

January 3, 2007 (10:21am)

OFFICE OF SECRETARY  
RULEMAKINGS AND  
ADJUDICATIONS STAFF



NUCLEAR ENERGY INSTITUTE

Douglas J. Walters  
SENIOR DIRECTOR, SECURITY  
NUCLEAR GENERATION DIVISION

January 2, 2007

2

Ms. Annette Vietti-Cook  
Secretary  
U.S. Nuclear Regulatory Commission  
Mail Stop O-16C1  
Washington, DC 20555-0001

Attention: Rulemakings and Adjudications Staff

Subject: Comments on the Proposed Rule, *Protection of Safeguards Information*, (71 Fed. Reg. 64004; October 31, 2006), RIN 3150-AH57)

Dear Ms. Vietti-Cook:

On behalf of the commercial nuclear energy industry, the Nuclear Energy Institute (NEI)<sup>1</sup> provides the following comments on the Proposed Rule, *Protection of Safeguards Information*.

The industry agrees with the U.S. Nuclear Regulatory Commission (NRC) that information concerning the security of the nation's nuclear facilities must be protected from inadvertent release or unauthorized disclosure. The tragic events of September 11, 2001, brought new focus on the need to protect this type of information in the broader public interest by, among other things, ensuring that only individuals, who have demonstrated trustworthiness and reliability, as well as demonstrating a need to know specific information, are allowed access to this type of information. Power reactors licensees have excellent controls on Safeguards Information already and other licensees have also begun implementing the necessary controls as a result of NRC

---

<sup>1</sup> 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 plants designers, major architect/engineering firms, fuel fabrication facilities, materials licensees, and other organizations and individuals involved in the nuclear energy industry.

Template = SECY-067

SECY-02

Ms. Annette Vietti-Cook  
Secretary, U.S. Nuclear Regulatory Commission  
January 2, 2007  
Page 2

orders. Consequently, Safeguards Information is already subject to considerable control.

Notwithstanding our strong support for ensuring that necessary protections are in place for security sensitive information, we have three major concerns with the proposed rule which are summarized below. Detailed comments on specific provisions in the proposed rule are provided as Enclosure 1.

#### Draft Regulatory Analysis and Backfit Analysis

Our first concern is the draft regulatory analysis referenced in Section X of the Federal Register Notice. The analysis is flawed in that it states on Page 37 that the proposed rule will be implemented in fiscal 2005 and fiscal 2006. The earliest it could possibly be implemented is fiscal 2007. Also, it uses 2005 dollars in the various analyses rather than the appropriate 2007 dollars.

Further, both the Regulatory Analysis and the Backfit Analysis completely ignore the substantial cost to power reactor licensees of the ten year review required by the proposed § 73.22(h). The Regulatory Analysis incorrectly estimates no costs for power reactors to modify their SGI programs while acknowledging significant cost expenditures to train staff about the modified SGI program. The Regulatory Analysis concludes that "Although significant costs are incurred as a result of the proposed rule, the qualitative benefits outweigh its costs." The NRC should provide some quantitative evidence which supports the qualitative conclusion. For instance why will the nation be safer with those transporting radioactive materials marking documents to suit both NRC and DOT regulations? How much of the material which is newly protected by the proposed rule has the NRC found released to the public due to lack of controls imposed by the proposed rule?

This rulemaking should be delayed until an accurate Regulatory Analysis and Backfit Analysis are completed. The analyses should consider the actual substantial cost of rule implementation regarding power reactor licensee costs to modify SGI programs and the significant costs of the ten year review required by the proposed § 73.22(h).

#### Implementation Period

The industry's second major concern is the proposed rule's implementation period. At 71 FR 64001 NRC notes that "This revised proposed rule reflects orders already imposed by the Commission and would expand the types of

security information covered by § 73.2. Considering the scope of the rule, the Commission proposes to set an effective date for the final rule of 90 days from publication in the Federal Register.” While it is true that NRC has issued a series of orders to various classes of licensees, the proposed rule contains many new requirements that will take more than 90 days to implement.

For instance, NRC issued orders to non-power reactor licensees (for example at 71 FR 59140) requiring fingerprinting for SGI access. However, the proposed rule goes beyond the orders and will require a comprehensive background check. As a result, hundreds of licensees will have to develop, implement and maintain comprehensive background check programs. There is a limited infrastructure in the nation capable of performing the comprehensive background checks and that infrastructure is already heavily loaded. This type of comprehensive background check program requires significant resources to develop and administer, as demonstrated by the programs that have long existed at nuclear power reactors. Based on that experience, an implementation time frame of at least a year would be appropriate to implement such a program at many licensee sites.

For power reactor licensees the proposed rule has many requirements not contained in any previously issued orders as evidenced by the fact the Federal Register Notice uses 14 pages to describe only the changes in 10 CFR 73 from the previously proposed rule. Many of these changes will require updates of existing procedures. The new definitions in § 73.2, for example, will require licensees to revise procedures to match. The mere reorganization of the rule from §73.21 only, to §§ 73.21, 73.22, and 73.23 will likewise need to be updated in procedures. After the procedures are revised and approved for use, training must be developed and then individuals who handle SGI must be trained. Similar to other classes of licensees, for power reactors an implementation time frame of at least a year would be appropriate to implement the proposed changes.

