ANTHONY R. PIETRANGELO
Senior Vice President and
Chief Nuclear Officer

1201 F Street, NW, Suite 1100
Washington, DC 20004
P: 202.739.8081
arp@nei.org
nei.org

NUCLEAR ENERGY INSTITUTE

January 15, 2015

The Honorable Stephen G. Burns
Chairman
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Cyber Security Event Notifications Final Rule (SECY-14-0129)

Project number: 689

Dear Chairman Burns:

The Nuclear Energy Institute (NEI)[1] understands the Commission is considering final action on proposed cyber security event notifications requirements (SECY-14-0129). On behalf of the commercial nuclear industry, NEI requests that the Commission not approve issuance of the final rule for the following reasons: new requirements are unnecessary given existing event notification requirements and guidance; the rule could result in a substantial number of nuisance reports; and, the rule is unnecessarily burdensome given the overly broad scope of the current cyber security requirements.

Each power reactor subject to the NRC's cyber security requirements is also subject to the requirements in Appendix G to 10 CFR Part 73, "Reportable Safeguards Events." These reporting requirements are sufficient because they do not address the method of attack (e.g., cyber versus physical), but rather focus on the potential impact to safety and security. For example, 10 CFR 73, Appendix G, Section (I)(a) requires licensees to report to the NRC within one hour of discovery of an event in which there is reason to believe that a person has committed, attempted, or has made a credible threat to commit or cause significant physical damage to a power reactor or its equipment, or interruption of normal operation. We believe that a cyber attack would clearly be reportable under this existing rule language.

[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.

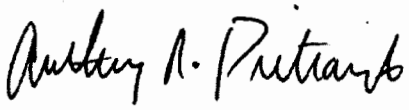
Also, Information Advisory (IA) 13-01 provides guidelines for reporting suspicious cyber security activity and events that may be used to support compliance with existing security event reporting requirements.

Based on how certain provisions of the new rule are interpreted, licensees may make large numbers of reports that would later be retracted – a nuisance for both the industry and the NRC. Appendix G to Part 73 requires events to be reported within one hour of discovery. In practice, licensees "discover" an event after a determination has been made that a safeguards event has occurred and that it meets reporting requirements. In the Public Comment Analysis for the new rule, the NRC states, "internal notifications and gathering information to make a determination as to whether it meets applicable reporting requirements could take several hours, or even days, depending on the amount of information needed to reach a conclusion. The time to report an event is upon recognition; the licensee can withdraw a report (based on subsequent analysis of the circumstances)..." NEI contends that this new interpretation is a deviation from established reporting practices. For the notification to have value in a cyber security context, it should be made when it can be confirmed that the event was caused by a cyber attack. If the equipment involved was significant from a safety perspective, a notification would have previously been made in accordance with 10 CFR 50.72.

The NRC's cyber security rule provides the programmatic requirements to defend against the design basis threat of radiological sabotage, as well as to protect systems and equipment that do not have a nexus to radiological sabotage. NEI has submitted a petition for rulemaking (PRM-73-18) to address this inconsistency in the cyber rule language with the physical security rule language. The proposed cyber security event notification requirements duplicate the overly broad scoping language that is the subject of NEI's petition, and as a result would require licensees to report events related to systems and equipment that have no nexus to radiological sabotage. NEI understands that licensees have many hundreds to a few thousand digital assets included within their cyber security programs. Accordingly, NEI contends that licensees could report large numbers of events to the NRC related to equipment that has no nexus to radiological sabotage. The numbers of reports would likely exceed the frequencies used in the regulatory analysis for the proposed rule, and would be unnecessarily burdensome to both NRC and the industry.

In summary, the industry believes the final rule should not be issued since the proposed requirements are unnecessary given existing security event notification requirements and guidance, could result in nuisance reporting and would be unnecessarily burdensome.

