment of the "current threat environment." The prompt reporting of actual or imminent hostile actions permits the NRC to execute its strategic missions of communicating hostile action against the facilities and activities it regulates to senior Federal officials and to other licensees and certificate holders; thereby protecting public health and safety, the common defense and security, and the environment.

The NRC's previous guidance on reporting and recording security events remains in effect until this revision to RG 5.62 is issued. Additionally, subsequent to the issuance of this revision to RG 5.62 the NRC plans to conduct a workshop on these revised security event reporting and recording requirements with the goal of producing Revision 1 to NUREG-1304, "Reporting of Safeguards Events." NUREG-1304 is based upon a workshop on reporting and recording safeguards events that was held in 1988 following the issuance of RG 5.62, Rev. 1. NUREG-1304 is structured in a question and answer format.

This draft regulatory guide is being issued for comment in support of the NRC's proposed revisions to the safeguards event reporting and recording requirements in 10 CFR 73.71 and Appendix G to 10 CFR Part 73 (Appendix G). However, this RG does not apply to licensees and certificate holders reporting fitness-for-duty events to the NRC.

The NRC issues regulatory guides to describe to the public the methods that the staff considers acceptable for use in implementing specific parts of the agency's regulations, to explain techniques that the staff uses in evaluating specific problems or postulated accidents, and to provide guidance to applicants. Regulatory guides are not substitutes for regulations and compliance with regulatory guides is not required.

This regulatory guide contains information collection requirements covered by 10 CFR Part 73 that the Office of Management and Budget (OMB) approved under OMB control number 3150-0002.

The NRC may neither conduct nor sponsor, and a person is not required to respond to, an information collection request or requirement unless the requesting document displays a currently valid OMB control number. The NRC has determined that this Regulatory Guide is not a major rule as designated by the Congressional Review Act and has verified this determination with the OMB.

A. INTRODUCTION.....	1
B. DISCUSSION.....	6
C. REGULATORY POSITION.....	7
1. Applicability.....	8
2. Telephonic Reportable Security Events.....	10
2.1 Facility Security Events To Be Reported within 15 Minutes.....	12
2.1.1 Notification Requirements.....	13
2.1.2 Examples of Reportable Events.....	13
2.2 Transportation Security Events To Be Reported within 15 Minutes.....	14
2.2.1 Notification Requirements.....	15
2.2.2 Examples of Reportable Events.....	16
2.3 Facility Security Events To Be Reported within 1 Hour.....	17
2.3.1 Notification Requirements.....	18
2.3.2 Examples of Reportable Events.....	20
2.4 Transportation Security Events To Be Reported within 1 Hour.....	25
2.4.1 Notification Requirements.....	26
2.4.2 Examples of Reportable Events.....	27
2.5 Facility Security Events To Be Reported within 4 Hours.....	28
2.5.1 Notification Requirements.....	29
2.5.2 Examples of Reportable Events.....	30
2.6 Facility-Security Events To Be Reported within 8 Hours.....	34
2.6.1 Notification Requirements.....	34
2.6.2 Examples of Reportable Events.....	34
2.7 Enhanced Weapons—Stolen or Lost, To Be Reported within 1 Hour or 4 Hours.....	35
2.7.1 Notification Requirements.....	36
2.7.2 Examples of Reportable Events.....	37
2.8 Enhanced Weapons—Adverse ATF Findings To Be Reported within 24 Hours.....	37
2.8.1 Notification Requirements.....	37
2.8.2 Examples of Reportable Events.....	38
3. Telephonic Reporting Process.....	38
3.1 Telephonic Reporting Process Requirements.....	38
3.2 Content of 15-Minute Reports.....	40
3.3 Content of 1-Hour, 4-Hour, and 8-Hour Reports.....	40
3.4 Content of 4-Hour Suspicious Activity Reports.....	41
3.5 Reports Containing Safeguards Information.....	41
3.6 Reports Containing Classified Information.....	41
3.7 Continuous Communications Channel Requirements.....	42
3.8 Reporting Significant Additional Information.....	42
3.9 Emergency Declarations and Duplicate Reports.....	43
3.10 Retraction of Previous Telephonic Security Event Reports.....	43
4. Written Followup Reports.....	43
4.1 Written Followup Report Requirements.....	44
4.2 Retraction of Previous Written Followup Reports.....	45
4.3 Significant Additional Information and Correction of Errors.....	45
4.4 Use of NRC Form 366.....	45
4.5 Content of Written Followup Reports.....	45
5. Security Events To Be Recorded within 24 Hours.....	47

5.1 Safeguards Event Log Record Requirements	48
5.2 Content of the Safeguards Event Log	50
5.3 Example of Facility Events To Be Recorded in the Safeguards Event Log	50
5.4 Examples of Transportation Events To Be Recorded in the Safeguards Event Log	52
6. Security Events that Are Not Considered Reportable or Recordable	53
6.1 Examples of Events that are Not Required to be Reported	53
6.2 Examples of Events that are Not Required to be Recorded in the Safeguards Event Log ...	54
7. Training of Nonsecurity Staff on Reporting and Recording Requirements	55
D. IMPLEMENTATION	56
GLOSSARY	57
REFERENCES	62
SUPERSEDED REFERENCES	64
APPENDIX A	A-1

B. DISCUSSION

The reports and records made by licensees and certificate holders under 10 CFR 73.71 and Appendix G are intended to inform the NRC, and potentially other Federal intelligence and law enforcement agencies, of security-related events that could (1) endanger public health and safety or the common defense and security, (2) provide information for threat-assessment processes, or (3) generate public or media inquiries. The required information also contributes to the NRC's analysis of the reliability and effectiveness of licensees' and certificate holders' security programs and systems.

The regulations in 10 CFR 73.71 and Appendix G require licensees and certificate holders to report certain security events to the NRC Headquarters Operations Center. These regulations require licensees and certificate holders to notify the NRC by telephone of the discovery of these security events. Additionally, the regulations in 10 CFR 73.71 and Appendix G require licensees and certificate holders to record certain other security events in a safeguards event log. NRC security inspectors periodically review and analyze the events listed in the safeguards event log as part of the NRC's routine security inspection, oversight, and enforcement programs. The regulations also require licensees and certificate holders to submit written followup reports to the NRC subsequent to certain verbal reports made under 10 CFR 73.71. The type of information to be reported to the NRC is generally focused on event descriptions, threat-related information, and security systems' performance, reliability, and effectiveness. This guide follows the structure of the proposed revision to 10 CFR 73.71 and Appendix G. Appendix G supports the regulations contained in 10 CFR 73.71 and provides a more detailed description of the types of events and information to be reported or recorded.

3 | The timing of these reports can range from within 15 minutes of discovery to within 24 hours of discovery, depending on the significance and impact of the event being reported or recorded. Significant security events may warrant immediate NRC actions. For example, 10 CFR 73.71 requires licensees and certificate holders to report actual or imminent hostile actions within 15 minutes of discovery. Upon notification of ~~such~~ a hostile action, the NRC will rapidly communicate this information to other NRC licensees and certificate holders and to other Federal agencies to enable them to immediately increase the response level of their security defenses.

Other less serious, but still significant, events require reports within 1 hour of discovery. Events involving suspicious activities and potential tampering or unauthorized operation of components require reports within 4 hours and 8 hours of discovery, respectively. For certain events, the NRC may, upon its discretion, request the licensee or certificate holder to establish a continuous communications channel with the NRC Headquarters Operations Center (to facilitate the communication of information during an ongoing event).

With the addition of provisions to 10 CFR Part 73 permitting certain licensees and certificate holders to possess enhanced weapons (see glossary), the regulations require 1-hour or 4-hour notifications for reporting the discovery of stolen or lost enhanced weapons. The NRC requires licensees or certificate holders to report within 24 hours of the receipt of an adverse inspection or enforcement finding or other adverse notice from ATF regarding the licensee's or certificate holder's possession, receipt, transfer, or storage of enhanced weapons.

4 | This revised guide explains the types of information that licensees and certificate holders should report to satisfy the requirements of the proposed rule and gives several examples to illustrate some of the events that may occur and should be reported. The NRC staff developed the examples, which illustrate the types of actual occurrences that should be reported. This draft guide contains many examples to help licensees, certificate holders, and NRC staff sort security-related events into the proper reporting categories. If these examples are understood~~interpreted~~ as being the only events to be reported, they may seem to be contradictory or confusing. For virtually every example provided, the addition or subtraction of a single aspect not explicitly detailed in the example could easily move it into a higher or lower timeliness category. Accordingly, the use of these examples should be tempered with the texts of 10 CFR

73.71, Appendix G, and other guidance contained in this guide. When determining the reportability of a particular event, a licensee, certificate holder, or the NRC staff should review the basic rule language and the guidance and the specific examples contained in this guide.

The NRC intends that licensees and certificate holders only report and record information required by the agency's regulations. To assist licensee and certificate holders, this guide also provides information and examples of occurrences that the NRC staff does not consider recordable. As with other portions of this guide, the NRC staff considers the information that is contained in Regulatory Position 6, "Security Events that Are Not Considered Recordable," as being neither limiting nor constraining, and the licensee or certificate holder is ultimately responsible for ensuring compliance with the regulatory requirements.

C. REGULATORY POSITION

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. However, licensees and certificate holders may contact the NRC and withdraw an invalid report (based upon a subsequent analysis of the circumstances of an event). A licensee or certificate holder may make withdrawals without prejudice to its security performance indicators. Confusion, misinterpretation, erroneous determinations, and a reluctance to report security events in the past have caused difficulties for the NRC staff and a lack of consistency among licensees and certificate holders.

The NRC staff has developed this guide based on examples of previous events and interactions between NRC staff and licensee or certificate holders. This guide is intended to provide assistance to licensees and certificate holders in evaluating a broad range of potential security events on whether these events should be reported or recorded under the provisions of 10 CFR 73.71 and Appendix G. The NRC staff considers the specific events listed in this guide as examples of reportable or recordable security events. As such, the NRC staff does not consider these lists as exhaustive or exclusive. Many of the examples listed herein have been created from actual events at NRC-regulated facilities or from licensee and certificate holder discussions with NRC staff on whether a particular event was reportable, recordable, or neither.

The NRC staff encourages licensees and certificate holders to report security notifications and subsequently retract them, if appropriate (e.g., as invalid events) rather than delaying the initial report to gather more information and thus have greater confidence in whether or not to make a report. If a licensee or certificate holder has questions about whether to report or record an event, the licensee or certificate holder can, if time permits, discuss the event with their appropriate NRC regional or Headquarters security staff before making a report or record. However, if the questions cannot be resolved, licensees or certificate holders should report all security events to the NRC within the timeliness requirements of 10 CFR 73.71. However, if the licensee or certificate holder subsequently determines that the event did not require a report (e.g., the event was invalid), the licensee or certificate holder may retract the report in accordance with the provisions of 10 CFR 73.71(j)(8) and 10 CFR 73.71(m)(13).

5 In addition to examples of events regarding failures and challenges to the licensee's or certificate holder's security programs and systems, the requirements in 10 CFR 73.18 and Appendix G direct licensees and certificate holders to also report suspicious events to the NRC. The NRC staff use the information developed from reports of suspicious activity in assessing the current threat environment. In addition, the NRC forwards appropriate reports of suspicious activities to federal law enforcement agencies and the intelligence community as part of the National threat assessment process. Accordingly, the NRC staff has added examples of suspicious events that should be reported to the NRC. The U.S. government considers suspicious activity as "observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity." Licensees and certificate holders are considered "key resource owners and operators" and can find additional guidance on examples of suspicious activities in the U.S. Department of Homeland Security's, "Terrorist Threats to the U.S. Homeland: Reporting Guide for Critical Infrastructure and Key Resource Owners and Operators," (Ref. 8).

Comment [z2]: Terminology should be consistent. Suspicious activity should also be a defined term in the Glossary. The term "Events" needs to be maintained separate from activities to avoid confusion by licensees when considering classification. This also allows for consistent use of the term "activity" within this section.

6 Although, the NRC staff views the overall goal of reducing unnecessary security event notifications as worthwhile, the NRC staff continues to believe that the time period for making notifications should begin at the licensee's or certificate holder's time of discovery of an issue, as opposed to the time when it concludes (following review and evaluation) that a reportable event has occurred. For example, a similar security event may have occurred at other facilities and may be related or indicate a broader trend. The timely integration of multiple intelligence or threat threads into the current threat assessment requires timely notification from licensees to develop this integrated assessment. For example, the NRC is concerned that a potentially innocuous activity event at a single site (that could indicate attempted reconnaissance or surveillance) is quite different from similar events occurring at multiple sites or across multiple sectors of the country. Because suspicious activities (e.g., attempted reconnaissance or challenges to security systems) may be indicative of preoperational malevolent activities and our nation's enemies have demonstrated a capability to simultaneously attack multiple independent targets, the NRC has established requirements for reporting suspicious activities. Analysis of individual activities (at separate facilities or activities) may reveal to the NRC, law enforcement authorities, or the intelligence community potential threats or patterns that warrants increasing the security posture for NRC-regulated facilities and activities, other government facilities and activities, and other national critical-infrastructure facilities.

1 Applicability

This regulatory position provides information to licensees and certificate holders on the classes of NRC-regulated facilities and activities that are subject to specific reporting and recording provisions of 10 CFR 73.71 and Appendix G.

- a. The regulations in 10 CFR 73.71(a) regarding 15-minute notifications for facilities apply to licensees and certificate holders subject to the provisions of 10 CFR 73.20, "General Performance Objective and Requirements"; 10 CFR 73.45, "Performance Capabilities for Fixed Site Physical Protection Systems"; 10 CFR 73.46, "Fixed Site Physical Protection Systems, Subsystems, Components, and Procedures"; and 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage." This includes fuel cycle facilities authorized to possess and use Category I quantities of SSNM and power reactor and production reactor facilities.
- b. The regulations in 10 CFR 73.71(b) regarding 15-minute notifications for shipments apply to licensees and certificate holders subject to the provisions of 10 CFR 73.20; 10 CFR 73.25, "Performance Capabilities for Physical Protection of Strategic Special Nuclear Material in Transit"; 10 CFR 73.26, "Transportation Physical Protection Systems, Subsystems, Components, and Procedures"; and 10 CFR 73.37, "Requirements for Physical Protection of Irradiated Reactor

Fuel in Transit.” This includes the transportation of Category I quantities of SSNM, SNF, and HLW.

- c. The regulations in 10 CFR 73.71(c) regarding 1-hour notifications for facilities apply to licensees and certificate holders subject to the provisions of 10 CFR 73.20; 10 CFR 73.45; 10 CFR 73.46; 10 CFR 73.50, “Requirements for Physical Protection of Licensed Activities”; 10 CFR 73.51, “Requirements for the Physical Protection of Stored Spent Nuclear Fuel and High-Level Radioactive Waste”; 10 CFR 73.54, “Protection of Digital Computer and Communication Systems and Networks”; 10 CFR 73.55; 10 CFR 73.60, “Additional Requirements for Physical Protection at Nonpower Reactors”; or 10 CFR 73.67, “Licensee Fixed Site and In-Transit Requirements for the Physical Protection of Special Nuclear Material of Moderate and Low Strategic Significance.” This includes fuel cycle facilities authorized to possess and use Category I quantities of SSNM, hot cell facilities, independent spent fuel storage installations (ISFSIs), monitored retrievable storage installations (MRSs), geologic repository operations areas (GROAs), power reactor facilities, production reactor facilities, research and test reactor facilities, and fuel cycle facilities authorized to possess and use Category II and Category III quantities of SNM.
- d. The regulations in 10 CFR 73.71(d) regarding 1-hour notifications for shipments apply to licensees and certificate holders subject to the provisions of 10 CFR 73.25, 10 CFR 73.26, 10 CFR 73.27, 10 CFR 73.37, and 10 CFR 73.67. This includes the transportation of SNF, HLW, or Category II and Category III quantities of SNM.
- e. The regulations in 10 CFR 73.71(e) regarding 4-hour notifications for facilities apply to licensees and certificate holders subject to the provisions of 10 CFR 73.20, 10 CFR 73.45, 10 CFR 73.46, 10 CFR 73.50, 10 CFR 73.51, 10 CFR 73.54, 10 CFR 73.55, 10 CFR 73.60, or 10 CFR 73.67. This includes fuel cycle facilities authorized to possess and use Category I quantities of SSNM, hot cell facilities, ISFSIs, MRSs, GROAs, power reactor facilities, production reactor facilities, research and test reactor facilities, and fuel cycle facilities authorized to possess and use Category II and Category III quantities of SNM.
- f. The regulations in 10 CFR 73.71(f) regarding 8-hour notifications for facilities apply to licensee and certificate holders subject to the provisions of 10 CFR 73.20, 10 CFR 73.45, 10 CFR 73.46, 10 CFR 73.50, 10 CFR 73.51, 10 CFR 73.54, 10 CFR 73.55, 10 CFR 73.60, or 10 CFR 73.67. This includes fuel cycle facilities authorized to possess and use Category I quantities of SSNM, hot cell facilities, ISFSIs, MRSs, GROAs, power reactor facilities, production reactor facilities, research and test reactor facilities, and fuel cycle facilities authorized to possess and use Category II and Category III quantities of SNM.
- g. The regulations in 10 CFR 73.71(g) regarding 1-hour or 4-hour notifications for stolen or lost enhanced weapons apply to licensee and certificate holders that fall within the classes of facilities, radioactive material, and other property specified in 10 CFR 73.18(c), “Authorization for Use of Enhanced Weapons and Preemption of Firearms Laws”; and the licensee or certificate holder possesses enhanced weapons under 10 CFR 73.18.
- h. The regulations in 10 CFR 73.71(h) regarding 24-hour notifications for the receipt of an adverse ATF inspection or enforcement finding or other adverse notices (regarding a licensee’s or certificate holder’s possession, receipt, transfer, or storage of enhanced weapons) apply to licensees and certificate holders possessing enhanced weapons under 10 CFR 73.18.

- i. The regulations in 10 CFR 73.71(j) regarding the process for making telephonic notifications of reportable security events under 10 CFR 73.71(a), (b), (c), (d), (e), (f), (g), and (h) apply to the licensees and certificate holders listed under Regulatory Positions 1.a through 1.h above. This includes fuel cycle facilities authorized to possess and use Category I quantities of SSNM, hot cell facilities, ISFSIs, MRSSs, GROAs, power reactor facilities, research and test reactor facilities, and fuel cycle facilities authorized to possess and use Category II and Category III quantities of SSNM. This includes the transportation of Category I quantities of SSNM, SNF, HLW, and Category II and III quantities of SSNM. This also applies to notifications of stolen or lost enhanced weapons or inspection or enforcement findings or other adverse notices from ATF.
- j. The regulations in 10 CFR 73.71(k) regarding the recording of security events in a safeguards event log apply to each licensee or certificate holder subject to the provisions of 10 CFR 73.20, 10 CFR 73.25, 10 CFR 73.26, 10 CFR 73.37, 10 CFR 73.45, 10 CFR 73.46, 10 CFR 73.50, 10 CFR 73.51, 10 CFR 73.54, 10 CFR 73.55, 10 CFR 73.60, and 10 CFR 73.67. This includes fuel cycle facilities authorized to possess and use Category I quantities of SSNM, hot cell facilities, ISFSIs, MRSSs, GROAs, power reactor facilities, research and test reactor facilities, and fuel cycle facilities authorized to possess and use Category II and Category III quantities of SSNM. This also includes the transportation of Category I quantities of SSNM, SNF, HLW, and Category II and III quantities of SSNM.
- k. The regulations in 10 CFR 73.71(m) regarding the submission of written followup reports of security events under 10 CFR 73.71(a), (b), (c), (d), (e), (f), and (g) apply to the licensees and certificate holders described in Regulatory Positions 1.a through 1.g above.
- l. The regulations in 10 CFR 73.71(n) regarding security events that also warrant an Emergency Classification apply to the reactor, fuel cycle, ISFSI, MRS, GROA, and gaseous diffusion facilities licensed or certified by the NRC.
- m. The regulations in paragraphs I, II, and III of Appendix G apply to licensees and certificate holders subject to the provisions of 10 CFR 73.71(c), (e), and (j) (see Regulatory Positions 1.a, 1.c, and 1.j above).
- n. The regulations in paragraphs I and III of Appendix G apply to licensees and certificate holders subject to the provisions of 10 CFR 73.71(c), (d), and (j) (see Regulatory Positions 1.c, 1.d, and 1.j above).
- o. The regulations in paragraph IV of Appendix G apply to licensees and certificate holders subject to the provisions of 10 CFR 73.71(k) (see Regulatory Positions 1.a through 1.g above).