#### Conflict with 49 CFR 15

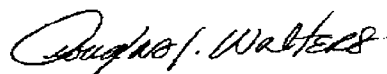
The third major concern is that the proposed 10 CFR 73.23 conflicts with the existing requirements contained in 49 CFR 15, *Protection of Sensitive Security Information*, regarding the protection of information associated with the transportation of certain types and quantities of radioactive materials. This results in licensees transporting nuclear material contending with two separate information protection regulations for some of the same information. As stated in our comments on the previous version of this rulemaking, we strongly recommend the NRC and the Department of Transportation develop

Ms. Annette Vietti-Cook  
Secretary, U.S. Nuclear Regulatory Commission  
January 2, 2007  
Page 4

a coordinated rulemaking to provide a stable regulatory framework for all involved stakeholders.

We appreciate the NRC's consideration of the industry's comments on the proposed rule. Although we share the NRC's interest in making sure that security-related information is properly protected, we believe that the NRC can satisfy that need in ways that do not pose unwarranted burdens on NRC licensees. If any further information is desired, please contact John Rycyna at 202.739.8127 or me.

Sincerely,

A handwritten signature in cursive script that reads "Douglas J. Walters".

Douglas J. Walters

Enclosure

c: Ms. Trish Holahan, NRC

**NEI January 2 Comments on the Proposed Rule, *Protection of Safeguards Information***

**1. Definition of Safeguards Information in Part 2**

**Discussion:** For purposes of Part 2, documents should be considered Safeguards Information if they have been designated as Safeguards Information in accordance with Part 73. In the event of any dispute about whether a document that has been designated as Safeguards Information should nevertheless be disclosed, the presiding officer must determine whether the person seeking disclosure should be granted access to the Safeguards Information – i.e., has a need to know and is trustworthy and reliable. The presiding officer should not consider whether the information in the document meets the definition of Safeguards Information. If the definition of Safeguards Information in Part 2 is the same as the definition in Part 73, it will appear that parties may seek a determination by the presiding officer on whether the information meets that definition.

It is clear from proposed §§ 2.336(f)(1), 2.705, 2.709 and 2.1010, which specify the grounds for a presiding officer to issue an order requiring disclosure of Safeguards Information, that a presiding officer would not be authorized to issue such an order on the grounds that the information does not meet the definition of Safeguards Information. This is appropriate and should not be changed because presiding officers generally are not inherently qualified to determine whether information meets the definition of Safeguards Information.

**Reference:** Proposed § 2.4 *Safeguards Information* provides the same definition of Safeguards Information as proposed § 73.2 *Safeguards Information*.

**Recommendation:** Modify § 2.4 *Safeguards Information* to state “*Safeguards Information* means information that has been determined to be Safeguards Information in accordance with 10 CFR 73.21-23.”

**2. Review of Adverse Ruling on Trustworthiness and Reliability.**

**Discussion:** The procedure specified in § 2.336(f)(1)(iv) for review of an adverse ruling on a party’s trustworthiness and reliability should avoid any appearance of biasing the proceeding. There may be an appearance of bias if the review is conducted by the presiding officer. Such a review would require the presiding officer to consider personal information about the party, its

attorney or consultant/expert witness to determine whether the person is trustworthy and reliable for purposes of having access to Safeguards Information, and might later be called upon to decide the merits of contention based on other considerations, potentially including the credibility and persuasiveness of witnesses and advocates. In such circumstances, questions may be raised about whether these judgments were improperly affected by personal information. It would be equally efficient, and avoid any appearance of bias to require that all requests for review be presented to the Chairman of the Atomic Safety and Licensing Board Panel for designation of an officer other than the presiding officer to review the adverse determination. Moreover, such a process would reduce the risk that the need to consider such a review would prevent the presiding officer from keeping the proceeding on schedule.

**Reference:** Section § 2.336(f)(1)(iv) states that: “(iv) Participants, potential witnesses, and attorneys for whom the NRC Office of Administration has made a final adverse determination on trustworthiness and reliability may request the presiding officer to review the adverse determination. The request may also seek to have the Chairman of the Atomic Safety and Licensing Board Panel designate an officer other than the presiding officer of the proceeding to review the adverse determination. For purposes of review, the adverse determination must be in writing and set forth the grounds for the determination. The request for review shall be served on the NRC staff and may include additional information for review by the presiding officer. The request must be filed within 15 days after receipt of the adverse determination by the person against whom the adverse determination has been made. Within 10 days of receipt of the request for review and any additional information, the NRC staff will file a response indicating whether the request and additional information has caused the NRC Office of Administration to reverse its adverse determination. The presiding officer may reverse the Office of Administration’s final adverse determination only if the officer finds, based on all the information submitted, that the adverse determination constitutes an abuse of discretion. The presiding officer’s decision must be rendered within 15 days after receipt of the staff filing indicating that the request for review and additional information has not changed the NRC Office of Administration’s adverse determination.”