Sincerely,



Anthony R. Pietrangelo

c: The Honorable Kristine L. Svinicki, COMM/OCMKS, NRC
The Honorable William C. Ostendorff, COMM/OCMWO, NRC
The Honorable Jeff M. Baran, COMM/OCMJB, NRC
Mr. Mark A. Satorius, EDO, NRC
Mr. Michael R. Johnson, DEDO, NRC
Mr. James T. Wiggins, NSIR, NRC
NRC Document Control Desk

CHAIRMAN Resource

From: PIETRANGELO, Tony <arp@nei.org>

Sent: Thursday, January 15, 2015 9:31 AM
To: CHAIRMAN Resource
Cc: CMRSVINICKI Resource; CMROSTENDORFF Resource; CMRBARAN Resource; Satorius, Mark; Johnson, Michael; Wiggins, Jim
Subject: Cyber Security Event Notifications Final Rule (SECY-14-0129)
Attachments: 01-15-15_NRC_Cyber Security Event Notifications Final Rule.pdf

January 15, 2015

The Honorable Stephen G. Burns
Chairman
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Cyber Security Event Notifications Final Rule (SECY-14-0129)

Project number: 689

Dear Chairman Burns:

The Nuclear Energy Institute (NEI)[1] understands the Commission is considering final action on proposed cyber security event notifications requirements (SECY-14-0129). On behalf of the commercial nuclear industry, NEI requests that the Commission not approve issuance of the final rule for the following reasons: new requirements are unnecessary given existing event notification requirements and guidance; the rule could result in a substantial number of nuisance reports; and, the rule is unnecessarily burdensome given the overly broad scope of the current cyber security requirements.

Each power reactor subject to the NRC's cyber security requirements is also subject to the requirements in Appendix G to 10 CFR Part 73, "Reportable Safeguards Events." These reporting requirements are sufficient because they do not address the method of attack (e.g., cyber versus physical), but rather focus on the potential impact to safety and security. For example, 10 CFR 73, Appendix G, Section (I)(a) requires licensees to report to the NRC within one hour of discovery of an event in which there is reason to believe that a person has committed, attempted, or has made a credible threat to commit or cause significant physical damage to a power reactor or its equipment, or interruption of normal operation. We believe that a cyber attack would clearly be reportable under this existing rule language. Also, Information Advisory (IA) 13-01 provides guidelines for reporting suspicious cyber security activity and events that may be used to support compliance with existing security event reporting requirements.

Based on how certain provisions of the new rule are interpreted, licensees may make large numbers of reports that would later be retracted – a nuisance for both the industry and the NRC. Appendix G to Part 73 requires events to be reported within one hour of discovery. In practice, licensees "discover" an event after a determination has been made that a safeguards event has occurred and that it meets reporting requirements. In the Public Comment Analysis for the new rule, the NRC states, "internal notifications and gathering information to make a determination as to whether it meets applicable reporting requirements could take several hours, or even days, depending on the amount of information needed to reach a conclusion. The time to report an event is upon recognition; the licensee

can withdraw a report (based on subsequent analysis of the circumstances)..." NEI contends that this new interpretation is a deviation from established reporting practices. For the notification to have value in a cyber security context, it should be made when it can be confirmed that the event was caused by a cyber attack. If the equipment involved was significant from a safety perspective, a notification would have previously been made in accordance with 10 CFR 50.72.

The NRC's cyber security rule provides the programmatic requirements to defend against the design basis threat of radiological sabotage, as well as to protect systems and equipment that do not have a nexus to radiological sabotage. NEI has submitted a petition for rulemaking (PRM-73-18) to address this inconsistency in the cyber rule language with the physical security rule language. The proposed cyber security event notification requirements duplicate the overly broad scoping language that is the subject of NEI's petition, and as a result would require licensees to report events related to systems and equipment that have no nexus to radiological sabotage. NEI understands that licensees have many hundreds to a few thousand digital assets included within their cyber security programs. Accordingly, NEI contends that licensees could report large numbers of events to the NRC related to equipment that has no nexus to radiological sabotage. The numbers of reports would likely exceed the frequencies used in the regulatory analysis for the proposed rule, and would be unnecessarily burdensome to both NRC and the industry.

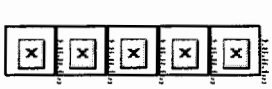
In summary, the industry believes the final rule should not be issued since the proposed requirements are unnecessary given existing security event notification requirements and guidance, could result in nuisance reporting and would be unnecessarily burdensome.

Sincerely,

Anthony R. Pietrangelo
Senior Vice President and Chief Nuclear Officer

Nuclear Energy Institute
1201 F Street NW, Suite 1100
Washington, DC 20004
www.nei.org

P: 202.739.8081
M: 202.439.2511
E: arp@nei.org



Sent through www.intermedia.com

---

[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.