2 Telephonic Reportable Security Events

The regulations in 10 CFR 73.71(a), (b), (c), (d), (e), (f), (g), and (h) require licensees and certificate holders to make a telephonic notification to the NRC of certain security events. Events requiring telephonic notifications ~~are considered significant and~~ require clear, person-to-person communication. Regulatory Position 4 below contains guidance regarding the information to be provided during telephonic notifications. The NRC staff is using the phrase "telephonic notification" to refer to verbal reports made using a telephone (e.g., using a land line, cellular, satellite, voice over IP capability, etc.), rather than e-mails, faxes, or text messages. The NRC views that human-to-human communication is necessary for these types of event reports to provide for follow-up questions and clarifications, requests for information or action, and to facilitate NRC response activities. For some events, the NRC Headquarters Operations Center may request the licensee or certificate holder establish a continuous

communications channel with the NRC. Regulatory Position 3.7 below provides guidance to the licensee or certificate holder on establishing a continuous communications channel, if requested by the NRC.

The purpose of a telephonic notification is to ensure timely, direct, and accurate communication of information to the NRC related to security matters that may require action by the licensee, certificate holder, the NRC, the intelligence community, or another government agency. These actions may involve a change in the NRC Headquarters Operations Center's and Regional Incident Response Center's response mode or a change in the need to respond to public or media inquiries about an event. Other methods of communication, such as e-mail or text messaging, should not be used unless extreme conditions prohibit telephonic reporting. This guide contains examples of reports to assist licensees and certificate holders and the NRC staff in evaluating the reportability of security events and information received from licensees and certificate holders. The NRC considers these examples to be neither limiting nor all-inclusive.

Telephonic notifications should be focused on occurring events, not their resolution, final analysis, suspected motivation of any participants, or technical evaluations. While those necessary actions should be considered part of the response function and should eventually be reported, they should not affect the timely telephonic communication of the event.

Depending on the type of licensee or certificate holder, and the type of information required to be reported, the timeliness of telephonic reports differ, as described below. Timeliness in telephonic reporting is important to ensure effective communication among potential responders, the intelligence and law enforcement communities, and other government agencies. The accuracy of information provided in telephonic reports is likewise important to ensure that decisions relating to potential response and threat analysis are appropriate. Licensees and certificate holders should provide the most complete and accurate information available to them when they make telephonic reports. Licensees and certificate holders should make additional calls describing substantive changes, additions, or modifications to the initial information in a timely manner after taking immediate actions to protect the facility or stabilize its operations, in accordance with their emergency operations and contingency response procedures.

In addition to notifications made to the NRC Headquarters Operations Center for security events under 10 CFR 73.71 and Appendix G, this guide describes notifications that should be made to LLEAs within 48 hours of discovery to report the theft or loss of an enhanced weapon under 10 CFR 73.18.

The NRC recognizes that some events that require telephonic security reports may also require the licensee or certificate holder to report and declare an emergency declaration under the applicable provisions of 10 CFR 50.72, "Immediate Notification Requirements for Operating Power Reactors" (Ref. 2); 10 CFR 70.50, "Reporting Requirements" (Ref. 3); 10 CFR 72.75, "Reporting Requirements for Specific Events and Conditions" (Ref. 4); or 10 CFR 76.120, "Reporting Requirements" (Ref. 5). Licensees and certificate holders should be aware that, while dual reporting (making two separate phone calls to report the same information) is not required under 10 CFR 73.71, a reportable security event may have more restrictive timeliness requirements than an emergency declaration (e.g., the imminent attack notification requirements of 10 CFR 73.71(a) and (b)). Furthermore, telephonic reports should not interfere with the licensee's or certificate holder's actual response to an emergency or security event or to requesting offsite assistance from an LLEA; however, licensees and certificate holders should consider telephonic notifications a high priority task, to ensure that the NRC and other government agencies respond appropriately to events with potentially broader implications than a single facility. Regulatory Position 4.7 below contains specific guidance regarding dual reporting of security events.

Comment [z3]: Emergency declarations are governed under 50.47 and so use of the word "declare" in this context does not comport with the 50.72 reference in the next part of the sentence.

Because of the importance of timely telephonic notifications, licensees and certificate holders making security event notifications that contain Safeguards Information may make such notifications to the NRC Headquarters Operations Center without using a secure communications system under the

exception of 10 CFR 73.22(f)(3) for emergency or extraordinary conditions. However, licensees or certificate holders should try to protect sensitive information whenever possible. If a license or certificate holder has provided Safeguards Information to the NRC Headquarters Operations Center over a nonsecure communications system, it should include this fact as part of the information conveyed to the NRC. Licensees and certificate holders should develop procedures to assist operations, security, and emergency response managers and other key personnel in evaluating events for their reportability, providing the necessary information to the NRC, and ensuring that the need for appropriate information security is balanced with the timeliness of providing information to the NRC.

For reports containing classified national security information or restricted data, licensees and certificate holders should make such telephonic notifications by using a secure communications system. Alternate provisions are discussed in Regulatory Position 4 below.

In addition to providing information on the physical security and information security events that are required to be reported and recorded under 10 CFR 73.71 and Appendix G, this guide includes information on reporting and recording cyber security events. However, cyber security event notifications only apply to licensees and certificate holders that are subject to the requirements of 10 CFR 73.54. This regulation requires power reactor licensees to establish and maintain a cyber security program at their facilities to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design-basis threat, as described in 10 CFR 73.1, "Purpose and Scope" (Ref. 1).

21 Facility Security Events To Be Reported within 15 Minutes

The regulations in 10 CFR 73.71(a) require each licensee or certificate holder subject to the provisions of 10 CFR 73.20, 10 CFR 73.45, 10 CFR 73.46, or 10 CFR 73.55 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 against a Category I SSNM facility or a power reactor facility. This rapid notification is intended to provide the NRC with an abbreviated set of facts that can be immediately disseminated to other licensees, certificate holders, and government agencies, to enable them to rapidly increase their security posture.

The fundamental purpose of a 15-minute report is to allow the NRC to (1) warn other licensees and certificate holders of this ongoing event (to immediately increase their defensive posture) and (2) notify other Federal agencies. Accordingly, the NRC has reduced the amount of information licensees and certificate holders should provide in the report. Furthermore, the NRC may require the licensee or certificate holder to establish a continuous communications channel as soon as possible after making the 15-minute report (see Regulatory Position 3.7 below). This flexibility is intended to relieve licensees and certificate holders of a communications burden while they immediately respond to the event, direct personnel, request LLEA assistance, and staff the communicator position (for a continuous communications channel) with an appropriately trained individual.

A licensee's or certificate holder's request for immediate LLEA assistance should take precedence over the notification to the NRC. Protecting public health and safety and the common defense and security should always be the licensee's and certificate holder's first priority. ~~Furthermore, this regulatory guide does not apply to aircraft threats and attacks. Guidance on licensee response to aircraft threats and attacks is found in Regulatory Guide 1.214, "Response Strategies for Potential Aircraft Threats" (Ref. 6).~~

Comment [z4]: RG 1.214, page 12 does refer to NRC notification of licensee actions. Stating here that aircraft threats and attacks are not included may lead to confusion on the part of the licensee as these are also a part of classifiable security events under 10 CFR 50.47 via NEI 99-01 Rev 5.

12

These reports involve both the licensee's or certificate holder's discovery of an imminent or actual hostile action and the initiation of a security response in accordance with the safeguards contingency plan or protective strategy that is based upon an actual or imminent hostile action or security condition. Although the licensee's and certificate holder's plans and procedures typically describe many levels of security response, for the purposes of this reporting requirement, the security response means the substantive implementation (or deployment) of the facility's armed response capabilities to defensive positions or locking down normal access to the facility or within the facility (i.e., a security contingency event response). The regulations do not require licensees and certificate holders to report security responses that are initiated as a result of a threat or warning information communicated to them by the NRC.

13

Reports made under this provision apply only to ongoing security events, either actual or imminent. ~~In the first circumstance, a licensee or certificate holder has been subject to a hostile action. A hostile action upon an applicable licensed facility or its personnel has either been committed or is in progress and includes the use of violent force to destroy equipment, take hostages, or intimidate the licensee or certificate holder. Hostile actions include attacks by air, land, or water, using weapons, explosives, projectiles, vehicles, or other devices to deliver destructive force. In the second circumstance, an imminent hostile action is one for which the licensee or certificate holder has received information on the potential action and it fits the characteristics (of a hostile action) described in this paragraph.~~

Comment [z5]: This paragraph does not match the NRC and Industry accepted definition of a hostile action and so should not be included

2.1.1 Notification Requirements

10 CFR 73.71(a) 15-minute notifications – facilities. Each licensee or certificate holder subject to the provisions of §§ 73.20, 73.45, 73.46, or 73.55 shall notify the NRC Headquarters Operations Center, as soon as possible but not later than 15 minutes after —

- (1) The discovery of an imminent or actual hostile action against a nuclear power or production reactor or Category I SSNM facility; or*
- (2) The initiation of a security response in accordance with a licensee's or certificate holder's safeguards contingency plan or protective strategy, based on an imminent or actual hostile action against a nuclear power reactor or Category I SSNM facility;*
- (3) These notifications shall:*
 - (i) Identify the facility name;*
 - (ii) Include the authentication code; and*
 - (iii) Briefly describe the nature of the hostile action or event, including:*
 - (A) Type of hostile action or event (e.g., armed assault, vehicle bomb, credible bomb threat, etc.);*

and

- (B) Current status (i.e., imminent, in progress, or neutralized).*
- (4) Notifications must be made according to paragraph (j) of this section, as applicable.*
- (5) The licensee or certificate holder is not required to report security responses initiated as a result of threat or warning information communicated to the licensee or certificate holder by the NRC.*
- (6) A licensee's or certificate holder's request for immediate local law enforcement agency (LLEA) assistance can take precedence over the notification to the NRC.*

2.1.2 Examples of Reportable Events

The NRC staff considers that the following facility-security events are examples of the types of events that require notification under 10 CFR 73.71(a):

- a. the licensee's or certificate holder's discovery of an imminent or actual hostile act against its nuclear power reactor or Category I SSNM facility

- b. the detonation of explosives or an explosive device at or in close proximity (within site boundaries) to the licensee's or certificate holder's facility, including the use of explosives by ground assault force personnel and the use of land-based or waterborne vehicle bombs
- c. unauthorized weapons being fired within any controlled area of licensee's or certificate holder's facility
- d. weapons being fired at the licensee's or certificate holder's facility and projectiles hitting the facility that causes an immediate threat to the facility or to security personnel
- e. the successful, forcible penetration of a protected area (PA), vital area (VA), material access area (MAA), or controlled access area (CAA) by unauthorized personnel or vehicles
- f. the taking of hostages onsite
- g. the taking of hostages offsite that is reasonably determined to be related to facility operations or security functions (e.g., the kidnapping of family members in order to coerce facility employees into violating laws, NRC regulations, or the facility's license or certificate of compliance)
- h. actual or believed theft of SSNM or SNF
- i. the licensee's or certificate holder's notification from law enforcement authorities or another reliable source that an explosion or other assault on the facility is imminent
- j. the licensee's or certificate holder's initiation of a security response in accordance with its safeguards contingency plan or protective strategy, based on an imminent or actual hostile action against its nuclear power reactor or Category I SSNM facility
- k. a vehicle demonstrating an actual or attempted violent breach or disablement of the vehicle barrier system (VBS) by overtly attempting to circumvent the barrier or by striking it violently, at a high rate of speed

The term "VBS" referred to in this regulatory position is the licensee's or certificate holder's engineered vehicle barrier system that is intended to stop vehicle-borne improvised explosive device (VBIED) attacks. The VBS is typically located at or beyond the exterior of the licensee's or certificate holder's protected area barrier. The VBS can consist of engineered security features or natural landform obstacles. The VBS uses these features to prevent vehicle progress and thus achieve a greater standoff distance between critical structures and personnel and the blast, shock, shrapnel, and impulse effects from the detonation of a VBIED. The NRC staff does not intend such reports under this regulatory position to include outer vehicle checkpoints located in the owner controlled area that are not part of the licensee's or certificate holder's VBS.

Licensees or certificate holders should evaluate an event that is not reportable under this requirement for reporting or recording under the other provisions of 10 CFR 73.71 and Appendix G.

2.2 Transportation Security Events To Be Reported within 15 Minutes

The regulations in 10 CFR 73.71(b) require each licensee or certificate holder subject to the provisions of 10 CFR 73.20, 10 CFR 73.25, 10 CFR 73.26, or 10 CFR 73.37 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 against shipments of Category I SSNM, SNF, and HLW. This rapid notification is intended to provide the NRC with an abbreviated set of facts that can be immediately

disseminated to other licensees, certificate holders, and government agencies, to enable them to rapidly increase their security posture.

These reports involve both the licensee's or certificate holder's discovery of an imminent or actual hostile action and the initiation of a security response in accordance with its safeguards contingency plan or protective strategy that is based upon an actual or imminent hostile action. Although the licensee's and certificate holder's plans and procedures typically describe many levels of security response, for the purposes of this reporting requirement, the security response means the substantive implementation (deployment) of armed response capabilities (i.e., a security contingency event response). The regulations do not require licensees and certificate holders to report security responses that are initiated as a result of a threat or warning information communicated to them by the NRC.

A licensee's or certificate holder's request for immediate LLEA assistance should take precedence over the notification to the NRC. Protecting public health and safety and the common defense and security should always be the licensee's and certificate holder's first priority.

Reports made under this provision are applicable only to ongoing security events, either actual or imminent. In the first circumstance, a licensee or certificate holder has been subject to a hostile action. A hostile action upon an applicable shipment or its accompanying personnel has either been committed or is in progress and includes use of violent force to steal the SSNM; destroy the transport vehicle or the SSNM, SNF, or HLW; take hostages; or intimidate the licensee or certificate holder. ~~Hostile actions include attacks by air, land, or water, using weapons, explosives, projectiles, vehicles, or other devices to deliver destructive force. In the second circumstance, an imminent hostile action is one for which the licensee or certificate holder has received information on the potential action and it fits the characteristics (of a hostile action) described in this paragraph.~~

Comment [z6]: This definition of hostile action does not match NRC or Industry accepted wording for this term.

The purpose of this notification is to allow the NRC to (1) warn other licensees and certificate holders and (2) notify other Federal agencies. Accordingly, the NRC has reduced the amount of information it should provide in the notification. Furthermore, the NRC may require the licensee or certificate holder to establish a continuous communications channel as soon as possible after making the 15-minute notification (see Regulatory Position 3.7 below). This flexibility is intended to relieve licensees and certificate holders of a communications burden while they immediately respond to the event, direct personnel, request LLEA assistance, and staff a trained individual in the communicator position (for the continuous communications channel).

The regulations permit licensees and certificate holders to directly report transportation events to the NRC themselves, or to use a contract service communications center to monitor and communicate with the shipment, contact LLEA if required, and report events to the NRC.

2.2.1 Notification Requirements

10 CFR 73.71(b) 15-minute notifications – shipments. Each licensee or certificate holder subject to the provisions of §§ 73.20, 73.25, 73.26, or 73.37 shall notify the NRC Headquarters Operations Center or make provisions to notify the NRC Headquarters Operations Center, as soon as possible but not later than 15 minutes after —

- (1) The discovery of an actual or attempted act of sabotage against shipments of spent nuclear fuel or high-level radioactive waste;*
- (2) The discovery of an actual or attempted act of sabotage or of theft against shipments of strategic special nuclear material; or*
- (3) The initiation of a security response in accordance with a licensee's or certificate holder's safeguards contingency plan or protective strategy, based on an imminent or actual*

hostile action against a shipment of spent nuclear fuel, high-level radioactive waste, or strategic special nuclear material.

(4) These notifications shall:

(i) Identify the name of the facility making the shipment, the material being shipped, and the last known location of the shipment; and

(ii) Briefly describe the nature of the threat or event, including:

(A) Type of threat or event (e.g., armed assault, vehicle bomb, theft of shipment, etc.);

and

(B) Threat or event status (i.e., imminent, in progress, or neutralized).

(5) Notifications must be made according to paragraph (j) of this section, as applicable.

(6) The licensee or certificate holder is not required to report security responses initiated as a result of threat or warning information communicated to the licensee or certificate holder by the NRC.

(7) A licensee's or certificate holder's request for immediate LLEA assistance can take precedence over the notification to the NRC.

2.2.2 Examples of Reportable Events

The NRC staff considers that the following transportation security events are examples of the types of events that require notification under 10 CFR 73.71(b).

- a. the licensee's or certificate holder's discovery of an imminent or actual hostile action against its shipment of Category I SSNM, SNF, or HLW
- b. the detonation of explosives or an explosive device at or near the licensee's or certificate holder's transport vehicle(s), including the use of explosives by ground assault force personnel and the use of land-based or waterborne VBIEDs
- c. weapons being fired at the licensee's or certificate holder's transport vehicle(s) and projectiles hitting the transport vehicle(s) that cause an immediate threat to the shipment, security personnel, or vehicle operators
- d. the successful, forcible penetration of a transport vehicle by unauthorized personnel
- e. the taking of hostages onsite (e.g., shipping facility, receiving facility, or communications center) or offsite, related to shipment operations or security
- f. the taking of hostages offsite that is reasonably determined to be related to shipment operations or security functions (e.g., the kidnapping of family members in order to coerce employees into violating laws, NRC regulations, or the shipping or receiving facility's license or certificate of compliance)
- g. actual or believed theft or sabotage of a shipment of Category I SSNM, SNF, or HLW
- h. the licensee's or certificate holder's notification by law enforcement authorities or another reliable source that an explosion or other assault against the shipment is imminent
- i. the licensee's or certificate holder's initiation of a security response in accordance with its safeguards contingency plan or protective strategy, based on an imminent or actual hostile action against its shipment of Category I SSNM, SNF, or HLW

Additionally, licensees or certificate holders should evaluate an event that is not reportable under this requirement for reporting or recording under the other provisions of 10 CFR 73.71 and Appendix G.

2.3 Facility Security Events To Be Reported within 1 Hour

The regulations in 10 CFR 73.71(c) require each licensee or certificate holder subject to the provisions of 10 CFR 73.20, 10 CFR 73.45, 10 CFR 73.46, 10 CFR 73.50, 10 CFR 73.51, 10 FR 73.54, 10 CFR 73.55, 10 CFR 73.60, or 10 CFR 73.67 to notify the NRC Headquarters Operations Center as soon as possible but not later than 1 hour after the discovery of significant facility-security events specified in paragraph I of Appendix G to Part 73. This regulation applies to Category I SSNM facilities, hot-cell facilities, ISFSIs, MRSs, GROAs, power reactor facilities, research reactor facilities, test reactor facilities, and Category II and Category III SNM facilities.

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 nonsafety-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 personnel or contraband.

The NRC staff considers contraband to be unauthorized weapons, explosives, or incendiaries. Licensees and certificate holders may also identify "prohibited items" under their facility procedures. The staff considers contraband items and prohibited items as separate categories. Licensees and certificate holders are not required under these regulations to report attempted or actual introduction events involving prohibited items. In addition, items that are possessed by authorized persons for authorized purposes inside of the facility should not be considered contraband. For example, weapons possessed by the facility's security personnel as part of their official duties, weapons possessed by sworn law enforcement personnel visiting the facility, squib valves used in certain types of reactors, or explosives intended for authorized and controlled demolition or construction activities at the facility should not be considered contraband.

Reports made under this provision also apply to power reactor facilities that fall within the scope of 10 CFR 73.54 regarding the discovery that a cyber attack has occurred or has been attempted against systems, networks, or equipment that would compromise or has compromised the facility's safety, security, and emergency preparedness (SSEP) functions. These affected systems, networks, or equipment would be equal to or greater than a Level 3 or Level 4 network, as described in RG 5.71, "Cyber Security Program for Nuclear Facilities," (Ref. 7).

Reporting requirements include security events or information not otherwise reported as 15-minute notifications under 10 CFR 73.71(a) (i.e., an actual and substantial armed response to an imminent or actual hostile act) but that provide reason to believe that a person has caused or attempted to cause an event or has threatened to cause the types of events outlined in paragraph I of Appendix G. In terms of the 1-hour reporting requirement, "reason to believe" should be supported by reliable and substantive information that includes physical evidence supporting the threat; additional information independent of the threat; or the identification of a specific, known group, organization, or individual that claims responsibility for the threat. As used in Appendix G, "attempts" is defined in the glossary as reliable and substantive information that an effort was made to accomplish the threat, even though it has not occurred or has not been completed because it was interrupted or stopped before completion. These

reports include security events that are not imminent in nature and that may not necessarily result in the deployment of the security force or a contingency response. These events may result in a commitment of staff to search a facility at the request and with the assistance of law enforcement authorities.