**Recommendation:** Revise § 2.336(f)(i)(iv) to state: “(iv) Participants, potential witnesses, and attorneys for whom the NRC Office of Administration has made a final adverse determination on trustworthiness and reliability may request the Chairman of the Atomic Safety and Licensing Board Panel to designate an officer other than the presiding officer of the proceeding to review the adverse determination. For purposes of review, the adverse determination must be in writing and set forth the grounds for the

determination. The request for review shall be served on the NRC staff and may include additional information for review by the designated officer. The request must be filed within 15 days after receipt of the adverse determination by the person against whom the adverse determination has been made. Within 10 days of receipt of the request for review and any additional information, the NRC staff will file a response indicating whether the request and additional information has caused the NRC Office of Administration to reverse its adverse determination. The designated officer may reverse the Office of Administration's final adverse determination only if the officer finds, based on all the information submitted that the adverse determination constitutes an abuse of discretion. The designated officer's decision must be rendered within 15 days after receipt of the staff filing indicating that the request for review and additional information has not changed the NRC Office of Administration's adverse determination."

### **3. Civil Penalty for Violation of a Protective Order**

**Discussion:** The provisions concerning civil penalties are appropriate for violations that involve the disclosure of Safeguards Information that by order is prohibited from being disclosed. In contrast, a violation of an order requiring disclosure of Safeguards Information should be subject only to the same penalties that would apply for violation of an order that requires disclosure of other types of information. The regulation regarding the potential for civil penalties for violation of an order should be clearly limited to disclosure of Safeguards Information in violation of provisions of an order that are imposed for the purpose of preventing unauthorized disclosure of Safeguards Information.

**Reference:** Proposed 10 CFR §§ 2.336(f)(5), 2.705(c)(5), 2.709(f)(5), and 2.1010(b)(6)(v) state that: "In addition to any other sanction that may be imposed by the presiding officer for violation of an order issued pursuant to this paragraph, violation of an order pertaining to the disclosure of Safeguards Information protected from disclosure under Section 147 of the Atomic Energy Act, as amended, may be subject to a civil penalty imposed under § 2.205."

**Recommendation:** Revise proposed §§ 2.336(f)(5), 2.705(c)(5), 2.709(f)(5) and 2.1010(b)(6)(v) to state that: "In addition to any other sanction that may be imposed by the presiding officer for violation of an order issued pursuant to this paragraph, disclosure of Safeguards Information in violation of limitations on such disclosure in an order pertaining to the disclosure of Safeguards Information may be subject to a civil penalty imposed under § 2.205."

#### 4. Criminal Penalty for Violation of a Protective Order

**Discussion:** Any provision concerning potential criminal penalties for violation of an order concerning disclosure of Safeguards Information should clearly state that any such penalty would be based on disclosure of Safeguards Information in violation of an order imposing limits on such disclosure. It should be clear that the criminal penalty provisions would not apply to violations of orders of presiding officers that impose obligations or limitations other than limitations imposed for the purpose of preventing disclosure of Safeguards Information to unauthorized persons.

**Reference:** Proposed §§ 2.336(f)(6), 2.705(c)(7), 2.70(f)(6) and 2.1010(b)(6)(vi) state that: “For the purpose of imposing the criminal penalties contained in Section 223 of the Atomic Energy Act, as amended, any order issued pursuant to this paragraph with respect to Safeguards Information is considered to be an order issued under Section 161b of the Atomic Energy Act.”

**Recommendation:** Revise §§ 2.336(f)(6), 2.705(c)(7), 2.709(f)(6) and 2.1010(b)(6)(vi) to state that: “For the purpose of imposing the criminal penalties contained in Section 223 of the Atomic Energy Act, as amended, a limitation on the disclosure of Safeguards Information included in any order issued pursuant to this paragraph is considered to be an order issued under Section 161b of the Atomic Energy Act.”

#### 5. Material Control & Accounting Procedures Controlled as Safeguards Information

**Discussion:** The Safeguards Information definition includes “control and accounting procedures” of special nuclear material (SNM) and indicates that they are associated with “physical protection.” However, unlike other aspects of the revised definition of Safeguards Information, there is no other information in the proposed rule that provides any qualifying details. Of particular concern is that based solely on this definition, the “control and accounting procedures” could be construed, by some, to be applicable to: (a) the “control procedures” associated with placement of SNM in pools or other on-site spent fuel storage facilities; and (b) “accounting procedures” regarding the quantity of special nuclear material maintained by a licensee. The industry believes the NRC intent is that information about the physical protection of special nuclear material must be controlled as Safeguards Information. This is in the definition of Safeguards Information in the current rule.



In the NRC Response to Comments, Item 2, "General Issues" 71 FR 64008, the discussion qualifies the "control and accounting procedures" to be associated with: § 73.22(a)(1) and § 73.23(a)(1) for alarm system layouts, intrusion detection equipment, and security communications systems; § 73.22(a)(2) and § 73.23(a)(2) for intrusion alarms, vehicle immobilization features, and plans for law enforcement coordination; § 73.22(a)(3) and § 73.23(a)(3) for inspection reports, audits, and evaluations to the extent that security measures or security vulnerabilities are discussed.

In the NRC Response to Comments, "Detailed Control and Accounting Procedures" 71 FR 64012, the discussion identifies that, "detailed control and accounting procedures do not include: (a) the written directions for transferring fuel between the fuel pool and the reactor; (b) the outage schedule that shows when fuel movement occurs; (c) the real-time communication channels or video monitoring to support fuel movement; or (d) the computer and software that performs the isotopic calculations for irradiated fuel. Further, the response identifies that "there should be no concern about restricting access to these types of information on the basis that they are SGI".

We believe the NRC staff intends power reactors to control SNM in accordance with ANSI N15.8, *Nuclear Material Control Systems for Nuclear Power Plants*. This standard is being rewritten concurrent with this rulemaking. The NRC staff is participating on the ANSI writing committee. As a national standard the document cannot be controlled as Safeguards Information. The industry understands the NRC staff intends to endorse the national standard in a Regulatory Guide for licensee use. Licensees will use the standard to revise their site procedures to comply with NRC guidance.

**References:**

**§ 73.2, "Definitions"**

The proposed § 73.2 definition of Safeguards Information is: "Safeguards Information means information not classified as National Security Information or Restricted Data which specifically identifies a licensee's or applicant's detailed control and accounting procedures for the physical protection of special nuclear material in quantities determined by the Commission through order or regulation to be significant to the public health and safety or the common defense and security; detailed security measures (including security plans, procedures, and equipment) for the physical protection of source, byproduct, or special nuclear material in quantities determined by the Commission through order or regulation to be significant to the public health and safety or the common defense and security; security measures for the physical protection of and location of certain plant equipment vital to the safety of production or utilization facilities; and any

other information within the scope of Section 147 of the Atomic Energy Act of 1954, as amended, the unauthorized disclosure of which, as determined by the Commission through order or regulation, could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of sabotage or theft or diversion of source, byproduct, or special nuclear material.”

**71 FR 64008, NRC response in the first comment in General Issues.**

“The Commission recognizes there are limits to its discretion under Section 147 of the AEA in determining what information presents security concerns significant enough to warrant protection as SGI. The revised proposed rule does not expand the Commission’s discretion beyond statutory limits—the revised proposed rule describes the information the Commission considers SGI and is within the scope of the authority granted by Section 147 of the AEA. Section 147 of the AEA authorizes the Commission to protect information that specifically identifies the control and accounting procedures or security measures, including plans, procedures, and equipment used to protect source, byproduct, and special nuclear material. The categories of information to be protected under the rule fall well within this scope. Sections § 73.22(a)(1) and § 73.23(a)(1) would protect information associated with physical protection such as alarm system layouts, intrusion detection equipment, and security communications systems, among other information. Sections §73.22(a)(2) and § 73.23(a)(2) would protect information associated with physical protection such as intrusion alarms, vehicle immobilization features, and plans for law enforcement coordination. Sections §73.22(a)(3) and § 73.23(a)(3) would protect inspection reports, audits, and evaluations to the extent they discuss security measures or security vulnerabilities. All of this and other information categorized in the regulations, if publicly disclosed, could be used to specifically identify the control and accounting procedures or security measures, including security plans, procedures, and equipment used to protect source, byproduct, and special nuclear material and allow the circumvention of those plans, procedures, or equipment.”

**71 FR 64012, Detailed Control and Accounting Procedures**

“Comment: One commenter suggested that the term “detailed control and accounting procedures” for SNM needs clarification, for example, as to whether it includes: (1) The written directions for transferring fuel between the fuel pool and the reactor; (2) the outage schedule that shows when fuel movement occurs; (3) the real-time communication channels or video monitoring to support fuel movement; or (4) the computer and software that performs the isotopic calculations for irradiated fuel. The commenter is concerned that restricting access to these types of detailed information would significantly hamper work coordination and communication within the

protected area, without affecting what is commonly known outside the protected area in a more general sense.

Response: In response to the request in this comment, the Commission notes that “detailed control and accounting procedures” do not include any of the four types of information set forth in this comment. Therefore, there should be no concern about restricting access to these types of information on the basis that they are SGI.”

**Recommendation:** Modify the definition of Safeguards Information in § 73.2 to: “Safeguards Information means information not classified as National Security Information or Restricted Data which specifically identifies a licensee’s or applicant’s detailed security measures (including security plans, procedures, and equipment) for the physical protection of source, byproduct, or special nuclear material in quantities determined by the Commission through order or regulation to be significant to the public health and safety or the common defense and security; security measures for the physical protection of and location of certain plant equipment vital to the safety of production or utilization facilities; and any other information within the scope of Section 147 of the Atomic Energy Act of 1954, as amended, the unauthorized disclosure of which, as determined by the Commission through order or regulation, could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of sabotage or theft or diversion of source, byproduct, or special nuclear material.”

## 6. Lack of Clarity Regarding Engineering and Safety Analyses

**Discussion:** The engineering and safety analyses in the proposed § 73.22(a)(1)(xii) are not clearly linked to security as are all other items described in the proposed § 73.22(a)(1). In order to avoid confusion it should be made very clear that the NRC intends this requirement to pertain to engineering and safety analyses related to physical protection.

**References:** The proposed § 73.22(a)(1)(xii) states: “Engineering and safety analyses, security-related procedures or scenarios, and other information revealing site-specific details of the facility or materials if the unauthorized disclosure of such analyses, procedures, scenarios, or other information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of source, byproduct, or special nuclear material.”