Licensees and certificate holders should also report the interruption of normal operations resulting from intentional tampering or unauthorized use or manipulation of equipment or components. This could include intentional tampering with a system or equipment that is normally in a standby condition but would need to operate if called upon by personnel or automatic start signals. Licensees and certificate holders should initiate an appropriate preliminary evaluation of potential or actual interruptions of operations to determine whether the causes are human error, mechanical failure, or intentional acts. This evaluation should include reasonable actions or information collected within 1 hour of discovery of the event. Should a licensee or certificate holder initially determine that the collected information does not represent an actual or attempted threat and later changes its determination, it should notify the NRC of its change in determination.

Licensees or certificate holders may need to record other failures, degradations, or discovered vulnerabilities of security systems not related to unauthorized or undetected access, as described in paragraph IV of Appendix G.

Regulatory Position 3 provides guidance to the licensee or certificate holder if the Headquarters Operations Center requests a continuous communications channel or if followup notifications are needed.

2.3.1 Notification Requirements

10 CFR 73.71(c) One-hour notifications – facilities. (1) Each licensee or certificate holder 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 within one hour after discovery of the facility safeguards events described in paragraph I of Appendix G to this part.

(2) Notifications must be made according to paragraph (j) of this section, as applicable.

(3) Notifications made under paragraph (a) of this section are not required to be repeated under this paragraph.

Appendix G to Part 73, Paragraph I. Events to be reported within one hour of discovery.

(a) Significant security events. Any event in which there is reason to believe that a person has committed or caused, or attempted to commit or cause, or has made a threat to commit or cause:

(1) A theft or diversion of special nuclear material;

(2) Significant physical damage to any nuclear reactor or facility possessing or using Category I strategic special nuclear material;

(3) Significant physical damage to any vehicle transporting special nuclear material, spent nuclear fuel, or high-level radioactive waste; or to the special nuclear material, spent nuclear fuel, or high-level radioactive waste itself;

(4) The unauthorized operation, manipulation, or tampering with any nuclear reactor's controls or with structures, systems, and components (SSCs) that results in the interruption of normal operation of the reactor; or

(5) The unauthorized operation, manipulation, or tampering with any Category I strategic special nuclear material (SSNM) facility's controls or SSCs that results in the interruption of normal operation of the facility.

(b) Unauthorized entry events.

(1) An actual entry of an unauthorized person into a facility's protected area (PA), vital area (VA), material access area (MAA), or controlled access area (CAA).

(2) An actual entry of an unauthorized person into a transport vehicle.

(3) *An attempted entry of an unauthorized person with malevolent intent into a PA, VA, MAA, or CAA.*

(4) *An attempted entry of an unauthorized person with malevolent intent into a vehicle transporting special nuclear material, spent nuclear fuel, or high-level radioactive waste; or to the special nuclear material, spent nuclear fuel, or high-level radioactive waste itself.*

(c) *Contraband events.*

(1) *The actual introduction of contraband into a PA, VA, MAA, or CAA.*

(2) *The actual introduction of contraband into a transport.*

(3) *An attempted introduction of contraband by a person with malevolent intent into a PA, VA, MAA, or CAA.*

(4) *An attempted introduction of contraband by a person with malevolent intent into a vehicle transporting special nuclear material, spent nuclear fuel, or high-level radioactive waste; or to the special nuclear material, spent nuclear fuel, or high-level radioactive waste itself.*

(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.*

(2) *Uncontrolled authorized weapons means weapons that are authorized by the licensee's or certificate holder's security plan and are not in the possession of authorized personnel or are not in an authorized weapons storage location.*

(e) *Vehicle barrier system events. For licensees and certificate holders with a vehicle barrier system protecting their facility, the actual or attempted introduction of explosives or incendiaries beyond the vehicle barrier.*

(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;*

(2) *Personnel or contraband into a PA, VA, MAA, or CAA; or*

(3) *Personnel or contraband into a vehicle transporting special nuclear material, spent nuclear fuel, or high-level radioactive waste; or to the special nuclear material, spent nuclear fuel, or high-level radioactive waste itself.*

(g) *Lost shipments of nuclear or radioactive material.*

(1) *The discovery of the loss of a shipment of Category I SSNM, Category II and III special nuclear material, spent nuclear fuel, or high-level radioactive waste.*

(2) *The recovery of or accounting for a lost shipment.*

(h) *Cyber security events.*

(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 threat to commit or cause, an act to modify, destroy, or compromise any systems, networks, or equipment that falls within the scope of, '+' 73.54 of this part.*

(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.*

(i) *[Reserved]*

(j) *Loss or theft of classified information. The discovery of the loss or theft of classified material (e.g., documents, drawings, analyses, or data) that contains either National Security Information or Restricted Data.*

(k) *Loss or theft of Safeguards Information. The discovery of the 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 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.

2.3.2 Examples of Reportable Events

The NRC staff considers that the following facility-security events as examples of the types of events that require notification under 10 CFR 73.71(c) and paragraph I of Appendix G.

- a. the successful, surreptitious penetration of a PA, VA, MAA, or CAA by unauthorized personnel
- b. an actual entry (i.e., the unauthorized penetration or the actual circumvention of security control measures) by a person who is not authorized access to the specific area in question
 - (1) 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 the failure of the security control to prevent the access of the person.
 - (3) If licensees or certificate holders conclude that the entry of the individual was inadvertent and did not threaten facility security, they may record this event in the safeguards event log. However, if it represents a vulnerability or an uncompensated degradation in a security system that could allow intentional undetected or unauthorized access, the licensee should make a 1-hour notification.
- c. 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
- d. an unauthorized entry attempt that was thwarted by responders or other security-system elements
- e. absent other suspicious information licensees and certificate holders should not report personnel who attempt to enter or actually enter a controlled area by tailgating into areas where they are not authorized entry but could have been authorized, if necessary, and their entry is not considered a threat to the facility
- f. the unauthorized entry of dismounted personnel onto or beyond the owner-controlled area (OCA) vehicle barrier system, reportable only when the actual or attempted entry threatens facility security; if there is an actual or attempted introduction of explosives or incendiaries beyond vehicle barriers, which are not designed to address dismounted individuals; or when the licensee or certificate holder identifies the entry as a threat
- g. absent other suspicious information, licensees and certificate holders should not report hunters who inadvertently enter on to OCA as a 1-hour report, but should evaluate whether the event is appropriate for a 4-hour suspicious activity report
- h. the actual or attempted introduction of contraband material (e.g., unauthorized weapons, explosives, or incendiaries)

- (1) Licensees and certificate holders should conduct an appropriate evaluation within the reporting time to determine whether the actual or attempted introduction of contraband into a controlled area occurred.
 - (2) If the licensee or certificate holder concludes, within an hour, that the entry of the contraband was inadvertent and did not threaten facility security, they 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, the NRC requires a 1-hour report.
 - (3) An actual or attempted introduction of contraband into the OCA is reportable when the contraband has been determined to represent a threat capable of reducing the effectiveness of the physical security plan (e.g., firearms are discovered and the licensee or certificate holder determines they represent a threat to the facility). This example does not impose additional search requirements but addresses contraband that may be found pursuant to other activities.
- i. the actual or attempted introduction of explosives or incendiaries beyond any vehicle barriers
 - j. a vehicle that strikes or challenges a component of the vehicle barrier system (VBS) in a manner that is more than a minor accident (i.e., the accident degrades the ability of the VBS to perform its intended functions)
 - k. uncompensated failures and degradations or discovered vulnerabilities of security systems that could allow unauthorized or undetected access to PAs, VAs, MAAs, or CAAs.
- (l) Uncompensated means compensatory measures were included in applicable security plans or procedures that have not been implemented, were implemented incorrectly, or were ineffective. To clarify, for the uncompensated failures just discussed, licensees and certificate holders should report mechanical or electrical problems and failures or inadequacies in procedure implementation and personnel practices or performance.
- l. the loss of intrusion detection and assessment capability that is not compensated in accordance with the facility's NRC-approved security plan
 - m. the loss of an alarm capability or locking mechanism at a material access portal that is not compensated in accordance with the facility's NRC-approved security plan
 - n. 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 to a PA, VA, MAA, or CAA
 - o. an uncompensated design flaw or vulnerability in a physical protection system that could have allowed unauthorized access to a PA, VA, MAA, or CAA or could have substantively eliminated or significantly reduced the licensee's or certificate holder's response capabilities
 - p. the uncompensated failure of all protected area lighting, when combined with any uncompensated outage of a PA perimeter intrusion detection, assessment, or delay systems
 - q. security events that could allow undetected or unauthorized access within 1 hour, usually affecting multiple layers of physical security systems or an individual, critical, single failure of a program element that would allow undetected or unauthorized access, or other failures,

degradations, or discovered vulnerabilities of security systems not relating to unauthorized or undetected access that may need to be recorded as described in paragraph IV of Appendix G

r. security events that involve an interruption of the normal operation of the licensee's or certificate holder's facility through the unauthorized use of, or tampering with, its components, controls, or security systems, as described below:

- (1) Tampering with plant equipment or physical security equipment that is confirmed to be suspicious, destructive, or malevolent; is not a reasonable mechanical failure; or is related to willful human error is reportable. Licensees and certificate holders should report, within 1 hour, tampering that results in an interruption of the normal operations of the facility. 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.
- (2) Confirmed cyber attacks on computer systems that may adversely affect safety, security, and emergency preparedness systems are reportable.
- (3) An actual or imminent strike (labor work slowdown or stoppage) by the security force is reportable.
- (4) A mass demonstration at or near the facility is reportable if the protesters do not have a demonstration permit from the appropriate local authorities or the demonstration is not overseen by LLEA personnel. The NRC staff considers a mass demonstration to consist of five or more individuals. A demonstration of less than five individuals for which the licensee or certificate holder has requested LLEA assistance would be reportable as a 4-hour notification under Regulatory Position 2.5 below.
- (5) A mass demonstration at or near the facility with the appropriate demonstration permits and LLEA oversight presence is reportable if LLEA personnel loses control of the demonstration and demonstrators enter the facility's property.
- (6) Bomb or extortion threats are reportable if the licensee or certificate holder 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.
- (7) The loss of all offsite communications capabilities is reportable if they are required to meet regulatory requirements (i.e., specified in the licensee's or certificate holder's security or emergency plans).
- (8) The loss or theft of a standard weapon from inside of the licensee's or certificate holder's PA, VA, MAA, or CAA. Reporting of the loss or theft of an enhanced weapon is discussed in Regulatory Position 2.7 below.

Comment [z7]: Condition 7 is classifiable under 10CRR50.47 and NEI 99-01, NESP-007 and NUREG 0654 EALs. As classified events are covered under reporting criteria established in 10 CFR 50.72, it seems the condition should not be listed here.

s. the discovery of a criminal act involving individuals granted unescorted access that could provide an opportunity to adversely affect facility safety or that represents a threat (e.g., crimes such as sabotage, arson, bombing, tampering with nuclear facilities, murder, being a member of a terrorist organization, or battery against plant staff; crimes involving nonviolent activities, such as espionage, drug trafficking, counterfeiting, conspiracy to commit a serious crime)

- t. the discovery of falsified identification badges, key cards, or other access-control devices that could allow unauthorized individuals access to controlled areas
- u. 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 actual or attempted use of the equipment or media where an unauthorized individual could or did gain entry into a controlled area
- v. the uncompensated loss of all alternating current (ac) power to security systems that could allow unauthorized or undetected access to a PA, VA, MAA, or CAA
- w. 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)
- x. the discovery of lost or stolen classified documents containing either national security information or restricted data.
- y. the discovery of lost or stolen Safeguards Information that would substantially assist an adversary in the circumvention of security systems or the loss of Safeguards Information in a manner that could allow a significant opportunity for the Safeguards Information to be compromised, where “substantially” refers to the characteristics and essential parts of the information (i.e., its composition or content) and “significant” refers to the importance or meaning of the information (i.e., its value)
- z. the unavailability of the minimum number of on duty security personnel in a shift after implementation of the appropriate recall procedures
- aa. the successful, surreptitious penetration or compromise of a critical digital asset (CDA) by unauthorized personnel
- bb. an actual penetration or compromise of a CDA, where a person who is not authorized access circumvented 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 security program or security measures.
 - (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, 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.
 - (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 possible, or (2) the cyber attack was not successful because it was interrupted or stopped before completion.

- (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.
- cc. the discovery of malware, unauthorized software, or firmware installed on a CDA
- dd. failures, degradations, or discovered vulnerabilities of CDAs or security measures that protect CDAs that would be likely to allow unauthorized or undetected access to those CDAs or that could result in compromising the CDA or an SSEP function when compensatory measures have not been employed (i.e., uncompensated)
- ee. the theft of sensitive cyber security data
- ff. the loss of cyber intrusion detection 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
- hh. an uncompensated design flaw or vulnerability in a cyber protection system that could have allowed unauthorized access to CDAs or could have substantively eliminated or significantly reduced the licensee's response capabilities
- 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
- jj. the discovery of falsified identification badges, key cards, or other access-control devices that could allow unauthorized individuals access to CDAs
- 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 or did gain entry to a CDA
- ll. the uncompensated loss of all ac power to security systems that could allow unauthorized or undetected access to a CDA
- mm. the discovery of lost or stolen Safeguards Information that would substantially assist an adversary in the circumvention of cyber security systems or the loss of Safeguards Information in a manner that could allow a significant opportunity for a CDA to be compromised, where "substantially" refers to the characteristics and essential parts of the information (i.e., its composition or content) and "significant" refers to the importance or meaning of the information (i.e., its value).
- nn. the unavailability of the minimum number of cyber security response personnel after implementation of the appropriate recall procedures
- oo. uncompensated failures, degradations, or discovered vulnerabilities with a CDA, personnel responses, communications, monitoring, or oversight that could increase the likelihood of an attempted attack on any CDA

Additionally, licensees or certificate holders should evaluate an event that is not reportable under this requirement for reporting or recording under the other provisions of 10 CFR 73.71 or Appendix G.

2.4 Transportation Security Events To Be Reported within 1 Hour

The regulations in 10 CFR 73.71(d) require each licensee or certificate holder subject to the provisions of 10 CFR 73.25, 10 CFR 73.26, 10 CFR 73.27, 10 CFR 73.37, or 10 CFR 73.67 to notify the NRC Headquarters Operations Center as soon as possible but not later than 1 hour after the discovery of significant transportation-security events specified in paragraph I of Appendix G. This regulation applies to licensees and certificate holders shipping Category I SSNM, Category II and III SNM, SNF, and HLW. These shipments may be made under any mode (including highway, rail, airborne, or water) by the licensee or certificate holder (i.e., private carriage) or by a transportation company under contract to the licensee or certificate holder (i.e., public carriage).

Licensees and certificate holders shipping materials by a U.S. Department of Energy (DOE) transportation system (e.g., the DOE Office of Secure Transportation) remain subject to the security event reporting and recording requirements of 10 CFR 73.71 and Appendix G. The NRC staff notes that, although licensees and certificate holders shipping materials are exempt under 10 CFR 73.6(d) from the applicable physical security requirements of 10 CFR Part 73, 10 CFR 73.6, "Exemptions for Certain Quantities and Kinds of Special Nuclear Material," does not exempt them from the security event reporting and recording requirements of 10 CFR 73.71 and Appendix G.

Generally, these events relate to committed or attempted acts and credible threats involving the theft or diversion of SSNM or SNM; significant physical damage to any vehicle transporting SNM, SNF, or HLW; significant physical damage to the SNM, SNF, or HLW itself; actual entry of an unauthorized person into a transport vehicle; attempted entry of an unauthorized person with malevolent intent into a vehicle transporting SNM, SNF, or HLW or into the SNM, SNF, or HLW itself; actual entry of contraband into a transport vehicle; and attempted introduction of contraband with malevolent intent into a vehicle transporting SNM, SNF, or HLW or into the SNM, SNF, or HLW itself.

Reporting requirements under this provision include security events or information not otherwise reported as 15-minute notifications under 10 CFR 73.71(b) (i.e., events requiring an actual and substantial armed response to an imminent or actual hostile act) but that provide reason to believe that a person has caused or attempted to cause an event or has threatened to cause the types of events outlined in paragraph I of Appendix G. In terms of the 1-hour reporting requirement, "reason to believe" should be supported by reliable and substantive information that includes physical evidence supporting the threat; additional information independent of the threat; or the identification of a specific, known group, organization, or individual that claims responsibility for the threat. As used in Appendix G, "attempts" is defined in the glossary to mean that reliable and substantive information exists regarding an effort to accomplish the threat, even though it has not occurred or has not been completed because it was interrupted or stopped before completion. These reports include security events that are not imminent in nature and that may not necessarily result in a substantive armed response or deployment of the security force or a contingency response. These events may result in a commitment of staff to search a transport vehicle at the request and with the assistance of law enforcement authorities.

The regulations permit licensees and certificate holders to directly report transportation events to the NRC themselves, or to use a contract service communications center to monitor and communicate with the shipment, contact LLEA if required, and report events to the NRC.

Regulatory Position 3 provides guidance to the licensee or certificate holder if the Headquarters Operations Center requests a continuous communications channel or if followup notifications are needed.

2.4.1 Notification Requirements

10 CFR 73.71(d) *One-hour notifications - shipments.* (1) Each licensee or certificate holder subject to the provisions of §§ 73.25, 73.26, 73.27, 73.37, and 73.67 shall notify the NRC Headquarters Operations Center within one hour after discovery of the transportation safeguards events described in paragraph I of Appendix G to this part.

(2) Notifications must be made according to paragraph (j) of this section, as applicable.

(3) Notifications made under paragraph (b) of this section are not required to be repeated under this paragraph.

Appendix G to Part 73, Paragraph I. Events to be reported within one hour of discovery.

(a) *Significant security events.* Any event in which there is reason to believe that a person has committed or caused, or attempted to commit or cause, or has made a threat to commit or cause:

(1) A theft or diversion of special nuclear material;

(2) Significant physical damage to any nuclear reactor or facility possessing or using Category I strategic special nuclear material;

(3) Significant physical damage to any vehicle transporting special nuclear material, spent nuclear fuel, or high-level radioactive waste; or to the special nuclear material, spent nuclear fuel, or high-level radioactive waste itself;

(4) The unauthorized operation, manipulation, or tampering with any nuclear reactor's controls or with structures, systems, and components (SSCs) that results in the interruption of normal operation of the reactor; or

(5) The unauthorized operation, manipulation, or tampering with any Category I strategic special nuclear material (SSNM) facility's controls or SSCs that results in the interruption of normal operation of the facility.

(b) *Unauthorized entry events.*

(1) An actual entry of an unauthorized person into a facility's protected area (PA), vital area (VA), material access area (MAA), or controlled access area (CAA).

(2) An actual entry of an unauthorized person into a transport vehicle.

(3) An attempted entry of an unauthorized person with malevolent intent into a PA, VA, MAA, or CAA.

(4) An attempted entry of an unauthorized person with malevolent intent into a vehicle transporting special nuclear material, spent nuclear fuel, or high-level radioactive waste; or to the special nuclear material, spent nuclear fuel, or high-level radioactive waste itself.

(c) *Contraband events.*

(1) The actual introduction of contraband into a PA, VA, MAA, or CAA.

(2) The actual introduction of contraband into a transport.

(3) An attempted introduction of contraband by a person with malevolent intent into a PA, VA, MAA, or CAA.

(4) An attempted introduction of contraband by a person with malevolent intent into a vehicle transporting special nuclear material, spent nuclear fuel, or high-level radioactive waste; or to the special nuclear material, spent nuclear fuel, or high-level radioactive waste itself.

(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.

(2) Uncontrolled authorized weapons means weapons that are authorized by the licensee's or certificate holder's security plan and are not in the possession of authorized personnel or are not in an authorized weapons storage location.

(e) *Vehicle barrier system events.* For licensees and certificate holders with a vehicle barrier system protecting their facility, the actual or attempted introduction of explosives or incendiaries beyond the vehicle barrier.

(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;*
- (2) Personnel or contraband into a PA, VA, MAA, or CAA; or*
- (3) Personnel or contraband into a vehicle transporting special nuclear material, spent nuclear fuel, or high-level radioactive waste; or to the special nuclear material, spent nuclear fuel, or high-level radioactive waste itself.*

(g) Lost shipments of nuclear or radioactive material.

(1) The discovery of the loss of a shipment of Category I SSNM, Category II and III special nuclear material, spent nuclear fuel, or high-level radioactive waste.

(2) The recovery of or accounting for a lost shipment.

(h) Cyber security events.

(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 threat to commit or cause, an act to modify, destroy, or compromise any systems, networks, or equipment that falls within the scope of, + ' 73.54 of this part.

(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.

(i) [Reserved]

(j) Loss or theft of classified information. The discovery of the loss or theft of classified material (e.g., documents, drawings, analyses, or data) that contains either National Security Information or Restricted Data.

(k) Loss or theft of Safeguards Information. The discovery of the 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 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.

2.4.2 Examples of Reportable Events

The NRC staff considers that the following transportation-security events as examples of the types of events that require notification under the requirements of 10 CFR 73.71(d) and paragraph I of Appendix G.

- a. the successful, surreptitious penetration of a transport vehicle by unauthorized personnel
- b. a shipment of Category I SSNM, Category II or III SNM, SNF, or HLW that is believed to be lost
- c. recovery of a lost Category I SSNM, Category II or III SNM, SNF, or HLW shipment
- d. notification of law enforcement authorities subsequent to the discovery of a suspicious vehicle following a licensed carrier transporting Category I SSNM, Category II or III SNM, SNF, or HLW
- e. the discovery of an attempted theft of a shipment of Category I SSNM, Category II or III SNM, SNF, or HLW

- f. the actual or attempted introduction of contraband material (e.g., unauthorized weapons, explosives, or incendiaries) into the transport vehicle that is transporting the Category I SSNM, Category II or III SNM, SNF, or HLW or into the nuclear or radioactive material itself
- g. uncompensated failures, degradations, or discovered vulnerabilities with a transportation system's security hardware, equipment, and personnel responses, communications, monitoring, or oversight that could increase the likelihood of an attempted theft of a shipment of Category I SSNM, Category II or III SNM, SNF, or HLW.

Additionally, licensees and certificate holders should evaluate an event that is not reportable under this requirement for reporting or recording under the other provisions of 10 CFR 73.71 or Appendix G.

2.5 Facility Security Events To Be Reported within 4 Hours

The regulations in 10 CFR 73.71(e) require each licensee or certificate holder subject to the provisions of 10 CFR 73.20, 10 CFR 73.45, 10 CFR 73.46, 10 CFR 73.50, 10 CFR 73.51, 10 CFR 73.54, 10 CFR 73.55, 10 CFR 73.60, or 10 CFR 73.67 to notify the NRC Headquarters Operations Center as soon as possible but not later than 4 hours after the discovery of facility-security events specified in paragraph II of Appendix G. This regulation applies to Category I SSNM facilities, hot-cell facilities, ISFSIs, MRSS, GROAs, power reactor facilities, research reactor facilities, test reactor facilities, and Category II and III SNM facilities.

Four-hour notifications fall within three categories—suspicious activities; unauthorized operation, manipulation, or tampering events that do not result in the interruption of facility operations, but could prevent the implementation of the protective strategy for protecting any target set; and notifications to and responses from LLEAs.

The reporting of suspicious activities is an important component of evaluating the threat against licensed facilities and material. The NRC reviews individual notifications of suspicious activities to evaluate whether potential preoperational activities (i.e., multiple events at a single site or multiple events at multiple sites) may be part of a larger plan and to integrate this information with other agencies in the homeland security and intelligence communities. The NRC is not requesting that the licensees and certificate holders actively gather intelligence, but rather that they report information they believe is relevant to the security of their facility or activity. The NRC staff has added examples of suspicious events that should be reported to the NRC. The U.S. government considers suspicious activity as “observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.” Additionally, licensees and certificate holders are considered “key resource owners and operators” and can find additional guidance on examples of suspicious events in the U.S. Department of Homeland Security’s, “Terrorist Threats to the U.S. Homeland: Reporting Guide for Critical Infrastructure and Key Resource Owners and Operators,” (Ref. 8). This reporting guide is designated as “Unclassified and For Official Use Only.”

Licensees or certificate holders should not report events based solely on speculation. They should report events that are believed to be real, including those substantiated by observations by licensee or certificate holder staff or local law enforcement personnel, evidence of the presence of unknown personnel, telephone contacts, suspicious documents, and testimony of credible witnesses. Licensees’ and certificate holders’ corporate and contractor personnel may also be sources of this information. Licensees and certificate holders can obtain additional information from the NRC, about terrorist activities or suspicious events they may encounter during the course of normal activities, on NRC’s protected Web server under Event No. 2464.

The NRC staff recommends that licensees and certificate holders contact organizations in their local area (i.e., military, government, law enforcement, and private sector) that could conduct aircraft operations in airspace over or near their facilities. Licensees and certificate holders should identify respective points of contact with these organizations in order to coordinate advance notification of upcoming activities and to verify any ongoing suspicious aircraft activity that was not previously coordinated.

The unauthorized operation, manipulation, or tampering events reported under this notification includes events that fall outside the 1-hour notification requirements (i.e., the event did not result in the interruption of facility operations) but that could prevent the implementation of the licensee's or certificate holder's protective strategy for the facility.

The NRC requires 4-hour notifications from licensees and certificate holders subject to 10 CFR 73.54, if they discover information that indicates that tampering; unauthorized access, use or modifications; or unauthorized gathering of information or data on systems has occurred or is occurring on networks or equipment within the scope of 10 CFR 73.54 or if the security measures that protect these SSEP functions are degraded.

The NRC's purpose in gathering notifications of communications to or from local law enforcement authorities is to enable the NRC to respond to any potential public and media inquiries resulting from licensee, certificate holder, or LLEA actions at NRC-regulated facilities. This objective is similar to other 4-hour safety-related notifications regarding press releases and contact with other agencies that are found elsewhere in the NRC's regulations.

2.5.1 Notification Requirements

10 CFR 73.71(e) Four-hour notifications – facilities. (1) 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 four hours after discovery of the safeguards events described in paragraph II of Appendix G to this part.

(2) Notifications must be made according to paragraph (j) of this section, as applicable.

Appendix G, Paragraph II. Events to be reported within four hours of discovery.

(a) Suspicious events. Any information received by the licensee of suspicious or surveillance activities or attempts at access, including:

(1) Any event or incident involving suspicious activity that may be indicative of potential pre-operational surveillance, reconnaissance, or intelligence-gathering activities directed against the facility. This type of activity may include, but is not limited to—

(A) Attempted surveillance or reconnaissance activity. Commercial or military aircraft activity considered routine or non-threatening by the licensee or certificate holder is not required to be reported;

(B) Elicitation of information from facility personnel relating to the security or safe operation of the facility; or

(C) Challenges to security systems (e.g., willful failure to stop for security checkpoints, possible tests of security response and security screening equipment, or suspicious entry of watercraft into posted off-limits areas).

(2) Any event or incident involving suspicious aircraft activity over or in close proximity to the facility. Commercial or military aircraft activity considered routine or non-threatening by the licensee or certificate holder is not required to be reported.

(b) Unauthorized operation or tampering events. An event involving—

The unauthorized operation, manipulation, or tampering of any nuclear reactor's or Category I SSNM facility's SSCs that could prevent the implementation of the licensee's or certificate holder's defensive strategy for protecting any target set.

(c) Suspicious cyber security events.

(1) Any information received or collected by the licensee or certificate holder of suspicious activity that may be indicative of tampering, malicious or unauthorized access, use, operation, manipulation, modification, potential destruction, or compromise 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.

(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.

(d) Law enforcement interactions. (1) An event related to the licensee's or certificate holder's implementation of their security program for which a notification was made to local, State, or Federal law enforcement officials and that does not otherwise require a notification under paragraph I or the other provisions of paragraph II of this appendix.

(2) An event 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.

2.5.2 Examples of Reportable Events

The NRC staff considers that the following security events as examples of the types of events that require notification under 10 CFR 73.71(e) and paragraph II of Appendix G.

The following are examples of security-related events involving suspicious activity that may indicate preoperational surveillance, reconnaissance, or intelligence-gathering activities directed against licensees, certificate holders, or their facilities:

- a. individual(s) with non-routine interests or inquiries related to security measures, personnel or vehicle entry points and access controls, or vehicle barrier systems, including fences, walls, or other barriers
- b. individual(s) conducting unapproved photographing or videotaping of licensed facilities on owner controlled property
- c. individual(s) conducting unapproved photographing or videotaping of licensed facilities from public property or non-owner controlled property when combined with other suspicious information gathered by security personnel challenges to, or interviews of, the individuals
- d. suspicious attempts to recruit or compromise employees or staff, including contractors, knowledgeable of key personnel, facilities, or systems, into providing classified information, Safeguards, information, or other sensitive physical security or cyber security information
- e. loitering for no apparent purpose in areas where intelligence could be gathered or where preoperational reconnaissance could be performed
- f. suspicious behavior (e.g., fleeing, moving quickly away from licensee or certificate holder personnel, unexpected vehicular movement)
- g. secretive sketching, making maps, or taking notes on the owner controlled area

- h. eliciting information from security or other site personnel regarding security systems or vulnerabilities
- i. unusual challenges to security systems that could represent attempts to gather information on system performance or personnel or equipment response actions
- j. unauthorized attempts to probe or gain access to the licensee's or certificate holder's business secrets or other sensitive information or to control systems, including the use of social engineering techniques (e.g., impersonating authorized users)
- k. theft or suspicious loss of official company identification documents, uniforms, or vehicles necessary for accessing plant facilities
- l. use of forged, stolen, or fabricated documents to support access control or authorization activities
- m. boating activities conducted in unauthorized locations or attempts to loiter near facility restricted areas
- n. unusual attempts to obtain information or documents related to site security training, techniques, procedures, or practices
- o. discovery of Internet site postings that make violent threats related to specific licensed facilities or activities
- p. unusual threats or terrorist-related activities that become known to facility security or management involving the following: (1) unusual surveillance, probing or reconnaissance, (2) attempts to gain unauthorized access, (3) attempts to gain access to or acquire hazardous or dangerous materials, (4) unusual use of materials, or (5) financing to support terrorist activities
- q. stated threat(s) against the licensee's or certificate holder's facility or staff, unless they are determined to be unsubstantiated
- 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)
- 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

The following are examples of aircraft overflight activities that do not represent an immediate threat to the facility but may be indicative of preoperational surveillance, reconnaissance, or intelligence-gathering activities directed against licensees, certificate holders, or their facilities:

- 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 precoordination efforts to reduce false positive (unnecessary) reports.

- u. Licensees and certificate holders should exercise judgment and discretion in determining whether flight activity is suspicious with respect to normal air traffic patterns in their locality. Factors that may be considered in evaluating normal air traffic patterns include proximity of the facility to local public, private, and commercial airports; U.S. military bases; the use of rivers, coastal waterways, and prominent landmarks (e.g., cooling towers) for navigational purposes; local weather conditions; and other local circumstances.
- v. Licensees and certificate holders are not required to notify the NRC of coordinated aircraft operations in airspace over or near their facilities.
- w. Licensees and certificate holders are not required to notify the NRC of military, government, and law enforcement aircraft operations in the airspace over or near their facilities that were not previously coordinated, provided the licensee or certificate holder communicates with the preestablished point of contact and verifies that the aircraft operations were, in fact, planned but not previously coordinated with the licensee or certificate holder.

The following are examples of events involving the notification or unanticipated response of local, State, or Federal law enforcement agencies that do not involve the licensee's or certificate holder's implementation of its contingency response plan or protective strategy:

- x. Licensees and certificate holders should notify the NRC of law enforcement personnel onsite to arrest a felon or fugitive from justice or to execute a search warrant.
- y. Licensees and certificate holders should notify the NRC of law enforcement personnel's pursuit of subjects into the facility's OCA.
- z. Licensees and certificate holders should notify the NRC of requests for law enforcement response to the facility because a crime may have been committed (e.g., assault and battery or discovery of controlled substances or unauthorized weapons).
- aa. Licensees and certificate holders are not required to notify the NRC of law enforcement personnel onsite for nonresponse duties, training exercises, familiarization and coordination activities, other scheduled activities, or the sharing of information.

The following are examples of unauthorized use or tampering with components or controls, including the security system, that do not interrupt the normal operation of the plant but could prevent the implementation of the licensee's or certificate holder's protective strategy for protecting any target set. Licensees or certificate holders should report the act of tampering, rather than the effects of the tampering, because it is not known whether the tampering could create potentially significant equipment issues.

- bb. the unauthorized operation, manipulation, or tampering with a nuclear reactor's controls, safety-related SSCs, or nonsafety-related SSCs that do not interrupt the normal operations of the reactor
- cc. the unauthorized operation, manipulation, or tampering with a Category I SSNM facility's controls, safety-related SSCs, or nonsafety-related SSCs that do not interrupt the normal operations of the facility
- dd. the unauthorized operation, manipulation, or tampering with security-related SSCs that could prevent the implementation of the licensee's or certificate holder's protective strategy for protecting the SSCs in a target set

- ee. the intentional cutting of wires that does not affect the facility or security operations
- ff. the overt changing of equipment or controls to settings that do not affect their intended function
- gg. the tampering with, or the destruction of, equipment that does not affect plant operations (e.g., water coolers, office equipment, maintenance tools)
- hh. the modification of security equipment that renders the equipment inoperable
- ii. the lost or theft of standard security weapons from a location outside of the licensee's or certificate holder's PA or CAA, provided the weapon could affect the implementation of the licensee's or certificate holder's protective strategy (e.g., high-power weapons or long weapons); otherwise the event should be recorded in the Safeguards Event Log
- jj. the loss or theft of enhanced security weapons from a location outside of the licensee's or certificate holder's PA or CAA is discussed in Regulatory Position 2.7

The following are examples of surveillance or reconnaissance of cyber systems; of tampering, malicious or unauthorized access, use, operation, manipulation, modification, potential destruction, or compromise of the systems, networks, and equipment that fall within the scope of 10 CFR 73.54; or of the security measures that could weaken or disable the protection for such systems, networks, or equipment:

- kk. the discovery of individuals with uncommon interests or inquiries related to the facility's cyber security measures, personnel, or security controls
- ll. the discovery of unauthorized personnel at or near the plant performing wireless reconnaissance of the licensee's wireless networks and communications systems
- mm. 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
- nn. the discovery of the theft or suspicious loss of smart cards, tokens, or other "two factor" authentication systems necessary for accessing CDAs
- oo. 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 CDAs or authorization activities
- pp. 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)
- qq. the discovery of an active attack, virus, or worm on an network adjacent to CDAs that, if security barriers were not in place, could adversely affect CDAs or SSEP functions
- rr. Information that a compromise of cyber systems 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)

- ss. the discovery of the degradation or failure of a CDA that is of suspicious or unknown origin that has not been reported under the 15-minute or 1-hour notification requirements and does not have an immediate or significant impact on SSEP functions or the normal operation of the facility

Additionally, licensees and certificate holders should evaluate an event that is not reportable under this requirement for reporting or recording under the other provisions of 10 CFR 73.71 or Appendix G.

2.6 Facility-Security Events To Be Reported within 8 Hours

The regulations in 10 CFR 73.71(f) require each licensee or certificate holder subject to the provisions of 10 CFR 73.20, 10 CFR 73.45, 10 CFR 73.46, 10 CFR 73.50, 10 CFR 73.51, 10 CFR 73.55, 10 CFR 73.60, or 10 CFR 73.67 to notify the NRC Headquarters Operations Center as soon as possible but not later than 8 hours after the discovery of facility-security events specified in paragraph III of Appendix G. This regulation applies to Category I SSNM facilities, hot-cell facilities, ISFSIs, MRSs, GROAs, power reactor facilities, research reactor facilities, test reactor facilities, and Category II and Category III SNM facilities.

Eight-hour notifications fall into two categories—(1) the licensee or certificate holder detects unauthorized operation, manipulation, or tampering events that do not result in the interruption of facility operations and do not prevent the implementation of the protective strategy (i.e., these events are not reportable under the 1-hour or 4-hour notification requirements), or (2) the licensee or certificate holder detects an unauthorized operation or manipulation of, or tampering with, networks or equipment within the scope of 10 CFR 73.54 or the security measures that protect such networks and equipment, but such actions did not interrupt or degrade the facility's SSEP functions.

2.6.1 Notification Requirements

10 CFR 73.71(f) Eight-hour notifications – facilities. (1) 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.

(2) Notifications must be made according to paragraph (j) of this section, as applicable.

Appendix G, Paragraph III. Events to be reported within eight hours of discovery.

Unauthorized operation or tampering events. An event involving—

(1) The unauthorized operation, manipulation, or tampering with any nuclear reactor's controls or SSCs that does not result in the interruption of the normal operations of the reactor;

(2) The unauthorized operation, manipulation, or tampering with any Category I SSNM facility's controls or SSCs that does not result in the interruption the normal operations of the facility; or

(3) The tampering, malicious or unauthorized access, use, operation, manipulation, or modification of any security measures associated with systems, networks, and equipment 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.

2.6.2 Examples of Reportable Events

The NRC staff considers that the following facility-security events as examples of the types of events that require notification under 10 CFR 73.71(f) and paragraph III of Appendix G.

The following are examples of unauthorized use or tampering with components or controls, including the security system, that does not interrupt the normal operation of the plant and does not prevent the implementation of the licensee's or certificate holder's protective strategy (i.e., events that are reportable under the 1-hour or 4-hour notification requirements). The act of tampering should be reported, rather than the effects of the tampering, because it is not known whether the tampering could create potentially significant equipment issues.

- a. the unauthorized operation, manipulation, or tampering with a nuclear reactor's controls, safety-related SSCs, or nonsafety-related SSCs that do not interrupt the normal operations of the reactor
- b. the unauthorized operation, manipulation, or tampering with a Category I SSNM facility's controls, safety-related SSCs, or nonsafety-related SSCs that do not interrupt the normal operations of the facility
- c. the unauthorized operation, manipulation, or tampering with the security-related SSCs that could prevent the implementation of the licensee's or certificate holder's protective strategy
- d. the intentional cutting of wires that does not affect the facility or security operations
- e. the modification of security equipment that renders the equipment inoperable
- f. the overt changing of equipment or controls to settings that do not affect their intended function
- g. the tampering with, or destruction of, equipment that does not affect plant operations or security (e.g., water coolers, office equipment, maintenance tools)

The following are examples of unauthorized operation or manipulation of, or tampering with, networks or equipment within the scope of 10 CFR 73.54 or the security measures that protect such networks and equipment but where such actions did **not** interrupt or degrade the facility's SSEP functions:

- h. the discovery of a vulnerability in a CDA or security measures, but with compensatory measures in place to mitigate the issue
- i. the discovery that a CDA is disabled or has failed but does not degrade any SSEP functions
- j. the discovery of the loss of control of a mobile CDA but the device has adequate "data at rest" protection and automatically wipes itself after a period of inactive use

Additionally, licensees or certificate holders should evaluate an event that is not reportable under this requirement for reporting or recording under the other provisions of 10 CFR 73.71 or Appendix G to 10 CFR Part 73.

2.7 Enhanced Weapons—Stolen or Lost, To Be Reported within 1 Hour or 4 Hours

The regulations in 10 CFR 73.71(g) require each licensee or certificate holder subject to the provisions of 10 CFR 73.18 who possesses enhanced weapons to notify the NRC Headquarters Operations Center as soon as possible but not later than either 1 hour or 4 hours (see below) after the discovery that their enhanced weapon has been stolen or lost. This regulation applies to the classes of facilities, radioactive material, and other property designated by the Commission in 10 CFR 73.18(c).

Licensees and certificate holders must make a 1-hour notification to the NRC upon the discovery that an enhanced weapon is missing from inside the PA, VA, or MAA of a designated facility. Licensees and certificate holders must make a 4-hour notification to the NRC subsequent to notifying ATF upon the discovery that an enhanced weapon is missing from outside the PA, VA, or MAA of a designated facility. The NRC staff views uncontrolled enhanced weapons inside a facility authorized to possess them as a greater risk to the facility (i.e., potential insider issue) that should be treated the same as other significant security events that warrant a 1-hour notification. In contrast, uncontrolled enhanced weapons outside a facility are considered less of an immediate risk to the facility itself, and may instead present a law enforcement risk (i.e., the weapons could assist in the commission of a crime away from the facility). Examples include enhanced weapons being stolen or lost outside a PA, VA, or MAA (e.g., from a training facility or while the weapons were being transported back after escorting a designated shipment of radioactive material).

A licensee or certificate holder possessing enhanced weapons is required to notify ATF under 27 CFR 479.141 (Ref. 9) independent of any notifications made to the NRC of stolen or lost enhanced weapons. However, licensees and certificate holders should notify the NRC first of weapons that are stolen or lost from within their PA, VA, or MAA, because the NRC staff considers enhanced weapons lost or unsecured within a facility as posing a threat to the facility (e.g., their use by an active-violent insider). The NRC staff considers enhanced weapons that are discovered to be stolen or lost outside of these facility security areas to have a greater potential for criminal activity separate from the licensee's or certificate holder's facility. Therefore, the licensee or certificate holder should notify ATF first in those circumstances.

In addition to notifying the NRC, 10 CFR 73.71(g)(1) requires licensees and certificate holders to notify appropriate LLEA officials within 48 hours of the discovery of stolen or lost enhanced weapons.

The regulations in 10 CFR 73.18 provide a distinction between the transfer of enhanced weapons (between two registered or licensed owners) and the transportation of enhanced weapons by a single owner/registrant (to and from the facility). The following examples reflect this distinction.