**Recommendation:** Modify § 73.22(a)(1)(xii) to state: “Engineering and safety analyses related to physical protection, security-related procedures or

scenarios, and other information revealing site-specific physical protection details of the facility or materials if the unauthorized disclosure of such analyses, procedures, scenarios, or other information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of source, byproduct, or special nuclear material.”

## **7. Conditions for Access Are Not Clear**

**Discussion:** The conditions for access described in § 73.22(b)(1) are very clear however the conditions for access described in § 73.22(b)(2) are confusing. The phrase “other means approved by the Commission” in § 73.22(b)(2) is completely undefined. Other than orders the Commission may issue to supplement the regulations in extraordinary circumstances, licensees should have, in the Code of Federal Regulations, the complete set of requirements which would provide stability for their Safeguards Information Programs. If the Commission is not, at this time, prepared to specify the requirements, the proposed rule should be withdrawn until it is complete. The NRC response to a similar comment submitted on the previous version of this rulemaking at 71 FR 64019 is “NRC staff plans to issue further guidance that will include a discussion of acceptable background checks that would satisfy the rule requirements by ‘other means’ and support a licensee’s trustworthiness and reliability determinations.” While the industry appreciates the NRC intention to issue guidance, the rule should contain a clear requirement. This is especially important in light of the NRC’s proposed very short implementation period.

**References:** The proposed § 73.22(b)(1) states: “Except as the Commission may otherwise authorize, no person may have access to Safeguards Information unless the person has an established “need to know” for the information and has undergone a Federal Bureau of Investigation criminal history check using the procedures set forth in § 73.57.”

The proposed § 73.22(b)(2) states: “In addition, a person to be granted access to SGI must be trustworthy and reliable, based on a background check or other means approved by the Commission.”

**Recommendation:** Modify § 73.22(b)(2) to state: “In addition, a person to be granted access to SGI must be trustworthy and reliable, based on a background check.”

## 8. Security Storage Containers

**Discussion:** The proposed § 73.22(c)(2) and § 73.23(c)(2) require cabinets storing Safeguards Information to not be marked. NRC did not incorporate the industry comment made previously on this requirement dispositioning it by stating, "The Commission is declining to adopt the change proposed by the commenter because marking locked security storage containers to indicate they contain SGI may assist in identifying the location of SGI. The fact that such containers may typically be located in areas without public access is irrelevant because not all individuals in such areas are authorized for access to SGI. An unauthorized individual seeking access to SGI might be aided by such markings, regardless of whether the SGI is stored in areas without public access." The industry notes that cabinets containing SGI are already obvious as they are the only lockable General Services Administration approved cabinets in the security organization area at an average power reactor site. It is very unlikely an individual who does not have access to SGI would be in this area. Visitors would usually be escorted. The proposed requirement would be detrimental to the common defense and security because the typical brightly colored mnemonic aids concerning verification that the Safeguards Information cabinet is locked would be prohibited. Finally, it is noted that in training course materials provided by NRC to the industry on December 6, 2006 that NRC uses the same type of brightly colored mnemonic aids concerning verification that the Safeguards Information cabinet is locked. We do not understand the NRC's reasoning for prohibiting the industry from following the same good practices.

**References:** The proposed § 73.22(c)(2) states: "While unattended, Safeguards Information must be stored in a locked security storage container. The container shall not identify the contents of the matter contained and must preclude access by individuals not authorized access in accordance with the provisions of this section. Knowledge of lock combinations protecting Safeguards Information must be limited to a minimum number of personnel for operating purposes who have a "need to know" and are otherwise authorized access to Safeguards Information in accordance with the provisions of this part. Access to lock combinations must be strictly controlled so as to prevent disclosure to an individual not authorized access to Safeguards Information."

The proposed § 73.23(c)(2) states: "While unattended, Safeguards Information designated as Safeguards Information-Modified Handling must be stored in a locked file drawer or cabinet. The container shall not identify the contents of the matter contained and must preclude access by individuals not authorized access in accordance with the provisions of this section. Knowledge of lock combinations or access to keys protecting Safeguards Information designated

as Safeguards Information-Modified Handling must be limited to a minimum number of personnel for operating purposes who have a “need to know” and are otherwise authorized access to Safeguards Information in accordance with the provisions of this part. Access to lock combinations must be strictly controlled so as to prevent disclosure to an individual not authorized access to Safeguards Information designated as Safeguards Information-Modified Handling.”

**Recommendations:** Modify § 73.22(c)(2) to state: “While unattended, Safeguards Information must be stored in a locked security storage container. The storage container must preclude access by individuals not authorized access in accordance with the provisions of this section. Knowledge of lock combinations protecting Safeguards Information must be limited to a minimum number of personnel for operating purposes who have a “need to know” and are otherwise authorized access to Safeguards Information in accordance with the provisions of this part. Access to lock combinations must be strictly controlled so as to prevent disclosure to an individual not authorized access to Safeguards Information.”