2.7.1 Notification Requirements

10 CFR 73.71(g) Enhanced weapons – stolen or lost. (1) Each licensee or certificate holder possessing enhanced weapons in accordance with the provisions of § 73.18 shall —

(i) Notify the NRC Headquarters Operations Center, as soon as possible but not later than one hour after the discovery of any stolen or lost enhanced weapons possessed by the licensee or certificate holder. This notification applies to enhanced weapons that were stolen or lost from within a licensee's or certificate holder's protected area, vital area, or material access area.

(ii) Notify the NRC Headquarters Operations Center, as soon as possible but not later than four hours subsequent to the notification of the U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) of the discovery of any stolen or lost enhanced weapons possessed by the licensee or certificate holder. This notification applies to enhanced weapons that were stolen or lost from outside of the licensee's or certificate holder's protected area, vital area, or material access area.

(iii) Notify the appropriate local law enforcement officials, as soon as possible but not later than 48 hours of the discovery of stolen or lost enhanced weapons. These notifications must be made by telephone to the appropriate local law enforcement officials. Licensees and certificate holders shall identify the appropriate local law enforcement officials for these notifications and include their contact phone number(s) in written procedures.

(2) Notifications must be made according to paragraph (j) of this section, as applicable.

(3) Independent of the requirements of this section, licensees and certificate holders possessing enhanced weapons in accordance with § 73.18 also have an obligation under ATF's regulations to immediately upon discovery notify ATF of any stolen or lost enhanced weapons (see 27 CFR 479.141).

2.7.2 Examples of Reportable Events

The NRC staff considers that the following security events as examples of the types of events that require notification under 10 CFR 73.71(g).

- a. enhanced weapons are lost during shipment to or from the licensee's or certificate holder's facility (e.g., a training facility or during the transportation of weapons preceding or following escort duties of a designated shipment of nuclear or radioactive material) (4-hour notification)
- b. enhanced weapons are lost during transfer to another authorized NRC licensee or certificate holder (4-hour notification)
- c. enhanced weapons are lost during transfer to another Federal firearms license holder or government agency (4-hour notification)
- d. enhanced weapons are discovered missing from their authorized storage location inside a PA, VA, or MAA during a periodic inventory (1-hour notification)
- e. enhanced weapons are discovered missing from their authorized storage location that is located outside of a PA, VA, and MAA during a periodic inventory (e.g., a licensee's or certificate holder's firing range) (4-hour notification)

2.8 Enhanced Weapons—Adverse ATF Findings To Be Reported within 24 Hours

The regulations in 10 CFR 73.71(h) require each licensee or certificate holder subject to the provisions of 10 CFR 73.18 who possesses enhanced weapons to notify the NRC Headquarters Operations Center as soon as possible but not later than 24 hours after the receipt of an adverse inspection or enforcement finding or other adverse notice from ATF regarding the licensee's or certificate holder's possession, receipt, transfer, or storage of enhanced weapons. This regulation applies to the classes of facilities, radioactive material, and other property designated by the Commission in 10 CFR 73.18(c).

This requirement is intended to alert the NRC to action by ATF involving an adverse inspection or enforcement action affecting an NRC licensee or certificate holder possessing enhanced weapons. This notification is intended to permit the NRC to respond to potential inquiries related to the ATF action.

2.8.1 Notification Requirements

10 CFR 73.71(h) Enhanced weapons – adverse ATF findings. (1) Each licensee or certificate holder possessing enhanced weapons in accordance with § 73.18 shall—

(i) Notify the NRC Headquarters Operations Center as soon as possible but not later than 24 hours after receipt of an adverse inspection or enforcement finding or other adverse notice from the ATF regarding the licensee's or certificate holder's possession, receipt, transfer, or storage of enhanced weapons; and

(ii) Notify the NRC Headquarters Operations Center as soon as possible but not later than 24 hours after receipt of an adverse inspection or enforcement finding or other adverse notice from the ATF regarding the licensee's or certificate holder's ATF issued federal firearms license.

(2) Notifications must be made according to paragraph (j) of this section, as applicable.

2.8.2 Examples of Reportable Events

The NRC staff considers that the following finding and notices as examples of the types of events that require notification under 10 CFR 73.71(h).

- a. receipt of a notice of violation from ATF following an inspection of the licensee's or certificate holder's facility
- b. receipt of an inspection finding from ATF of less than adequate (but not noncompliant) recordkeeping regarding the receipt or transfer of enhanced weapons
- c. notification that ATF will issue a press release of an adverse inspection or enforcement finding regarding a specific licensee's or certificate holder's possession, receipt, or transfer of enhanced weapons

3 Telephonic Reporting Process

The regulations in 10 CFR 73.71(j) require licensees and certificate holders to make a telephonic notification to the NRC Headquarters Operations Center of certain security events specified in 10 CFR 73.71(a), (b), (c), (d), (e), (f), (g), and (h). Licensees and certificate holders should make these telephonic reports via any method that will ensure that a report is received by the NRC Headquarters Operations Center or other specified government officials within the timeliness requirements. Methods of communication include, but are not limited to, standard land phone circuits (wire or fiber optic), cellular phone circuits, satellite phone circuits, or licensee proprietary phone circuits (e.g., load dispatcher phone circuits).

Licensees and certificate holders should contact the NRC Headquarters Operations Center using the commercial telephone numbers that are specified in Table 1, "Mailing Addresses, Telephone Numbers, and E-mail Addresses," of Appendix A to Part 73 (Ref. 1).

Licensees and certificate holders are not required to make separate notifications for security events that also result in their declaration of an emergency. In such circumstances, licensees or certificate holders should make the necessary emergency notifications required by the various regulations applicable to their specific facility or activity. When making such a notification, the licensee or certificate holder should indicate to the NRC that the notification is also to report a security event under a specific paragraph of 10 CFR 73.71.

3.1 Telephonic Reporting Process Requirements

(j) Notification process. (1) Each licensee and certificate holder shall make the telephonic notifications required by paragraphs (a), (b), (c), (d), (e), (f), (g), and (h) of this section to the NRC Headquarters Operations Center via any available telephone system. Commercial telephone numbers for the NRC Headquarters Operations Center are specified in Table 1 of Appendix A of this part.

(2) Licensees and certificate holders shall make required telephonic notifications via any method that will ensure that a report is received by the NRC Headquarters Operations Center or other specified government officials within the timeliness requirements of paragraphs (a), (b), (c), (d), (e), (f), (g), and (h) of this section, as applicable.

(3) Notifications required by this section that contain Safeguards Information may be made to the NRC Headquarters Operations Center without using secure communications systems under the exception of § 73.22(f)(3) of this part for emergency or extraordinary conditions.

(4)(i) Notifications required by this section that contain classified national security information and/or restricted data must be made to the NRC Headquarters Operations Center using secure communications systems appropriate to the classification level of the message. Licensees and certificate holders making classified telephonic notifications shall contact the NRC Headquarters Operations Center at the commercial numbers specified in Table 1 of Appendix A to this part and request a transfer to a secure telephone, as specified in paragraph III of Appendix A to this part.

(ii) If the licensee's or certificate holder's secure communications capability is unavailable (e.g., due to the nature of the security event), the licensee or certificate holder shall provide as much information to the NRC as is required by this section, without revealing or discussing any classified information, in order to meet the timeliness requirements of this section. The licensee or certificate holder shall also indicate to the NRC that its secure communications capability is unavailable.

(iii) Licensees and certificate holders using a non-secure communications capability may be directed by the NRC Emergency Response management to provide classified information to the NRC over the non-secure system, due to the significance of the ongoing security event. In such circumstances, the licensee or certificate holder shall document this direction and any information provided to the NRC over a non-secure communications capability in the follow-up written report required in accordance with paragraph (m) of this section.

(5)(i) For events reported under paragraph (a) of this section, the NRC may request that the licensee or certificate holder maintain an open and continuous communication channel with the NRC Headquarters Operations Center as soon as possible. Licensees and certificate holders shall establish the requested continuous communication channel once the licensee or certificate holder has completed other required notifications under this section, § 50.72 of this chapter, Appendix E of part 50 of this chapter, or § 70.50 of this chapter; or completed any immediate actions required to stabilize the plant, to place the plant in a safe condition, to implement defensive measures, or to request assistance from the LLEA.

(ii) When established, the continuous communications channel shall be staffed by a knowledgeable individual in the licensee's security, operations, or emergency response organizations from a location deemed appropriate by the licensee.

(iii) The continuous communications channel may be established via any available telephone system.

(6)(i) For events reported under paragraph (b) of this section, the NRC may request that the licensee or certificate holder maintain an open and continuous communication channel with the NRC Headquarters Operations Center as soon as possible. Licensees and certificate holders shall establish the requested continuous communication channel once the licensee or certificate holder has completed other required notifications under this section, § 50.72 of this chapter, Appendix E of part 50 of this chapter, or § 70.50 of this chapter; or requested assistance from the LLEA.

(ii) When established, the continuous communications channel shall be staffed by a knowledgeable individual in the communication center monitoring the shipment.

(iii) The continuous communications channel may be established via any available telephone system.

(7) For events reported under paragraphs (c), (d), (e), (f), (g), and (h) of this section, the NRC may request that the licensee or certificate holder maintain an open and continuous communication channel with the NRC Headquarters Operations Center.

(8) Licensees and certificate holders desiring to retract a previous security event report that has been determined to be 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.

10 CFR 73.71(n) Declaration of emergencies. Notifications made to the NRC for the declaration of an emergency class shall be performed in accordance with §§ 50.72, 70.50, 72.75, and 76.120 of this chapter, as applicable.

10 CFR 73.71(o) Elimination of duplication. Separate notifications and reports are not required for events that are also reportable in accordance with §§ 50.72, 50.73, 70.50, 72.75, and 76.120 of this chapter. However, these notifications should also indicate the applicable § 73.71 reporting criteria.

32 Content of 15-Minute Reports

Licensees or certificate holders should include, at a minimum, the following information in their report:

- a. name and location of the facility or activity
- b. caller's name and callback number
- c. authentication code (only for facility events reported under 10 CFR 73.71(a))
- d. emergency classification (only if declared)
- e. description of the imminent or hostile act (e.g., armed assault, vehicle bomb, or credible bomb threat)
- f. current event status (e.g., imminent, in progress, neutralized, or unknown)

33 Content of 1-Hour, 4-Hour, and 8-Hour Reports

Licensees or certificate holders should include, at a minimum, the following information in their report:

- a. name and location of the facility or activity
- b. caller's name and callback number
- c. emergency classification (only if declared)
- d. event description including the following information:
 - (1) who was involved
 - (2) what occurred during the event
 - (3) time the event was discovered and when initiated and completed, if known
 - (4) location of the event (this may include plant or security systems or geographic locations affected)
 - (5) why the event occurred, if known
 - (6) how the event occurred
- e. current event status (e.g., ongoing, neutralized, anticipated, unknown)
- f. security response and corrective actions taken
- g. offsite assistance (e.g., requested or not requested, arrived, status)

- h media interest, if any, including licensee or certificate holder issued press releases

34 Content of 4-Hour Suspicious Activity Reports

Licensees or certificate holders should include, at a minimum, the following information in their report:

- a name and location of the facility or activity
- b. caller's name and callback number
- c event description
 - (1) who was involved
 - (2) what occurred during the event
 - (3) when the event was discovered and when initiated and completed, if known
 - (4) location of the event (this may include plant or security systems or geographic locations effected)
 - (5) why the event occurred, if known
 - (6) how the event occurred
- d. source of the information (if a law enforcement agency, provide contact telephone number)

35 Reports Containing Safeguards Information

Licensees and certificate holders making notifications required by 10 CFR 73.71 that contain Safeguards Information may notify the NRC Headquarters Operations Center without using a secure communications system (to communicate the Safeguards Information). The NRC's regulations in 10 CFR 73.22(f)(3) (Ref. 1) provide an exception to the requirement to communicate Safeguards Information using a secure communications system under emergency or extraordinary conditions.

All licensee and certificate holder reports of security events made to the NRC under the provisions of 10 CFR 73.71 are considered emergency or extraordinary conditions (i.e., the use of a secure communications system to communicate is not required under the exception of 10 CFR 73.22(f)(3)). However, if the licensee or certificate holder has ready access to a secure communications system within the time limits of 10 CFR 73.71, then the licensee or certificate holder should use such a secure communications system to communicate information to the NRC and protect the Safeguards Information contained in the report from unintentional or inadvertent disclosure. Additionally, licensees and certificate holders should apply this exception to actual events only. As such, it should not be applied to simulated events communicated as part of a drill or exercise, or to routine events, e.g., the retraction of a previous security report as invalid.

36 Reports Containing Classified Information

Licensees and certificate holders making notifications required by 10 CFR 73.71 that contain classified National Security Information (NSI) or Restricted Data (RD) should notify the NRC Headquarters Operations Center using secure communications systems appropriate to the classification

level of the communication. Licensees and certificate holders making classified notifications should contact the NRC Headquarters Operations Center at the commercial telephone numbers specified in Table 1 of Appendix A to Part 73 and request a transfer to a secure telephone as specified in paragraph III of Appendix A.

If the licensee's or certificate holder's secure communications capability is unavailable (e.g., because of the nature of the security event), the licensee or certificate holder should provide as much information to the NRC as is required by 10 CFR 73.71, without revealing or discussing any classified information, to meet the time limits of 10 CFR 73.71. The licensee or certificate holder should also indicate to the NRC at the beginning of the notifications that its secure communications capability is unavailable, in order to prevent the inadvertent disclosure of classified information.

If the nature of the security event warrants, NRC Emergency Response Management may direct the licensee or certificate holder to use any available nonsecure communications method to immediately communicate classified information to the NRC (regarding security event notifications required by 10 CFR 73.71). If so directed, the licensee or certificate holder should provide the classified information to the NRC over the best available nonsecure system. For example, the NRC staff considers using an available nonsecure land line as preferable to using an available nonsecure cellular or satellite system. Additionally, licensees and certificate holders should apply this exception to actual events only. As such, it should not be applied to simulated events communicated as part of a drill or exercise, or to routine events, e.g., the retraction of a previous security report as invalid.

In the written followup report for the event (required by 10 CFR 73.71(m)), the licensee or certificate holder should document this direction from the NRC, the reason for the unavailability of a secure communications capability, and the specific classified information communicated to or from the NRC over a nonsecure communications capability (see also Regulatory Position 4 of this guide). The written followup report should be appropriately classified by the licensee or certificate holder. The NRC will use the information in the written followup report to assess the impact of the possible compromise of the specific classified information communicated by the licensee, certificate holder, or the NRC over a nonsecure system, as required by Executive Order 13526, "Classified National Security Information." (Ref. 10).

3.7 Continuous Communications Channel Requirements

The NRC may request licensees and certificate holders reporting security events under 10 CFR 73.71(a), (b), (c), (d), (e), (f), (g), or (h) to maintain an open and continuous communications channel with the NRC Headquarters Operations Center. When so requested by the NRC, licensees and certificate holders should establish a continuous communications channel using an appropriate individual who is able to continuously interact with the NRC from a location the licensee or certificate holder deems appropriate. Licensees and certificate holders should consider using as an "appropriate individual" persons from their security, operations, or emergency response organization who are both knowledgeable in their security programs and requirements and received training as a communicator.

3.8 Reporting Significant Additional Information

Licensees and certificate holders who discover significant supplemental information after the initial telephonic notification to the NRC Headquarters Operations Center (in accordance with 10 CFR 73.71(j)), or after the submission of the written followup report (in accordance with 10 CFR 73.71(m)), should report this significant supplemental information by telephone to the NRC Headquarters Operations Center in accordance with 10 CFR 73.71(j).

Comment [z8]: I am not familiar with this specific training. Is this referring to ERO type training or another form of Security training?

Formatted: Highlight

3.9 Emergency Declarations and Duplicate Reports

Licensees and certificate holders reporting security events, under 10 CFR 73.71, that also involve the declaration of an Emergency Classification (e.g., Alert, Site Area Emergency, or General Emergency), in accordance with the licensee's or certificate holder's NRC-approved Emergency Response plan, should follow the appropriate regulations regarding the declaration of an emergency (i.e., emergency declarations have primacy over security event reports). Consequently, to reduce unnecessary burden and duplication, licensees and certificate holders may make a single report of security events that are subject to both emergency response and security event notification regulations. Licensees and certificate holders should indicate in their telephonic report all of the applicable reporting requirements for the event. However, this provision does not obviate a licensee's or certificate holder's responsibility to report significant additional information (see Regulatory Position 3.8 above).

3.10 Retraction of Previous Telephonic Security Event Reports

Licensees and certificate holders desiring to retract a previous telephonic security event report that they have determined (through their analysis or investigation) to be invalid should notify the NRC Headquarters Operations Center by telephone, in accordance with 10 CFR 73.71(j), and should indicate the report being retracted and the basis for the retraction. Such retractions should not be made over a non-secure communications system (see Regulatory Positions 3.5 and 3.6 above).

18

Security events notifications may be retracted at any time following the initial report to the NRC. However, see additional direction in Regulatory Position 4.2 below on documenting this retraction, if a 60-day written followup report has already been submitted.

4 Written Followup Reports

The regulations in 10 CFR 73.71(m) require licensees and certificate holders who have made a telephonic report to the NRC Headquarters Operations Center of security events specified in 10 CFR 73.71(a), (b), (c), (d), (e), (f), and (g) to submit a written followup report to the NRC within 60 days of the telephonic report. Licensees and certificate holders should submit the written followup report in accordance with the provisions of 10 CFR 73.4 (Ref. 1).

The NRC does not require licensees and certificate holders who have made a telephonic report to the NRC Headquarters Operations Center of security events specified in 10 CFR 73.71(h) to submit a written followup report for these events. Additionally, the NRC does not require licensees and certificate holders who have made a telephonic report to the NRC Headquarters Operations Center of security events specified in 10 CFR 73.71(e) involving suspicious-activity or law-enforcement events to submit written followup reports for these events. Events recorded in the safeguards event log under 10 CFR 73.71(k) also do not require a written followup report.

Licensees' and certificate holders' written followup reports should contain sufficient details and information to allow a knowledgeable individual to understand what occurred during the event, whether any personnel errors or equipment malfunctions occurred, whether any compensated or uncompensated vulnerabilities or degradations existed, and, if appropriate, whether any corrective actions to prevent recurrence were taken by the licensee or certificate holder. Licensees and certificate holders should retain a copy of any written reports submitted to the NRC for at least 3 years or until the termination of the license or certificate of compliance, whichever is longer.

Licensees and certificate holders who submit written reports to the NRC containing Safeguards Information should create, store, mark, label, handle, and transmit these written reports in accordance

with the applicable information security requirements of 10 CFR 73.21 and 10 CFR 73.22, "Protection of Safeguards Information: Specific Requirements" (Ref. 1) Licensees and certificate holders should perform a safeguards designation of such reports in accordance with the NRC's Designation Guide for Safeguards Information (DG-SGI-1). Written reports should be portion marked to indicate the designation level of the report's information.

Licensees and certificate holders who submit written reports to the NRC containing classified NSI or RD should create, store, mark, label, handle, and transmit these reports in accordance with the applicable information security requirements of 10 CFR Part 95, "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data" (Ref. 11). Licensees and certificate holders should perform a derivative classification of such reports in accordance with the classification guide(s) applicable to their facility or activity. Written reports should be portion marked to indicate the classification level of the report's information. If the follow-up report requires an original classification determination, then the licensee or certificate holder should make a provisional classification decision; mark, handle, store, and transmit the document according to that provisional decision; and forward the document to the NRC for an original classification determination.

4 Written Followup Report Requirements

10 CFR 73.71(m) Written reports. (1) Each licensee or certificate holder making an initial telephonic notification under paragraphs (a), (b), (c), (d), (e), (f), and (g) of this section shall also submit a written follow-up report to the NRC within 60 days of the telephonic notification, in accordance with § 73.4.

(2) Licenses and certificate holders are not required to submit a written report following a telephonic notification made under paragraphs (g) and (h) of this section.

(3) Licenses and certificate holders are not required to submit a written report following a telephonic notification made under paragraph (j) of this section involving suspicious event or law enforcement interaction specified in paragraph II(a), II(c), or II(d) of Appendix G.

(4) Each licensee and certificate holder shall submit to the Commission written reports that are of a quality that will permit legible reproduction and processing.

(5) Licensees subject to § 50.73 of this chapter shall prepare the written report on NRC Form 366.

(6) Licensees and certificate holders not subject to § 50.73 of this chapter shall prepare the written report in letter format.

(7) In addition to the addressees specified in § 73.4, the licensee or certificate holder shall also provide one copy of the written report addressed to the Director, Office of Nuclear Security and Incident Response (NSIR). The copy of a classified written report to the Director, NSIR, shall be provided to the NRC headquarters' classified mailing address specified in Table 2 of Appendix A to this part or in accordance with paragraph IV of Appendix A to this part.

(8) The report must include sufficient information for NRC analysis and evaluation.

(9) Significant supplemental information that becomes available after the initial telephonic notification to the NRC Headquarters Operations Center or after the submission of the written report must be telephonically reported to the NRC Headquarters Operations Center under paragraph (j) of this section and also submitted in a revised written report (with the revisions indicated) as required under paragraph (m) of this section.

(10) Errors discovered in a written report must be corrected in a revised written report with the revisions indicated.

(11) The revised written report must replace the previous written report; the update must be complete and not be limited to only supplementary or revised information.

(12) Each licensee and certificate holder shall maintain a copy of the written report of an event submitted under this section as a record for a period of three years from the date of the report or until termination of the license or the certificate of compliance.

(13)(i) If the licensee or certificate holder subsequently retracts a telephonic notification made under this section as 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 as 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.

(14) Each written report containing Safeguards Information or classified information must be created, stored, marked, labeled, handled, and transmitted to the NRC in accordance with the requirements of §§ 73.21 and 73.22 of this part or with Part 95 of this chapter, as applicable.

42 Retraction of Previous Written Followup Reports

If a licensee or certificate holder subsequently retracts a telephonic report made under 10 CFR 73.71(j) and has not yet submitted the followup written report required by 10 CFR 73.71(k), the NRC does not require the licensee or certificate holder to submit a written followup written report. However, if the licensee or certificate holder has already submitted a followup written report to the NRC before it retracts the telephonic report, the licensee or certificate holder should then submit a revised written report to the NRC indicating the initial event has been retracted and the basis for that conclusion. This supplemental written followup report is necessary because without the supplemental report (retracting the notification), the only NRC official agency record on the notification would be the initial written followup report.

4.3 Significant Additional Information and Correction of Errors

Licensees and certificate holders who discover significant supplemental information after the submission of a written followup report to the NRC should submit a revised written report, in accordance with the same processes as used to submit the initial written report. Licensees and certificate holders who discover errors in a written report previously submitted to the NRC should submit a revised written report, in accordance with the same processes as used to submit the initial written report. A revised written report should replace the previous written report (i.e., the updated report should be complete and should not be limited to only the supplementary or revised information). The revised report should indicate the revisions with revision bars to assist the reader.

44 Use of NRC Form 366

Reactor licensees should submit any written followup reports to the NRC required by 10 CFR 73.71 using NRC Form 366, "Licensee Event Report (LER)." All other licensees and certificate holders should submit any written followup reports to the NRC using a standard letter format.

45 Content of Written Followup Reports

Licensees and certificate holders preparing written followup reports should include sufficient information for the NRC to analyze the event. The NRC staff recommends that followup reports contain, at a minimum, the following information, as applicable:

- a date and time of the event, including chronological time line, if applicable; date and time of notifications to the NRC, State officials, or LLEA

- b. locations of the actual or threatened event in a PA, VA, MAA, CAA, OCA, or other area
- c. for power reactor licensees, the reactor's operating mode (e.g., shut down, operating, construction, decommissioning)
- d. safety, security, or emergency response systems directly or indirectly affected, damaged, or threatened
- e. type of onsite security force (i.e., proprietary or contract)
- f. number and type of personnel involved or contacted, such as contractors; security personnel; visitors; plant staff; perpetrators or attackers; NRC personnel; local, State, or Federal responders; and other personnel (please specify)
- g. method of discovery of the incident, event, or information, such as routine patrol or inspection, test, maintenance, alarm annunciation, chance, communicated threat, unusual circumstances (include details)
- h. immediate actions taken in response to the event and any compensatory measures established
- i. description of media interest and press releases
- j. indications or records of previous similar events
- k. procedural or human errors or equipment failures, as applicable
- l. cause of the event or the licensee's or certificate holder's analysis of the event (including a brief summary in the report and references to any ongoing or completed detailed investigations, assessments, analyses, or evaluations)
- m. corrective actions taken or planned, including dates of completion
- n. name and phone number of a licensee's or certificate holder's point of contact
- o. for reported uncompensated failures, degradations, or discovered vulnerabilities of security systems, licensees and certificate holders should also provide the following information, in addition to items a. through n. above:
 - (1) description of failed, degraded, or vulnerable equipment or systems (e.g., manufacturer and model number, procedure number)
 - (2) status of the equipment or system before the event (e.g., operating, being maintained secure, being implemented) and, as applicable, the compensatory measures put in place
 - (3) description of the failure, degradation, or vulnerability identified (specify)
 - (4) unusual conditions that may have contributed to the failures, degradations, or discovered vulnerabilities of the security system (e.g., environmental conditions, plant outage)
 - (5) apparent cause of component or system failure, degradation, or vulnerability
 - (6) secondary functions affected (for multiple-function components)

(7) effect on plant safety or emergency response capabilities

p. for threat-related incidents, licensees and certificate holders should also provide the following information, in addition to items a. through n. above (maintaining the integrity of any threat material, as it may become evidence in a law enforcement investigation):

- (1) type of threat (e.g., bomb threat, extortion, tampering, interruption of normal operations, attempted diversion of SSNM, theft, armed assault)
- (2) detailed description of perpetrators or attackers (e.g., number, armament, method of threat, appearance, personal characteristics)
- (3) method or means of the threat's communication (e.g., letter, telephone, e-mail)
- (4) text or transcript of the threat
- (5) clear photocopy of threat letter and accompanying envelope, if applicable

5. Security Events To Be Recorded within 24 Hours

The regulations in 10 CFR 73.71(k) require licensees and certificate holders subject to the provisions of 10 CFR 73.20, 10 CFR 73.25, 10 CFR 73.26, 10 CFR 73.37, 10 CFR 73.45, 10 CFR 73.46, 10 CFR 73.50, 10 CFR 73.51, 10 CFR 73.54, 10 CFR 73.55, 10 CFR 73.60, and 10 CFR 73.67 to maintain a safeguards event log. The NRC requires licensees and certificate holders to record security events specified in paragraph IV of Appendix G in a safeguards event log within 24 hours of the discovery of the event. This regulation applies to Category I SSNM facilities, hot-cell facilities, ISFSIs, MRSs, GROAs, power reactor facilities, research reactor facilities, test reactor facilities, and Category II and III SNM facilities. This also includes the transportation of Category I quantities of SSNM, SNF, HLW, and Category II and III quantities of SNM.

The NRC requires licensees and certificate holders to retain the safeguards event log as an official record for a period of 3 years after the last entry is made in each log or until the termination of their respective license or certificate of compliance, whichever is greater. The NRC does not require licensees and certificate holders to record (i.e. duplicate), in a safeguards event log, any security events that they reported to the NRC under the telephonic notification provisions of 10 CFR 73.71, including the events listed under paragraphs I, II, and III of Appendix G.

In general, licensees and certificate holders should record events in the safeguards event log that are less significant than those required to be reported telephonically to the NRC. However, further analysis of these recordable events may result in the identification of system or performance vulnerabilities, deficiencies, or trends that may require corrective action and may be generic in nature. The NRC expects all recordable security events to be recorded in the safeguards event log, regardless of who identifies the issue (i.e., licensee or certificate holder staff or contractors, NRC or State inspectors, or independent auditors).

Events recorded in the safeguards event log include failures, degradations, or discovered 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. These events also include failures, degradations, or discovered vulnerabilities that could have allowed unauthorized or undetected access to a vehicle transporting fresh nuclear fuel, SNF, or HLW; or to the nuclear fuel, SNF, or HLW regulated by the NRC. These events may also include a compensated vulnerability, failure, or degradation of security systems that, except for the compensatory actions, could

have allowed unauthorized access or contraband into a PA, VA, MAA, or CAA, or explosives or incendiaries beyond a vehicle barrier. These events may include a compensated vulnerability, failure, or degradation of security systems that, except for the compensatory actions, could have allowed unauthorized access or contraband into a vehicle transporting fresh nuclear fuel, SNF, or HLW; or to the nuclear fuel, SNF, or HLW itself. Finally, these events may also include a threatened, committed, or attempted act that would degrade the licensee's or certificate holder's protective strategy.

Compensatory measures may include backup equipment, additional security personnel, or other measures taken to ensure that the effectiveness of the physical protection program and systems or subsystems is not reduced by the failure or other contingency affecting the operation of security equipment or structures. To determine whether an event should be recorded or reported, the compensatory measures need to be implemented before the event or within the time limits described in the licensee's or certificate holder's NRC-approved security plans. Compensatory measures should also provide a level of protection equivalent to the system or systems that were degraded or that protect against the identified vulnerability.

Events recorded in the safeguards event log also include those that decreased or degraded the effectiveness of the licensee's or certificate holder's cyber security program or allowed unauthorized or undetected access to any systems, networks, or equipment that falls within the scope of 10 CFR 73.54. Decreases in the effectiveness of the cyber security program include any other threatened, attempted, or committed act not previously specified in Appendix G that has resulted, or has the potential for a decrease in the effectiveness of the cyber security program in a licensee's or certificate holder's NRC-approved cyber security plan.

Comment [z9]: Is this term appropriate given the change to "Reduction in Effectiveness" as described in 10 CFR 50.47 rulemaking?

Formatted: Highlight

The significance of a system defect or vulnerability are key factors in determining whether an event is reportable or recordable. Even compensatory measures implemented promptly after discovery of the defect or vulnerability, which did not provide protection for the period of time that the defect or vulnerability existed, would be reportable. Therefore, any failure, degradation, or discovered vulnerability that is known to have existed for a significant period of time and was not discovered in the course of patrols, surveillance, operational tests, or other means, should be considered for reporting within 1 hour (see Regulatory Position 2.3 of this guide).

Recordable events related to failures and degradations may include mechanical or electrical problems, procedural-related failures, or failures regarding personnel performance. Recordable events typically affect single elements of physical security systems or an individual, critical, single-failure program element that would not permit unauthorized access. However, for example, a properly compensated degraded barrier may involve multiple elements. Other failures, degradations, or discovered vulnerabilities of security systems not related to unescorted or unauthorized access should be recorded as described in paragraph IV of Appendix G.

5.1 Safeguards Event Log Record Requirements

10 CFR 73.71(k) Safeguards event log. Each licensee or certificate holder subject to the provisions of §§ 73.20, 73.25, 73.26, 73.37, 73.45, 73.46, 73.50, 73.51, 73.54, 73.55, 73.60, or 73.67 shall maintain a safeguards event log.

(1) The licensee or certificate holder shall record the facility-based or transportation-based events described in paragraph IV of Appendix G of this part within 24 hours of discovery in the safeguards event log.

(2) The licensee or certificate holder shall retain the safeguards event log as a record for three years after the last entry is made in each log or until the termination of the license or certificate of compliance.

Appendix G, Paragraph IV. Events to be recorded in the safeguards event log within 24 hours of discovery.

(a) Compensated security events. Any failure, degradation, or discovered vulnerability in a safeguards system, had compensatory measures not been established, that could have—

(1) Allowed unauthorized or undetected access of—

- (i) Explosives or incendiaries beyond a vehicle barrier;*
- (ii) Personnel or contraband into a PA, VA, MAA, or CAA; or*
- (iii) Personnel or contraband into a vehicle transporting special nuclear material, spent nuclear fuel, or high-level radioactive waste; or to the special nuclear material, spent nuclear fuel, or high-level radioactive waste itself.*

(2) Degrade the effectiveness of the licensee's or certificate holder's cyber security program or 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.

(b) Ammunition events.

(1) 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.

(2) A discovery that unauthorized ammunition is inside a PA, VA, MAA, or CAA.

(3)(i) Uncontrolled authorized ammunition means ammunition authorized by the licensee's or certificate holder's security plan or contingency response plan that is not in the possession of authorized personnel or is not in an authorized ammunition storage location.

(ii) Uncontrolled unauthorized ammunition means ammunition that is not authorized by the licensee's or certificate holder's security plan or contingency response plan.

(iii) Ammunition in the possession of law-enforcement personnel performing official duties inside a PA, VA, MAA, or CAA is considered controlled and authorized.

(4) The discovery of lost or uncontrolled authorized or unauthorized ammunition under circumstances that indicate the potential for malevolent intent shall be reported under paragraph I(f) of this appendix.

(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, provided—

(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.

(d) Loss of control or protection of Safeguards Information. A discovery that a loss of control over, or protection of, classified material containing Safeguards Information has occurred, provided—

(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; or

(3) the material would not have allowed unauthorized or undetected access to facility or transport contingency response procedures or strategies.

(e) Decreases in the effectiveness of the physical security program or the cyber security program. 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 licensee's or certificate holder's physical security program or cyber security program below that committed to in a licensee's or certificate holder's NRC-approved physical security plan or cyber security plan.

(f) Non duplication. Events reported under paragraphs I, II, or III of this appendix are not required to be recorded under the safeguards event log.

52 Content of the Safeguards Event Log

Licensees and certificate holders should record the following information, as a minimum and as applicable, in the safeguards event log for recordable security events:

- a. date and time of the event or condition
- b. brief (one-line) description of the event
- c. brief (one-line) description of compensatory measures implemented or corrective actions taken
- d. area or security element affected (e.g., PA, VA, OCA, perimeter alarm system, response capability, vehicle barriers, transport vehicle, communications)
- e. method of detection (e.g., alarm, patrol, test, informants, plant staff observations)
- f. reference to more detail when applicable (e.g., Incident Report 09-1234, Surveillance Test 04-2348, plant condition report number)

53 Example of Facility Events To Be Recorded in the Safeguards Event Log

The NRC staff considers that the following facility-security events as examples of the types of events that require recording under 10 CFR 73.71(k) and paragraph IV of Appendix G.

The following are examples of events involving failures, degradation, or discovered vulnerabilities in a security system that could have allowed unauthorized or undetected access to a PA, VA, MAA, or CAA, had compensatory measures not been established:

- a. properly compensated security computer or card reader failures
- b. properly compensated loss of the ability to detect intrusion (1) at the protected area perimeter when the loss involves several zones, or (2) within a single intrusion detection zone
- c. failure of search equipment for a short period (e.g., less than 1 hour), which could have allowed unsearched individuals or packages to enter controlled areas
- d. an individual requiring escort who becomes separated from his or her escort for a short period of time (e.g., less than 10 minutes) but no unauthorized areas were entered
- e. an individual who is incorrectly authorized access to areas not authorized but does not or cannot enter those areas and would have been granted access, if necessary
- f. tailgating through a security barrier into an area when the individual is authorized or could have been authorized
- g. 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)
- h. failure to adequately compensate for an event or identified failure, degradation, or vulnerability that would **not** have allowed undetected or unauthorized access or that has existed for only a very

short period of time (e.g., posting a compensatory officer in 12 minutes instead of the 10 minutes specified under the NRC-approved security plan)

- i. failures, degradations, or discovered vulnerabilities that, had compensatory measures not been implemented, might have allowed explosives or incendiaries beyond a vehicle barrier or personnel or contraband into a PA, VA, MAA, or CAA
- j. threatened, attempted, or confirmed acts, not previously defined in Appendix G, that have resulted in or have the potential for a decrease in the effectiveness of the licensee's or certificate holder's physical protection system

The following are examples of ammunition events that should be recorded in the licensee's or certificate holder's safeguards event log:

- k. The licensee or certificate holder discovers that authorized ammunition has been lost or is uncontrolled within a PA, VA, MAA, or CAA. Uncontrolled authorized ammunition means ammunition authorized by the licensee's or certificate holder's security plan or contingency response plan that is not in the possession of authorized personnel or is not in an authorized ammunition storage location.
- l. The licensee or certificate holder discovers that unauthorized ammunition is within a PA, VA, MAA, or CAA. Unauthorized ammunition means ammunition that is not authorized by the licensee's or certificate holder's security plan or contingency response plan. Ammunition in the possession of law-enforcement personnel performing official duties inside a licensee's or certificate holder's PA, VA, MAA, or CAA is considered controlled and authorized.

The following are examples of cyber security events that should be recorded in the licensee's or certificate holder's safeguards event log:

- m. accidental deletion of security logs
- n. properly compensated CDA failures
- o. an individual who is incorrectly authorized access to a CDA but does not or cannot access that CDA and would have been granted access, if necessary

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:

- p. failure or degradation of lighting below security-plan requirements, as long as the entire perimeter intrusion detection system remains operational
- q. loss of partial capability of one alarm station (for facilities with two alarm stations) to remotely monitor, assess, or initiate a response to alarms, as long as the same capability remains operable in the other alarm station
- r. loss of control or protection over Safeguards Information when there does not appear to be evidence of theft or compromise and the information is recovered within 1 hour

- s. loss of control or protection over Safeguards Information that would not have allowed unauthorized or undetected access or significantly affected a contingency response
- t. loss of control or protection over classified information when there does not appear to be evidence of theft or compromise and the information is recovered within 1 hour
- u. loss of control or protection over Safeguards Information that would not have allowed unauthorized or undetected access or significantly affected a contingency response
- v. loss of control of an authorized standard security weapon within a PA, VA, MAA, or CAA that is retrieved within 1 hour of the discovery of its loss
- w. theft or loss of standard security weapons from a location outside of the licensee's or certificate holder's PA or CAA, provided the weapon would not affect the implementation of the licensee's or certificate holder's protective strategy
- x. access control failures that unlock a door but where alarms are operable, or where an alarm failure occurs with an operable secured door
- y. unsubstantiated bomb or extortion threats, meaning a threat for which no specific organization or individual claims responsibility, it is determined to be fictitious, and it is not supported by any evidence other than the threat message itself
- z. frequent nuisance alarms caused by mechanical, electrical, or environmental conditions and false alarms that meet or exceed the invalid rates, as specified in the licensee's or certificate holder's NRC-approved physical security plans or procedures
- aa. unplanned missed security patrols which resulted in a failure to meet security requirements
- bb. termination of personnel whose job duties and responsibilities actively support the licensee's or certificate holder's insider mitigation program
- 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
- dd. loss of partial capability to monitor, assess, or initiate response to cyber events as long as the same capability remains operable at another ~~staffed~~^{manned} location
- ee. unsubstantiated cyber threats, meaning a threat for which no specific organization or individual claims responsibility, is determined to be fictitious, and is not supported by evidence other than the threat message itself
- ff. unplanned missed cyber vulnerability assessments

5.4 Examples of Transportation Events To Be Recorded in the Safeguards Event Log

The NRC staff considers that the following transportation-security events as examples of the types of events that require recording under 10 CFR 73.71(k) and paragraph IV of Appendix G.

The following are examples of failures, degradations, or discovered vulnerabilities in a security system that could have allowed unauthorized or undetected access into a vehicle transporting Category I SSNM, Category II or III SNM, SNF, or HLW; or to the Category I SSNM, Category II or III SNM, SNF, or HLW, had compensatory measures not been established:

- a. failures, degradations, or discovered vulnerabilities that, had compensatory measures not been implemented, might have allowed explosives or incendiaries into a vehicle transporting Category I SSNM, Category II or III SNM, SNF, or HLW; or into the Category I SSNM, Category II or III SNM, SNF, or HLW itself
 - b. loss of intra-convoy communications for SSNM, SNF, or HLW transport when the ability to communicate with the movement control center remains intact
 - c. unplanned loss of the ability to monitor a transporter's remote position
 - d. unplanned loss of the ability of the movement control center to monitor a transporter's position
 - e. unplanned loss of the ability to communicate with the movement control center
 - f. unplanned (i.e., inadvertent) activation of immobilization or intrusion delay systems
- 6 Security Events that Are Not Considered Reportable or Recordable

In general, reporting and recording security events should provide relevant, timely, and factual information regarding events, system failures, or vulnerabilities, as well as information that may be of value in assessing the significance of the threat. The NRC staff recognizes that there may be other failures that would not reduce security system effectiveness or would have little or no security significance. The NRC staff has evaluated previous security reports and determined that some were not needed, causing unnecessary burdens on licensees, certificate holders, and the NRC.

Licensees and certificate holders should use the guidance in this regulatory position to determine whether or not an event should be reported or recorded. Licensees and certificate holders should use sound and reasonable judgment when determining whether to record or report an event. The examples provided below represent the types of events that need not be reported and are not intended to be all-inclusive or limiting. Should questions arise regarding whether to report or record an event, the licensee or certificate holder may consider discussing the matter with the appropriate NRC regional or Headquarters staff, if time permits.

6.1 Examples of Events that are Not Required to be Reported

The NRC staff considers the following as examples of the type of security-related events that are not required to be reported under 10 CFR 73.71 and Appendix G:

- a. discovery of prohibited items that are found during entrance searches to a facility
- b. discovery of prohibited items that are found inside the controlled area of a facility or inside a transport
- c. discovery of weapons that are found during entrance searches to a facility, provided the licensee concludes the individual had no malevolent intent

Prohibited items are identified by the licensee or certificate holder as banned from its site by its written procedures or policies. However, prohibited items do not include contraband items that are reportable under Regulatory Position 2.3 above.