Modify § 73.23(c)(2) “While unattended, Safeguards Information designated as Safeguards Information-Modified Handling must be stored in a locked file drawer or cabinet. The storage container must preclude access by individuals not authorized access in accordance with the provisions of this section. Knowledge of lock combinations or access to keys protecting Safeguards Information designated as Safeguards Information-Modified Handling must be limited to a minimum number of personnel for operating purposes who have a “need to know” and are otherwise authorized access to Safeguards Information in accordance with the provisions of this part. Access to lock combinations must be strictly controlled so as to prevent disclosure to an individual not authorized access to Safeguards Information designated as Safeguards Information-Modified Handling.”

## **9. Flexibility Should be Permitted in Marking Safeguards Information Documents**

**Discussion:** The NRC did not incorporate the industry’s previous comment on the § 73.22(d)(1) noting that “The Commission is not modifying § 73.22(d)(1) as the commenter suggests because the information specified in § 73.22(d)(1)(i) through (iii) should be noted on the first page of the document itself rather than in a separate document, such as a cover sheet. The Commission does not expect that licensees or applicants must go back and mark documents for which a cover sheet was used for the required information instead of the first page of the document, as set forth in § 73.22(d)(1).”

Some licensees have modeled their Safeguards Information cover sheets on the NRC cover sheet, NRC Form 461 (3-2003), which includes the information about violations being subject to civil or criminal penalties. It seems unreasonable to have these licensees change their programs especially in light of the fact that their procedures require all Safeguards Information documents to have the coversheet. If the NRC will not change the proposed requirement and the NRC does not expect that licensees or applicants must go back and mark documents for which a cover sheet was used for the required information, then the rule should make that clear. Finally, it is our view that it is more important that the top of a Safeguards Information document is clearly marked to indicate that the document should be protected than to be concerned with exactly where to describe the criminal penalties and exactly where to place the determination block. The prescriptive nature of the proposed language is sure to lead to issues between licensees and NRC inspectors that are essentially meaningless. The rule should require the top of the document, whether cover sheet, first page, or binder cover, to clearly indicate the document is safeguards information. The criminal penalties information and determination information should be on or near the top or front of the document.

**References:** The proposed § 73.22(d)(1) states: “Each document or other matter that contains Safeguards Information as described in § 73.21(a)(1)(i) and this section must be marked to indicate the presence of such information in a conspicuous manner on the top and bottom of each page. The first page of the document must also contain:

- (i) The name, title, and organization of the individual authorized to make a Safeguards Information determination, and who has determined that the document contains Safeguards Information;
- (ii) The date the determination was made; and
- (iii) An indication that unauthorized disclosure will be subject to civil and criminal sanctions.”

**Recommendation:** Modify § 73.22(d)(1) to state: “Each document or other matter that contains Safeguards Information as described in § 73.21(a)(1)(i) and this section must be marked to indicate the presence of such information in a conspicuous manner on the top and bottom of each page. The first page, cover sheet, or binder cover must indicate that unauthorized disclosure will be subject to civil and criminal sanctions. The first page, cover sheet, or binder cover of the document must also contain:

- (i) The name, title, and organization of the individual authorized to make a Safeguards Information determination, and who has determined that the document contains Safeguards Information;
- (ii) The date the determination was made.”

If the NRC will not finalize the rule to provide this flexibility then the recommendation is: “Effective on [insert implementation date] each document or other matter that contains Safeguards Information as described in § 73.21(a)(1)(i) and this section must be marked to indicate the presence of such information in a conspicuous manner on the top and bottom of each page. The first page of the document must also contain:

- (i) The name, title, and organization of the individual authorized to make a Safeguards Information determination, and who has determined that the document contains Safeguards Information;
- (ii) The date the determination was made; and
- (iii) An indication that unauthorized disclosure will be subject to civil and criminal sanctions. For documents produced prior to [insert implementation date] documents must be marked as was required by the licensees Safeguards Information Program at the time the document was produced.”

## **10. Lack of Clarity Regarding Data Processed on a Computer**

**Discussion:** The proposed § 73.22(g)(2) prohibits the use of various storage media when processing Safeguards Information on a computer and restricts appropriate flexibility for locating computers used for processing Safeguards Information. It should permit external storage media use as long as the media are properly controlled and should allow computers used to process Safeguards Information to be located in controlled access areas (e.g. locked and alarmed, when unattended by persons authorized access to Safeguards Information) in conjunction with password protection.

**References:** The proposed § 73.22(g)(2) states: “Each computer not located within an approved and lockable security storage container that is used to process Safeguards Information must have a removable storage medium with a bootable operating system. The bootable operating system must be used to load and initialize the computer. The removable storage medium must also contain the software application programs, and all data must be processed and saved on the same removable storage medium. The removable storage medium must be secured in a locked security storage container when not in use.”

**Recommendation:** Modify § 73.22(g)(2) to state: “Each computer must have password protection and be located within a controlled access area (e.g. locked and alarmed, when unattended by persons authorized access to Safeguards Information) or be located within an approved and lockable security storage container that is used to protect Safeguards Information. Each computer not located within a controlled access area or an approved and lockable security storage container that is used to process Safeguards



Information must have a removable storage medium with a bootable operating system. The bootable operating system must be used to load and initialize the computer. The removable storage medium must also contain the software application programs, and all data must be processed on the same removable storage medium. The data may be saved on the same removable storage medium or on other storage media as long as the media are adequately controlled. The removable storage medium must be secured in a locked security storage container when not in use or controlled as Safeguards Information.”