Licensees and certificate holders discovering weapons contraband during the entrance search to a facility should evaluate whether malevolent intent is present and the individual legally possesses the

weapon under State law (e.g., the individual has a permit for the weapon). If the licensee or certificate holder suspects malevolent intent is present, the licensee or certificate holder should report the event as a 1-hour event. If the licensee or certificate holder concludes that malevolent intent is not present, the licensee or certificate holder should record the event the Safeguards Event Log. Licensees and certificate holders discovering explosive and incendiary contraband during the entrance search to a facility should report such events as a 1-hour event in all circumstances. NRC staff considers that while an individual may legally possess a weapon outside of an NRC-regulated facility, they typically are never authorized to possess explosives and incendiaries. Therefore, the NRC staff presumes that malevolent intent is present in such cases. Moreover, licensees and certificate holders identifying instances where contraband has actually entered a PA, VA, MAA, or CAA should report such events as 1-hour events (see Regulatory Position 2.3 above).

A licensee's or certificate holder's discovery of prohibited items inside of controlled areas should be evaluated under the licensee's or certificate holder's corrective action program, particularly if the event indicates weaknesses or failures in licensee's or certificate holder's security screening processes (to detect and prevent the entry of the prohibited items).

62 Examples of Events that are Not Required to be Recorded in the Safeguards Event Log

The NRC staff considers the following as examples of security-related events that are not required to be recorded under 10 CFR 73.71 and Appendix G:

- a. failure, degradation, or compromise of security systems that are preplanned, as long as adequate compensatory measures are in place prior to the failure
- b. a non-threatening individual (e.g., a child) attempting but failing to climb a PA fence
- c. a fire or explosion, if it can be determined, within 1 hour, that it is not suspicious (e.g., a fire in a trash bin, a lightning strike, or a transformer fault)
- d. infrequent nuisance alarms caused by mechanical, electrical, or environmental problems and false alarms that do not exceed the invalid rates, as specified in the licensees' or certificate holders' NRC-approved security plans or their implementing procedures, or that do not degrade system effectiveness
- e. suspected tampering with safety equipment that is determined, within 1 hour, not to be tampering
- f. cuts or holes made through required barriers by authorized persons for legitimate reasons (e.g., to install a pipe), as long as there is prior approval, coordination, and proper implementation of compensatory measures prior to the work commencing
- g. infrequent and nonrecurring failure of search equipment (with compensatory measures properly implemented), if the licensee or certificate holder discovers the failure before entry of the person or vehicle into a controlled area
- h. lost, stolen, unaccounted for, or improperly controlled (to include unauthorized, offsite removal) access-control devices, including picture badges, keys, key cards, or access-control computer codes that the licensee or certificate holder determined could not be used to allow unauthorized or undetected access to controlled areas

- i. an individual requiring an escort who becomes separated from his or her escort, when the escort recognizes and immediately reestablishes escort duties, provided the licensee or certificate holder determines that the individual did not enter any unauthorized areas
- j. an individual requiring an escort who enters a nonsensitive area with limited entry and exit (such as a restroom), while the escort maintains observation of the exit (not intruding into a visitor's personal activities but ensuring supervision of the physical whereabouts of the visitor)
- k. individuals photographing facilities from tourist areas, provided no other suspicious activity is involved
- l. normal and routine inquiries from students or members of the public regarding facilities or activities
- m. normal and routine inquiries from members of the media regarding facilities or activities, recognizing that accredited working journalists may conduct normal and recognizable research on the licensee's or certificate holder's security performance and protection capabilities, and thus, if the inquiries are common and understandable, their elicitation of sensitive information should not be reported or recorded
- n. routine, prearranged, and unsuspicious aircraft overflight activity
- o. responses to information provided to the licensee or certificate holder by the NRC (e.g. threat warnings)

7. Training of Nonsecurity Staff on Reporting and Recording Requirements

The discovery or identification of reportable or recordable events is not limited to members of the licensee's or certificate holder's security organization. All site employees with unescorted access should receive training on this subject to foster awareness and to understand their responsibility to immediately notify site security or management personnel of anomalies, failures, degradations, or vulnerabilities of security systems, or of suspicious activities. Licensees and certificate holders may provide this training during general plant training and periodic refresher training. The NRC staff notes that some licensees or certificate holders have also found it beneficial to include training "tips" or elements of the training program in recurring plant publications, such as newsletters, electronic signs, or other organizational reminders.

In accordance with 10 CFR 73.55(i)(5), the NRC requires power reactor licensees to ensure that their physical protection program includes surveillance, observation, and monitoring, as needed, to satisfy the design requirements of 10 CFR 73.55(b), identify indications of tampering, or otherwise implement the physical protection program. This specific regulatory requirement does not exist for other classes of licensees and certificate holders. However, regardless of regulatory requirements, the NRC staff considers it prudent for all licensees and certificate holders subject to 10 CFR 73.71 to include guidance for all employees regarding the observation or discovery of possible tampering, unusual activities, or unusual equipment conditions, as well as the prompt reporting of such information to facility or security management.

D. IMPLEMENTATION

The purpose of this regulatory position is to provide information to applicants, licensees, and certificate holders regarding the NRC's plans for using this draft regulatory guide. The previous version of this document, RG 5.62, Revision 1, remains in effect until Revision 2 is issued. Supporting guidance document NUREG-1304, "Reporting of Safeguards Events," issued February 1988 (Ref. 12), also remains in effect. NUREG-1304 is based upon a workshop on reporting and recording safeguards events that was held in 1988 following the issuance of RG 5.62, Rev. 1. NUREG-1304 is structured in a question and answer format. However, given the changes to the regulations and this regulatory guidance, the NRC plans to conduct a workshop on these revised safeguards event reporting and recording requirements (approximately 6 to 9 months after the effective date for a final rule and the issuance of RG 5.62, Rev. 2) with the goal of issuing Revision 1 to NUREG-1304.

The NRC has issued this draft guide to encourage public participation in its development. The NRC will consider all public comments received in the development of the final guidance document. Applicants, licensees, or certificate holders may propose an alternative or use a previously established acceptable alternative method for complying with the specified portions of the NRC's regulations. Otherwise, the NRC will use the methods described in this guide in evaluating compliance with the applicable regulations for license and certificate applications, license and certificate amendment applications, and amendment requests.

GLOSSARY

This glossary is intended to aid the reader in implementing this guide to meet the requirements set forth in 10 CFR 73.71 and Appendix G. Definitions for certain security terms are also found in 10 CFR 73.2 (Ref. 1).

Any failure, degradation, or discovered vulnerability—the performance of a system or component or security measure that has been reduced to the degree that it is rendered ineffective for the intended purpose. This includes cessation of proper functioning or performance of equipment, personnel, or procedures that are part of the physical protection program necessary to meet the requirements in 10 CFR Part 73, or a discovered defect in such equipment, personnel, or procedures that degrades a function or performance that could be exploited for the purpose of committing acts described in Appendix G to 10 CFR Part 73.

Attempts—reliable and substantive information exists that an effort to accomplish the threat has taken place. This includes events that have not occurred or have not been completed because they were interrupted or stopped before completion, or would have occurred in more than 2 hours.

Contraband—materials banned from a protected area, vital area, material access area, or controlled access area. Contraband consists of unauthorized firearms, explosives, and incendiary devices that can be used to commit acts of sabotage as specified under Section 236 of the *Atomic Energy Act of 1954*, as amended (AEA) (42 U.S.C. § 2284). Contraband may be carried or concealed on personnel or in packages, materials or vehicles.

Covered weapons—any handgun, rifle, shotgun, short-barreled shotgun, short-barreled rifle, semiautomatic assault weapon, machine gun, ammunition for any such weapon, or a large capacity ammunition feeding device, as specified under Section 161A of the AEA (42 U.S.C. § 2201a). Covered weapons include both enhanced weapons and standard weapons.

Credible threat—credible information that has been received from a source determined to be reliable (e.g. law enforcement, government agency), or has been verified to be true. A threat can be verified to be true or considered credible under the following conditions:

- (1) physical evidence supporting the threat exists,
- (2) information independent from the actual threat message exists that supports the threat, or
- (3) a specific known group or organization claims responsibility for the threat,

or when the information is considered so significant that, regardless of the absence of (1), (2), or (3), licensee or certificate holder management has determined that action is required.

Critical digital asset (CDA)—the electronic systems, networks, or equipment that fall within the scope of 10 CFR 73.54 (i.e., within the Level 3 or 4 boundaries described in Regulatory Guide 5.71). Such systems, networks, and equipment have the ability to compromise the facility's safety, security, or emergency response (SSEP) functions.

Dedicated observer—a trained person, not necessarily a member of the security force, who is posted as a temporary compensatory measure for a degraded assessment or detection capability, or both. While performing this function, the person's duties must be limited to detection and assessment. As a minimum, the person must be able to view the entire area affected by the degradation and must be able to communicate with the alarm stations. Regulations permit the use of optical or electronic surveillance devices.

Discovery (time of)—the specific time at which the licensee or certificate holder determines that a verified degradation of a security safeguards measure, contingency situation, or reportable event exists.

Diversion of special nuclear material (SNM) (at any level)—the unauthorized removal or control of SNM from an NRC-licensed or -certified facility or authorized transport vehicle.

Enhanced weapons—any short-barreled shotgun, short-barreled rifle, or machine gun. Enhanced weapons do not include destructive devices as defined in 18 U.S.C. § 921(a). Enhanced weapons do not include standard weapons.

False alarm—an alarm generated without an apparent cause. Investigation discloses no evidence of a valid alarm condition, including tampering or nuisance alarm conditions, or an equipment malfunction.

High-level radioactive waste (HLW)—(1) the highly radioactive material resulting from the reprocessing of spent nuclear fuel, including liquid waste produced directly in reprocessing and any solid material derived from such liquid waste that contains fission products in sufficient concentrations; and (2) other highly radioactive material that the Commission, consistent with existing law, determines by rule requires permanent isolation.

Hostile action—an act directed against an NRC-licensed or -certified facility, or its personnel, that includes the use of violent force to destroy equipment, take hostages, or intimidate the licensee or certificate holder to achieve an end. This includes an attack by air, land, or water, using weapons, explosives, projectiles, vehicles, or other devices to deliver destructive force. This may also include other acts, not involving the use of overt violent force, such as tampering or covertly causing damage, that satisfy the overall intent of this term.

21

Hostile Action: An act toward a NPP or its personnel that includes the use of violent force to destroy equipment, take HOSTAGES, and/or intimidate the licensee to achieve an end. This includes attack by air, land, or water using guns, explosives, PROJECTILES, vehicles, or other devices used to deliver destructive force. Other acts that satisfy the overall intent may be included. HOSTILE ACTION should not be construed to include acts of civil disobedience or felonious acts that are not part of a concerted attack on the NPP. Non-terrorism-based EALs should be used to address such activities (i.e., this may include violent acts between individuals in the owner controlled area).

Comment [z10]: Suggest replacing this definition with the one below from NEI 03-12 and NEI 99-01 Rev 5, both of which have been endorsed by the NRC. This will allow for consistency between regulatory documents.

Formatted: Space Before: 0 pt

Formatted: Font: Bold

22

Hostile Force: One or more individuals who are engaged in a determined assault, overtly or by stealth and deception, equipped with suitable weapons capable of killing, maiming, or causing destruction.

Formatted: Font: Bold

23

Imminent: Mitigation actions have been ineffective, additional actions are not expected to be successful, and trended information indicates that the event or condition will occur.

Comment [z11]: Suggest adding this definition from NEI 03-12 and NEI 99-01 Rev 5, both of which have been endorsed by the NRC. This will allow for consistency between regulatory documents.

Formatted: Right: 0", Space Before: 0 pt, Widow/Orphan control, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Interruption of normal operation—a departure from normal operations or conditions that, if accomplished, would result in a challenge to the facility's safety, security, or emergency response systems. This may also include an event that causes a significant redistribution of security, safety, or emergency response resources. This could include intentional tampering with systems or equipment that is normally in a standby mode, but would need to operate if called upon in an abnormal or emergency situation. Section 236 of the AEA (42 U.S.C. § 2284) treats as sabotage the interruption of normal operation of any such facility through the unauthorized use of, or tampering with, the machinery, components, or controls of any such facility, or attempting or conspiring to carry out such an act.

Comment [z12]: Suggest adding this definition from NEI 03-12 and NEI 99-01 Rev 5, both of which have been endorsed by the NRC. This will allow for consistency between regulatory documents.

Items relied on for safety—means structures, systems, equipment, components, and activities of personnel [at SNM facilities licensed under 10 CFR Part 70] that are relied on to prevent potential accidents at a facility that could exceed the performance requirements in 10 CFR 70.61 or to mitigate their potential consequences. This does not limit the licensee from identifying additional structures, systems, equipment, components, or activities of personnel (i.e., beyond those in the minimum set necessary for compliance with the performance requirements) as items relied on for safety.

Loss of SNM—a failure to measure or account for SNM by the material control and accounting system approved for the facility, when the material is authorized to be possessed and is not confirmed to be stolen or diverted. This also means an accidental (i.e., unplanned) offsite release or dispersal of SNM, that is known or suspected to be 10 times greater than normal losses, or the discovery of empty or missing SNM containers or fuel elements.

Lost SNM—SNM that is no longer in the possession or control of the authorized licensee or certificate holder.

Malevolent intent—any perceptible actions, statements, observations, or circumstances that are considered by the licensee or certificate holder to indicate rancor, enmity, or a desire to cause harm. Any manifestations of harm or injury focused toward a licensee's or certificate holder's facility, personnel, equipment, or security systems is considered malevolent. This includes events demonstrating ill will, spite, or maliciousness (malice-in-fact).

Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA)—a document detailing the agreement between a licensee or certificate holder and any local law enforcement agencies (at all levels) or emergency service agencies (e.g., firefighting, decontamination, medical) to increase site security, safety, emergency response, or compensatory actions taken in response to onsite events (including, but not limited to, personnel, equipment, and professional assistance).

Nuisance alarm—a detection or monitoring system alarm generated by an identified input to a sensor or monitoring device that does not represent a safeguards threat and is not a result of normal authorized activity. Nuisance alarms may be caused by environmental conditions (e.g., rain, sleet, snow, lightening) or natural objects (e.g., animals or tall grass).

Properly compensated—measures, including backup equipment, additional security personnel, or specific procedures put in place to ensure that the effectiveness of the security system is not reduced by failure or other contingencies affecting the operation of the security-related equipment, structures, or processes. Preplanned compensatory measures are normally described in NRC-approved security plans and their associated implementing procedures.

Reason to believe—as mentioned in “credible threat,” a licensee or certificate holder may have reason to believe information received should be considered reliable when substantive information includes physical evidence supporting the threat, additional information independent of the threat, or the identification of a specific known group, organization, or individual that claims responsibility for the threat.

Reliable source—a source of information considered trustworthy or authentic, or that is consistent in performance or results.

Safeguards—the term “safeguards” historically refers to the two major components of NRC and international programs for the protection of special nuclear material. These programs include material control, material accounting, physical security, and information security functions. The

term “security” usually refers to physical or procedural means of protecting this special nuclear material, or the facility possessing such material, from malevolent acts. However, common usage frequently interchanges the terms “security” and “safeguards.” The NRC staff notes that under NRC regulations and guidance documents, the term “safeguards” may also have a specific contextual meaning, e.g., “Safeguards Information” in 10 CFR 73.21, 10 CFR 73.22, and 10 CFR 73.23, or “Safeguards Event Log” in 10 CFR 73.71 and Appendix G to Part 73.

Safeguards event log—a written or electronic compilation of entries for security events that meet the criteria described in paragraph III of Appendix G to 10 CFR Part 73,

Safety-related structures, systems, and components (SSCs)—for production and utilization facilities licensed under 10 CFR Part 50 or 10 CFR Part 52, those structures, systems, and components that are relied on to remain functional during and following design-basis events to ensure the integrity of the reactor coolant pressure boundary, the capability to shut down the reactor and maintain it in a safe shutdown condition, or the capability to prevent or mitigate the consequences of accidents that could result in a potential offsite exposure comparable to the guidelines in 10 CFR 50.34(a)(1).

25

Security Condition—Any Security Event as listed in the approved security contingency plan that constitutes a threat/compromise to site security, threat/risk to site personnel, or a potential degradation to the level of safety of the plant. A security condition does not involve a Hostile Action.

26

Security Event—any occurrence which incident represents an attempted, threatened, or actual breach of the security system; or a reduction in the physical protection program. Security Events may be Security Incidents, Security Conditions or Hostile Actions.

27

Security Incident—Any Security Event listed in the approved security contingency plan that may impact a security system, involve communication with LLEAs or draw media attention. A Security Incident does not involve a Security Condition or a Hostile Action.

Security-related SSCs—for the purposes of 10 CFR 73.71 and Appendix G to 10 CFR Part 73, those SSCs that the licensee or certificate holder would rely upon to implement the physical protection program, including the physical security plan, training and qualification plan, and safeguards contingency plan.

Security response—the licensee’s or certificate holder’s implementation of its armed response capabilities; or the request to local law enforcement for armed response or assistance.

Security system—the compilation of all elements in the physical protection program that are necessary to meet 10 CFR Part 73 requirements, including, but not limited to, equipment, procedures, and personnel practices.

Significant physical damage—physical damage that occurs to the licensee’s or certificate holder’s facility, equipment, transport vehicle or equipment, or reactor fuel, so that it is not able to perform its normal function (this applies to a power reactor, a facility possessing SSNM or its equipment, carrier equipment transporting nuclear or spent nuclear fuel (SNF), or the nuclear fuel or SNF that the facility or carrier possesses).

Spent nuclear fuel or spent fuel (SNF)—the nuclear fuel that has been withdrawn from a production, power, research, or test reactor following irradiation and that has not been chemically separated into its constituent elements by reprocessing. Spent fuel includes the special nuclear material, byproduct material, source material, and other radioactive materials associated with a fuel

Comment [z13]: Suggest adding this definition from NEI 03-12 and NEI 99-01 Rev 5, both of which have been endorsed by the NRC. This will allow for consistency between regulatory documents.

Formatted: Widow/Orphan control, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Comment [z14]: Suggest adding a newly defined term for events which are reportable but do not rise to the level of emergency classification as described in 10 CFR 50.47.

assembly.

Standard weapon—any handgun, rifle, shotgun, semiautomatic assault weapon, or a large capacity ammunition feeding device. Standard weapons do not include enhanced weapons.

Tampering—altering equipment, for improper purposes or in an improper manner, or intentional unauthorized manipulation of equipment. This may include deliberately damaging, disabling, or altering plant or security equipment specified in security plans. Tampering also refers to the unauthorized operation, manipulation of, or tampering with reactor controls or controls for other facilities belonging to licensees or certificate holders, or with safety-related SSCs or nonsafety-related SSCs.

Unaccounted for SNM—SNM that has not been received at its delivery point 4 hours or more after its estimated, expected arrival.

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 unauthorized manner, such as circumventing established access-control procedures by tailgating behind an authorized person.

Uncompensated—compensatory measures included in security plans or procedures that have either not been implemented, were ineffective, or were implemented incorrectly.

REFERENCES¹

1. 10 CFR Part 73, "Protection of Plants and Materials," U.S. Nuclear Regulatory Commission, Washington, DC.
2. 10 CFR 50.72, "Immediate Notification Requirements for Operating Power Reactors," U.S. Nuclear Regulatory Commission, Washington, DC.
3. 10 CFR 70.50, "Reporting Requirements," U.S. Nuclear Regulatory Commission, Washington, DC.
4. 10 CFR 72.75, "Reporting Requirements for Specific Events and Conditions," U.S. Nuclear Regulatory Commission, Washington, DC.
5. 10 CFR 76.120, "Reporting Requirements," U.S. Nuclear Regulatory Commission, Washington, DC.
6. Regulatory Guide 1.214, "Response Strategies for Potential Aircraft Threats," U.S. Nuclear Regulatory Commission, Washington, DC.
7. Regulatory Guide 5.71, "Cyber Security Program for Nuclear Facilities," U.S. Nuclear Regulatory Commission, Washington, DC.
8. "Terrorist Threats to the U.S. Homeland: Reporting Guide for Critical Infrastructure and Key Resource Owners and Operators," U.S. Department of Homeland Security, Washington, DC, January 24, 2005. ² [For Official Use Only]
9. 27 CFR 479.141, "Stolen or Lost Firearms," U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosives, Washington, DC.
10. Executive Order 13526 - Classified National Security Information Memorandum of December 29, 2009 - Implementation of the Executive Order "Classified National Security Information" Order of December 29, 2009 – Original Classification Authority, *Federal Register*, Volume 75, Number 2, pp. 705-731, January 5, 2010, Washington, DC.
11. 10 CFR Part 95, "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data," U.S. Nuclear Regulatory Commission, Washington, DC.
12. [Placeholder for revision to] NUREG-1304, Revision 1, "Reporting and Recording Safeguards Events," U.S. Nuclear Regulatory Commission, Washington, DC, (DATE subsequent to issuance of final rule).
13. NEI 99-01, Revision 5, "Methodology for Development of Emergency Action Levels," Nuclear Energy Institute, Washington DC
14. NEI 03-12, Revision x, "Generic Security Plan Template," Nuclear Energy Institute, Washington DC

Formatted: Space After: 12 pt

¹ Publicly available NRC published documents are available electronically through the Electronic Reading Room on the NRC's public Web site at: <http://www.nrc.gov/reading-rm/doc-collections/>. The documents can also be viewed on-line or printed for a fee in the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, MD; the mailing address is USNRC PDR, Washington, DC 20555; telephone 301-415-4737 or (800) 397-4209; fax (301) 415-

3548; and e-mail pdr.resource@nrc.gov.