## **11. Ten Year Review Period**

**Discussion:** It is our view that the ten year review requirement should be eliminated. It is an unnecessary activity resulting in an inefficient use of key resources with no obvious benefit to protecting the health and safety of the public. In fact, it is more conservative to retain such documents as Safeguards Information than to decontrol them. Decontrolling such documents is a human-error prone situation and would open licensees up to second guessing by NRC inspectors. The ten year review requirement was not in the version of the rule published on February 11, 2005. No order has been issued requiring such a review. It is not discussed in comment disposition at 71 FR 64022 or at 71 FR 64026. It is not discussed in Table 1 at 71 FR 64043 or at 71 FR 64048. It is entirely without basis or discussion. It may also have an unintended consequence of burdening the NRC staff. A large number of decisions required to decontrol documents would be directed to the NRC as it is unlikely that the individuals who controlled the documents originally would be available to review them ten years later for decontrol. Others in the same organization would be hesitant to second guess the individual who controlled the document originally.

Based on a survey NEI conducted in 2005 the average power reactor site had 2,293 Safeguards Information documents and was producing 235 Safeguards Information documents per year. In ten years, given the same rate of document production, there will be 4643 Safeguards Information documents at the average site. The review would require first a sort to determine which were ten years old and required reviews. Then the 2,293 ten year old documents would require the NRC to review for decontrol.

If there is a perception that decontrol of licensee Safeguards Information documents will somehow provide such information to the public it is unfounded. Unlike the public sector, almost no licensees have any obligation to make any of their internal documents available to the public.

Finally licensees should be able to decontrol documents they have marked as Safeguards Information without approval of NRC as long as the individual who initially controlled the document concurs or another authorized determination agent makes the determination.

**Reference:** The proposed § 73.22(h) states: "*Removal from Safeguards Information category.* Documents originally containing Safeguards Information must be removed from the Safeguards Information category at such time as the information no longer meets the criteria contained in this part. A review of such documents to make that determination shall be conducted every 10 years. Documents that are 10 years or older and designated as SGI or SGI-M shall be reviewed for a decontrol determination if they are currently in use or removed from storage. Care must be exercised to ensure that any document decontrolled not disclose Safeguards Information in some other form or be combined with other unprotected information to disclose Safeguards Information. The authority to determine that a document may be decontrolled shall be exercised only by the NRC or with NRC approval, or if possible, in consultation with the individual or organization that made the original determination."

**Reference:** The proposed § 73.23(h) states: "*Removal from Safeguards Information Modified Handling category.* Documents originally containing Safeguards Information designated as Safeguards Information- Modified Handling must be removed from the Safeguards Information category at such time as the information no longer meets the criteria contained in this Part. A review of such documents to make that determination shall be conducted every 10 years. Documents that are 10 years or older and designated as SGI or SGI-M shall be reviewed for a decontrol determination if they are currently in use or removed from storage. Care must be exercised to ensure that any document decontrolled shall not disclose Safeguards Information in some other form or be combined with other unprotected information to disclose Safeguards Information. The authority to determine that a document may be decontrolled shall be exercised only by the NRC or with NRC approval, or if possible, in consultation with the individual or organization that made the original determination.

**Recommendation:** If the provision is not eliminated then § 73.22(h) should be modified to state: "*Removal from Safeguards Information category.* Documents originally containing Safeguards Information may be removed from the Safeguards Information category at such time as the information no longer meets the criteria contained in this part. Care must be exercised to ensure that any document decontrolled does not disclose Safeguards Information in some other form or be combined with other unprotected information to disclose Safeguards Information. The authority to determine

that a document may be decontrolled shall be exercised by the NRC, or if possible, by the individual or organization that made the original determination.”

**Recommendation:** If the provision is not eliminated then § 73.23(h) should be modified to state: “*Removal from Safeguards Information Modified Handling category.* Documents originally containing Safeguards Information Modified Handling may be removed from the Safeguards Information Modified Handling category at such time as the information no longer meets the criteria contained in this part. Care must be exercised to ensure that any document decontrolled does not disclose Safeguards Information Modified Handling in some other form or be combined with other unprotected information to disclose Safeguards Information Modified Handling. The authority to determine that a document may be decontrolled shall be exercised by the NRC, or if possible, by the individual or organization that made the original determination.”

## 12. Use of Undefined Terms

**Discussion:** The undefined terms “additional security measures,” “protective measures,” and “interim compensatory measures” are removed from § 73.22(a) but the proposed rule does not make the corresponding change to remove these terms from § 73.23(a). The NRC comment discussion at 71 FR 64015 addresses the industry’s previous comment on this issue for § 73.22(a) however the comment has not been addressed for § 73.23(a).

**References:** The proposed § 73.22(a) states: “*Information to be protected.* The types of information and documents that must be protected as Safeguards Information include non-public security-related requirements such as:”

The proposed § 73.23(a) states: “*Information to be protected.* The types of information and documents that must be protected as Safeguards Information-Modified Handling include non-public security-related requirements such as protective measures, interim compensatory measures, additional security measures, and the following, as applicable:”

**Recommendation:** Modify § 73.23(a) to state: “The types of information and documents that must be protected as Safeguards Information-Modified Handling include non-public security-related requirements such as:”

### 13. Lack of Clarity Regarding Engineering and Safety Analyses for SGI-M

**Discussion:** The engineering and safety analyses in the proposed § 73.23(a)(1)(x) are not clearly linked to security as are all other items described in the proposed § 73.23(a)(1). In order to avoid confusion it should be made very clear that the NRC intends this requirement to pertain to engineering and safety analyses related to physical protection.

**References:** The proposed § 73.23(a)(1)(x) states: “Engineering and safety analyses, security-related procedures or scenarios, and other information revealing site-specific details of the facility or materials if the unauthorized disclosure of such analyses, procedures, scenarios, or other information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of source, byproduct, or special nuclear material.”

**Recommendation:** Modify § 73.23(a)(1)(x) to state: “Engineering and safety analyses related to physical protection, security-related procedures or scenarios, and other information revealing site-specific physical protection details of the facility or materials if the unauthorized disclosure of such analyses, procedures, scenarios, or other information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of source, byproduct, or special nuclear material.”

### 14. Conditions for Access Are Not Clear for SGI-M

**Discussion:** The conditions for access described in § 73.23(b)(1) are very clear while the conditions for access described in § 73.23(b)(2) are confusing. The phrase “other means approved by the Commission” in § 73.23(b)(2) is completely undefined. Other than orders the Commission may issue to supplement the regulations in extraordinary circumstances, licensees should have, in the Code of Federal Regulations, the complete set of requirements which would provide stability for their Safeguards Information Programs. If the Commission is not, at this time prepared to specify the requirements, the proposed rule should be withdrawn until it is complete. The NRC response to a similar comment submitted on the previous version of this rulemaking at 71 FR 64019 is “NRC staff plans to issue further guidance that will include a discussion of acceptable background checks that would satisfy the rule requirements by ‘other means’ and support a licensee’s trustworthiness and reliability determinations.” While the industry appreciates the NRC

intention to issue guidance, the rule should contain a clear requirement. This is especially important in light of the NRC's proposed very short implementation period.

**References:** The proposed § 73.23(b)(1) states: "Except as the Commission may otherwise authorize, no person may have access to Safeguards Information unless the person has an established "need to know" for the information and has undergone a Federal Bureau of Investigation criminal history check using the procedures set forth in § 73.57."

The proposed § 73.23(b)(2) states: "In addition, a person to be granted access to SGI must be trustworthy and reliable, based on a background check or other means approved by the Commission."

**Recommendation:** Modify § 73.23(b)(2) to state: "In addition, a person to be granted access to SGI must be trustworthy and reliable, based on a background check." Or the Commission should withdraw the proposed rule until it is complete.

**From:** "WALTERS, Doug" <djw@nei.org>  
**To:** <secy@nrc.gov>  
**Date:** Tue, Jan 2, 2007 9:41 PM  
**Subject:** Comments on the Proposed Rule, Protection of Safeguards Information, (71 Fed. Reg. 64004; October 31, 2006), RIN 3150-AH57)

Comments on the Proposed Rule, Protection of Safeguards Information, (71 Fed. Reg. 64004; October 31, 2006), RIN 3150-AH57) are enclosed.

Sincerely;

Douglas J. Walters  
Senior Director-Security  
Nuclear Energy Institute  
1776 I Street N.W.  
Washington, D.C. 20006

This electronic message transmission contains information from the Nuclear Energy Institute, Inc. The information is intended solely for the use of the addressee and its use by any other person is not authorized. If you are not the intended recipient, you have received this communication in error, and any review, use, disclosure, copying or distribution of the contents of this communication is strictly prohibited. If you have received this electronic transmission in error, please notify the sender immediately by telephone or by electronic mail and permanently delete the original message.

**Mail Envelope Properties** (459B17B3.6FC : 1 : 46844)

**Subject:** Comments on the Proposed Rule, Protection of Safeguards Information,  
(71 Fed. Reg. 64004; October 31, 2006), RIN 3150-AH57)  
**Creation Date** Tue, Jan 2, 2007 9:41 PM  
**From:** "WALTERS, Doug" <[djw@nei.org](mailto:djw@nei.org)>  
**Created By:** [djw@nei.org](mailto:djw@nei.org)

**Recipients**

nrc.gov  
TWGWPO02.HQGWDO01  
SECY (SECY)

**Post Office**

TWGWPO02.HQGWDO01

**Route**

nrc.gov

<b>Files</b>	<b>Size</b>	<b>Date &amp; Time</b>
MESSAGE	867	Tuesday, January 2, 2007 9:41 PM
NEIComments010207Final.doc	177152	
Mime.822	246244	

**Options**

**Expiration Date:** None  
**Priority:** Standard  
**ReplyRequested:** No  
**Return Notification:** None

**Concealed Subject:** No  
**Security:** Standard

**Junk Mail Handling Evaluation Results**

Message is eligible for Junk Mail handling  
This message was not classified as Junk Mail

**Junk Mail settings when this message was delivered**

Junk Mail handling disabled by User  
Junk Mail handling disabled by Administrator  
Junk List is not enabled  
Junk Mail using personal address books is not enabled  
Block List is not enabled