- 2 Copies of the non-NRC documents included in these references may be obtained directly from the publishing organization.

13. 76 FR xxxx (10 CFR Part 73), "Proposed Rule—Enhanced Weapons, Firearms Background Checks, and Security Event Notifications," *Federal Register*, Volume 76, Number xxx, pages yyyy-zzzz, Month xx, 2011, Washington, DC.
14. 74 FR 13925 (10 CFR Parts 50, 52, 72, and 73), "Final Rule—Power Reactor Security Requirements," *Federal Register*, Volume 74, Number 58, pages 13925-13993, March 27, 2009, Washington, DC.
15. Regulatory Issue Summary 2009-10, "Communications Between the NRC and Reactor Licensees During Emergencies and Significant Events," U.S. Nuclear Regulatory Commission, Washington, DC, June 19, 2009.
16. 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," U.S. Nuclear Regulatory Commission, Washington, DC.
17. 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Washington, DC.
18. 10 CFR Part 60, "Disposal of High-Level Radioactive Waste in Geologic Repositories," U.S. Nuclear Regulatory Commission, Washington, DC.
19. 10 CFR Part 63, "Disposal of High-Level Radioactive Waste in a Geologic Repository at Yucca Mountain, Nevada," U.S. Nuclear Regulatory Commission, Washington, DC.
20. 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material," U.S. Nuclear Regulatory Commission, Washington, DC.
21. 10 CFR Part 72, "Licensing Requirements for the Independent Storage of Spent Nuclear Fuel, High-Level Radioactive Waste, and Reactor-Related Greater than Class C Waste," U.S. Nuclear Regulatory Commission, Washington, DC.
22. 10 CFR Part 76, "Certification of Gaseous Diffusion Plants," U.S. Nuclear Regulatory Commission, Washington, DC.
23. 10 CFR Part 95, "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data," U.S. Nuclear Regulatory Commission, Washington, DC.

SUPERSEDED REFERENCES

1. Bulletin 2005-02, "Emergency Preparedness and Response Actions for Security-Based Events," U.S. Nuclear Regulatory Commission, Washington, DC, July 18, 2005.
2. Regulatory Issue Summary 2006-12, "Endorsement of Nuclear Energy Institute Guidance 'Enhancements to Emergency Preparedness Program for Hostile Action,'" U.S. Nuclear Regulatory Commission, Washington, DC, July 19, 2006.
3. Generic Letter 1991-03, "Reporting of Safeguards Events," U.S. Nuclear Regulatory Commission, Washington, DC, March 6, 1991.
4. NUREG-1304, "Reporting of Safeguards Events," U.S. Nuclear Regulatory Commission, Washington, DC, February 1988.

APPENDIX A

REPORTING SUSPICIOUS AVIATION-RELATED ACTIVITIES AND COORDINATION WITH THE FEDERAL AVIATION ADMINISTRATION

The purpose of this appendix is to provide further guidance on (1) reporting of suspicious aviation-related activities (required to be reported in 4 hours) that occur within the airspace in proximity to a licensee's or certificate holder's facility; and (2) coordination with the Federal Aviation Administration (FAA). Suspicious activity is defined as behavior that may be indicative of intelligence-gathering or preoperational planning (surveillance) related to terrorism, criminal, espionage, or other illicit intentions. This appendix also provides guidance on activities that need not be reported.

In 2004, the FAA issued the following Notice to Airmen (NOTAM). This NOTAM advises pilots to avoid not only the airspace above or in proximity to U.S. nuclear power plants but also includes other key infrastructure facilities. The following is the published language contained in the most current NOTAM:

FDC 4/0811 FDC ... Special Notice ... This is a restatement of a previously issued advisory notice. In the interest of national security and to the extent practicable, pilots are strongly advised to avoid the airspace above, or in proximity to such sites as power plants (nuclear, hydro-electric, or coal), dams, refineries, industrial complexes, military facilities and other similar facilities. Pilots should not circle as to loiter in the vicinity over these types of facilities.

The NRC staff recommends that licensees and certificate holders contact their nearest FAA Air Traffic Control (ATC) facility to discuss this NOTAM and its relevance to their facility, and to maintain a rapport with ATC personnel. Information on FAA Air Traffic Organization, Air Traffic Control Towers, Terminal Radar Approach Control facilities, Air Route Traffic Control Centers, and Flight Standards District Offices are available on the FAA Web site at <http://www.faa.gov>.

Licensees and certificate holders should immediately report suspicious flight activity above, or in close proximity to, nuclear power plants and other NRC-licensed facilities to their local FAA ATC facility in an attempt to identify suspicious aircraft. Licensee and certificate holder security managers should exercise judgment and discretion in determining whether a flight activity is suspicious with respect to normal air traffic patterns, proximity of the facility to local airports and U.S. military bases, the use of rivers and coastal waterways for navigational purposes, local weather conditions, and other unforeseen local circumstances. However, licensees and certificate holders should report multiple sightings of the same commercial or general aviation aircraft, circling or loitering above or in close proximity to facilities, or photographing the facility or surrounding area.

To allow for effective followup of these events by law enforcement agencies, a licensee's or certificate holder's incident reporting should be timely and should include, to the extent available, key information on the aircraft (e.g., aircraft registration number (N-number), physical description of aircraft, observed flight activity, date and time of incident, altitude, and direction of flight). The use of special photographic or visual sighting equipment may enhance the ability to capture pertinent information more accurately. (Several Web sites are available to identify N-numbers: http://registry.faa.gov/aircraftinquiry/NNum_inquiry.asp, <http://registry.faa.gov/aircraftinquiry>, and <http://www.landings.com>.)

If contact with the local FAA facility results in a determination that the aircraft is associated with a municipal, State, or Federal entity, or if the FAA can provide a valid explanation for the flight deviation that satisfies the facility security manager, then the licensee or certificate holder should not report the flight activity further. However, if the FAA cannot identify the aircraft or provide a valid flight plan or explanation of activity, then the licensee or certificate holder should immediately report the suspicious flight activity to local law enforcement.

There is no need for a licensee or certificate holder to notify the NRC Headquarters Operations Center in the event of an aviation-related activity involving government aircraft unless the licensee or certificate holder deems the activity suspicious in nature and it cannot be resolved at the local level. Otherwise, licensees or certificate holders should report suspicious aviation-related activity and incidents to the NRC Headquarters Operations Center in accordance with 10 CFR 73.71 and Appendix G. The NRC continues to work closely with FAA, the Transportation Security Administration, the U.S. Northern Command, and the North American Aerospace Defense Command, with respect to these types of suspicious aviation incidents, and will conduct additional coordination, if necessary.

Licensees and certificate holders should contact and coordinate with the following organizations with respect to suspicious aviation-related activities or incidents, in this order of priority:

1. their local FAA ATC facility or office,
2. their local law enforcement agency, and
3. the NRC Headquarters Operations Center, in accordance with 10 CFR 73.71.

The NRC will continue to forward information it has received on precoordinated overflight operations to affected licensees and certificate holders (e.g., waterfowl surveillance operations, power line surveys).

Licensees and certificate holders should contact organizations (i.e., military, government, and private sector) in their local area that could conduct aircraft operations in airspace over or near their facility, to coordinate and establish a link for advance notification of upcoming activity and for verification of ongoing activity that was not previously coordinated.

Gallagher, Carol

Comment Submission No. 14
(ML11220A087)

From: Moore, Jerry W. (Vogtle) [JEWMOORE@southernco.com]
Sent: Thursday, August 04, 2011 7:36 AM
To: Gallagher, Carol
Subject: Draft Reg Guide Recommendation / Comment

I am a nuclear security firearms instructor at Plant Vogtle. Just a small recommendation to assist if you feel it is applicable referencing NRC-2011-0015 (DG-5020) while it is in draft format.

(Comment-Response Document Abbreviation: JM)

DG-5020, Section 8, Page 19... Recommend addition:

1 Security Training Firearms Instructors must be trained or certified by a State or nationally recognized entity for each enhanced weapon for which the individual will be providing instruction and this is consistent with Reg Guide 5.75.

Reason: This would enhance consistency and act as a reminder to those who may not remember the previous guidance on standard weapons as well as the new guide on enhanced weapons.

Thank you...

Jerry Moore
Plant Training Instructor
Vogtle Security
706.826.3742

2/03/2011
76 FR 6086

2

RECEIVED

2011 AUG -4 PM 4:45

RULES AND REGULATIONS
DIVISION

SUNSI Review Complete
Template = ADM-013

1
E-RIDS = ADM-03
Add = R. Carpenter (VGE1)
m. Ouse (m5c)
P. Brachman (P96)

2/03/2011
76FR 6085

Comment Submission No. 15
(ML11221A139)

Mendiola, Doris

From: Dimitriadis, Anthony
Sent: Friday, August 05, 2011 4:23 PM
To: Brochman, Phil
Cc: NRCREP Resource; Trapp, James; Wastler, Sandra
Subject: Comment on Draft Reg Guide DG-5019, Rev 1

4

RECEIVED

2011-08-05 21:11:26

REGIONS

Good Afternoon: (Comment-Response Document Abbreviation: AD)

Section 2.3.1 of Draft Regulatory Guide DG-5019 discusses the current and proposed reporting requirements applicable in part to licensees subject to 10 CFR 73.55.

The current Notification requirements listed in Appendix G to Part 73, (c) discusses "Contraband events".

Specifically, the current requirement and the proposed requirement regarding the attempted introduction of contraband makes it a One-hour notification if the person had malevolent intent to enter the PA, VA, etc.

The current Draft Regulatory Guide outlines examples of Reportable Events in section 2.3.2. Section (h) expounds on the issue of "actual or attempted introduction of contraband material (e.g., unauthorized weapons, explosives, or incendiaries) and lists in section (h)(2) the following: "If the licensee or certificate holder concludes, within an hour, that the entry of the contraband was inadvertent and did not threaten facility security, they may record this event in the safeguards event log."

[1] As a security inspector in Region 1, I have first-hand knowledge of at least two instances where contraband (unauthorized weapons) was either attempted or introduced into the protected area of two different reactor sites in 2010. I believe that the language which permits the licensee or certificate holder to investigate and determine whether the attempted or actual entry into the PA should be deleted. I believe that the licensees should report such an event to the NRC headquarters operations officer within One-hour regardless of the intent of the individual introducing contraband.

[2] The NRC staff encourages licensees to report security notifications and subsequently retract them, if appropriate, rather than wait for an internal investigation to be conducted and a determination of whether "malevolent intent" was present. For example, take into consideration the events of September 11, 2001, where numerous adversaries boarded 5 separate flights at 5 different airports, bypassing security at those airports. There were multiple adversaries in multiple In a similar fashion, it is not unthinkable for adversaries to present a challenge to 5 or even 10 different reactor sites where they attempt to introduce contraband on the same day in the hopes of committing: either a feeling of terror, or an attempt at radiological sabotage. If the current reporting requirement stands, and permits licensees to assess whether the individual attempting to introduce contraband into a given protected area, there will likely be a significant delay in determining whether "malevolent intent" was present. This could prevent the NRC from rapidly communicating this information to other NRC licensees, from notifying law enforcement authorities, and the intelligence community of such events in a timely fashion. This would defeat the entire purpose of the reportability requirements, as intended by the NRC staff.

[3] As outlined in the introduction to the Draft Regulatory Guide, the licensees or certificate holder should not consider security events reported under this guide (or in the regulation) as indicative of performance failures. In the example I listed above, the discovery of contraband at the search train at a given site would be viewed as a case where the system worked in the way it was supposed to work. This would be a success. The intent of the notification of such an event is to simply have the NRC receive information early in order to be the central clearing house of such information so that the staff can assess the information as part of a larger pool of incoming notifications to be in a better position to make an intelligent decision on whether the event is unique to one plant, or if there is a pattern that clearly indicates that the nuclear infrastructure is under a coordinated attack.

SUNSI Review Complete
Template = ADM-013

1

E-RIDS = ADM-03
Add = R. Carpenter (RCE1)
m. crew (m. sc) - P. Brochman (P96)

- 4 I strongly believe that the attempted introduction of contraband into any reactor site should be reported within One Hour regardless of other circumstances.

Respectfully submitted,

Anthony Dimitriadis
Senior Physical Security Inspector



US NRC Region I
475 Allendale Road
King of Prussia, PA 19406
Telephone: 610-337-6953
Cell Phone: 484-919-8349
Fax: 610-337-5320
E-mail: Anthony.Dimitriadis@nrc.gov

1

PUBLIC SUBMISSION

As of: January 30, 2013
Received: January 25, 2013
Status: Pending_Post
Tracking No. lxx-83ba-uw7v
Comments Due: February 25, 2013
Submission Type: Web

Docket: NRC-2011-0018
Enhanced Weapons, Firearms Background Checks, and Security Event Notifications

Comment On: NRC-2011-0018-0028
Enhanced Weapons, Firearms Background Checks, and Security Event Notifications

Document: NRC-2011-0018-DRAFT-0030
Comment on FR Doc # 2013-00237

DOCKETED
USNRC
January 30, 2013 (9:16 a.m.)
OFFICE OF THE SECRETARY
RULEMAKINGS AND
ADJUDICATIONS STAFF

**Note: This was the only comment submission on the 1st
Supplemental Proposed Rule issued on January 10, 2013.**

Submitter Information

Name: Michael DeAngelo (Comment-Response Document Abbreviation: MD)
Address:
111 Koehler Street
Pittsburgh, Pennsylvania, 15223

General Comment

- 1 I think strict gun control is just what this country needs.. Look how the regulations on drugs have influenced drug trafficking.
Oops sorry that didn't work either.
But this is a proposed rule, and not a law. Laws are made to be broken in the good old US of A.
But a PROPOSED RULE!!! The people who shouldn't have guns, like criminals, will really be scared of this one.

SECY-067

DS10

RulemakingComments Resource

From: Gallagher, Carol
Sent: Wednesday, January 30, 2013 9:16 AM
To: RulemakingComments Resource
Subject: Comment on Enhanced Weapons, Firearms Background Checks, and Security Event Notifications
Attachments: NRC-2011-0018-DRAFT-0030.pdf

Attached for docketing is a comment on the above noted proposed rule (78 FR 2214; January 10, 2013) from Michael DeAngelo that I received via the regulations.gov website on January 25, 2013.

Thanks,
Carol

DAVID R. KLINE
Director, Security

1201 F Street, NW, Suite 1100
Washington, DC 20004
P: 202.739.8174
dk@nei.org
nei.org

Note: This was the 1st comment submission on the 2nd Supplemental Proposed Rule issued on September 22, 2015.

December 7, 2015 (Comment-Response Document Abbreviation: NEI2)

Ms. Annette L. Vietti-Cook
Secretary
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
ATTN: Rulemakings and Adjudications Staff

Subject: Supplemental Proposed Rule: Enhanced Weapons, Firearms Background Checks, and Security Event Notifications (10 CFR Part 73; RIN-3150-AI49) (Docket ID NRC-2011-0018)

Project Number: 689

Dear Ms. Vietti-Cook:

The Nuclear Energy Institute (NEI)¹ appreciates the opportunity to review and participate in discussion regarding the Supplemental Proposed Rule for Enhanced Weapons, Firearms Background Checks, and Security Event Notifications. The industry believes the revised requirements more effectively address the needs of both the industry and the Nuclear Regulatory Commission.

1 NEI has identified one issue associated with implementation of this rule. §73.18(s)(3) requires affected licensees to update any procedures, instructions and training materials within 60 days after the effective date of the rule. §73.19(b) requires that affected licensees "...must establish a Firearms Background Check Plan." Further, "Licensees and certificate holders must establish this plan as part of their overall NRC-approved Training and Qualification plan...." The nuclear power industry has incorporated an NRC-approved, industry standard NEI template for the Physical Security Plan, Security Training and Qualification Plan, Security Contingency Plan, and Independent Spent Fuel Storage Installation (ISFSI) Security Program. Formal revision of this template cannot be effected until final rule language is published. The template must

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

Ms. Annette L. Vietti-Cook

December 7, 2015

Page 2

then be reviewed and approved by the industry and then submitted to the NRC for endorsement. Based on historic examples, a more reasonable time frame for meeting this objective would be 9-months.

If you have any questions or concerns, please contact Dick Speer at (202) 739-8121; rjs@nei.org or me.

Sincerely,

A handwritten signature in black ink, appearing to read "David R. Kline". The signature is stylized with a large "D" and "K".

David R. Kline

c: Ms. Sandi L. Wastler, NSIR/DSP/MWSB, NRC
Mr. Philip G. Brochman, NSIR/DSP/MWSB, NRC
NRC Document Control Desk

7 December 2015

**Note: This was the 2nd comment submission on the 2nd
Supplemental Proposed Rule issued on September 22, 2015.**

Secretary, US Nuclear Regulatory Commission **(Comment-Response Document Abbreviation: SH2)**

Subject: Comments on Proposed Rule (Docket ID NRC-2011-0015 and NRC-2011-0018)

I would like to continue register my support for the NRC's efforts to issue a rule to increase the weaponry available to NRC licensees to protect Americans from acts of terrorism. However, I would like to suggest two items in the proposed rule that are in error and one item that should be improved to increase the capability of the NRC's final rule.

1

First, in 10 CFR 73.19(b)(1) licensees who apply for "stand-alone preemption authority or combined enhanced weapons authority and preemption authority" must establish a firearms background check plan. However, in 10 CFR 73.19(r) no mention is made of developing a firearms background check plan for those licensees who were previously issued orders designating them as eligible to apply for Section 161A authority; and are now transitioning to the final rule. In Designation Order EA-13-092, Attachment 3, the NRC did not specify any requirement for developing a firearms background check plan (see 78 FR 35984; 14 Jun 2013). Therefore, I believe 10 CFR 73.19(r) should be changed to indicate that licensees shifting from orders to the new regulations must also develop a firearms background check plan.

2

Second, in 10 CFR 73.19(r)(3) licensees have 60 days to develop "procedures, instructions, and training material." However, I believe this length of time is insufficient for these affected licensees to develop a firearms background check plan after the final rule is issued. Consequently, I believe the NRC should change this provision to a longer period of time. Development of a firearms background check plan meeting the requirements of 10 CFR 73.19(b) is more complex than updating procedures, instructions, and training material. Therefore, I would suggest 4 months is more appropriate, for this more complex task.

3

Finally, I believe the NRC should take advantage of this current rulemaking opportunity to include stand-alone spent fuel storage facilities and transportation of spent fuel within the classes of designated facilities and activities in 10 CFR 73.18(c). In the NRC's supplemental proposed rule in 2013, the NRC proposed to add only at-reactor ISFSIs [independent spent fuel storage installations]. However, since the NRC's proposed action in 2013, objective reality has changed with two separate firms indicating they intend to apply for Part 72 licenses for centralized spent fuel storage installations. In public meetings and public conferences with the NRC, these firms indicated they would submit applications in 2016 to obtain licenses. The firms also indicated that these two facilities could receive 3000 to 4000 shipments each of spent fuel. This information should be considered by the NRC in the final rule.

The NRC in the 2013 proposed rule has indicated that facilities storing spent fuel are appropriate for Section 161A authority. Consequently, I believe such a change to include stand-alone ISFSIs is consistent with the scope of this rulemaking. Secondly, since the NRC has indicated that facilities at each end of the transportation transaction are appropriate for Section 161A authority (i.e., the reactor facility shipping the spent fuel and a central ISFSI receiving the spent fuel), then the spent fuel during transportation is also appropriate for Section 161A authority and should be considered within the scope of this overall rulemaking effort. Addressing this issue in the final rule would be both more effective and efficient for the NRC and would also support a national strategy for moving shutdown reactors to central ISFSIs.

S. Hardin, Mt. Airy, MD