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

SECRETARY

March 17, 2008

COMMISSION VOTING RECORD

DECISION ITEM: SECY-07-0131

TITLE: FINAL RULE – 10 CFR PART 73 "SAFEGUARDS INFORMATION PROTECTION REQUIREMENTS" (RIN 3150 – AH57)

The Commission (with Chairman Klein and Commissioner Lyons agreeing) approved the final rule as noted in an Affirmation Session and recorded in the Staff Requirements Memorandum (SRM) of March 17, 2008. Commissioner Jaczko while approving 10 CFR Part 73, disapproved the use of separate handling requirements for Safeguards Information-Modified Handling (SGI-M) and supported inclusion of a requirement for a periodic decontrol review. Commissioner Jaczko also disapproved the abuse of discretion standard in changes to 10 CFR Part 2.

This Record contains a summary of voting on this matter together with the individual vote sheets, views and comments of the Commission.

Annette L. Vietti-Cook
Secretary of the Commission

Attachments:
1. Voting Summary
2. Commissioner Vote Sheets

cc: Chairman Klein
Commissioner Jaczko
Commissioner Lyons
OGC
EDO
PDR

VOTING SUMMARY - SECY-07-0131

RECORDED VOTES

	APRVD	DISAPRVD	ABSTAIN	NOT PARTICIP	COMMENTS	DATE
CHRM. KLEIN	X				X	12/17/07
COMR. JACZKO	X	X			X	10/15/07
COMR. LYONS	X				X	12/1X/07

COMMENT RESOLUTION

In their vote sheets, Chairman Klein and Commissioner Lyons approved the staff's recommendation and provided some additional comments. Commissioner Jaczko while approving 10 CFR Part 73, disapproved the use of separate handling requirements for Safeguards Information-Modified Handling (SGI-M) and supported inclusion of a requirement for a periodic decontrol review. Commissioner Jaczko also disapproved the abuse of discretion standard in changes to 10 CFR Part 2.

Subsequently, the Commission approved the final rule as noted in an Affirmation Session and reflected in the SRM issued on March 17, 2008.

AFFIRMATION ITEM

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

FROM: CHAIRMAN KLEIN

SUBJECT: SECY-07-0131 - FINAL RULE - 10 CFR PART 73 "SAFEGUARDS INFORMATION PROTECTION REQUIREMENTS" (RIN 3150 - AH57)

Approved XX Disapproved _____ Abstain _____

Not Participating _____

COMMENTS: Below___ Attached XX None ___

SIGNATURE

12/17/07

DATE

Entered on "STARS" Yes ✓ No ___

CHAIRMAN KLEIN'S COMMENTS ON SECY-07-0131

I approve the draft final rule on Safeguards Information Protection Requirements, subject to the comments below. The final product reflects a very substantial and important effort to update our regulations to reflect expanded authority under the Energy Policy Act of 2005, post-911 security requirements, and clarifications of the process for access to SGI in NRC adjudications.

I support the recommendation not to include a 10-year SGI decontrol review requirement, and I concur in Commissioner Lyons' comments on the issue. I also concur in his comments regarding the desirability of more consistency in the treatment of the scope of violations of protective orders in adjudication that could lead to civil or criminal penalties.

A public commenter stated that information about types and quantities of material listed on a license in some cases should be considered SGI when the license contains nuclides and quantities of concern. The proposed response explains that licensing documents are reviewed to determine if they contain SGI or other information warranting protection and that information on possession limits for radionuclides generally does not meet the definition of SGI. The proposed response also states: "This information, although not categorized as SGI, may be withheld from public disclosure if disclosure of the information could raise security concerns." *See* Draft *Federal Register* notice, p. 13. An example of such an instance would be useful, as Commissioner Lyons suggests. I recommend either deleting the quoted sentence or adding some clarification, such as the following: "For example, in some contexts information on actual quantities possessed in relation to possession limits could raise security concerns."

The *Federal Register* notice, on pages 141 and 152, addresses processing SGI on electronic systems. Commissioner Lyons suggests that the requirements make clear that stand-alone computers or computer systems for processing SGI must be cleared of recoverable SGI prior to being returned to non-exclusive use. This would be beneficial if it is practical to do so at this stage. I recommend that at least the statement of considerations address the matter and note that the NRC will develop guidance on preventing such an occurrence.

Dale E. Klein 12/7/07

AFFIRMATION ITEM

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

FROM: **COMMISSIONER JACZKO**

SUBJECT: SECY-07-0131 - FINAL RULE - 10 CFR PART 73 "SAFEGUARDS INFORMATION PROTECTION REQUIREMENTS" (RIN 3150 - AH57)

Approved X in part Disapproved X in part Abstain _____

Not Participating _____

COMMENTS: Below___ Attached __X__ None ___

SIGNATURE

1/28/08

DATE

Entered on "STARS" Yes _X_ No ___

Commissioner Jaczko's Comments on SECY-07-0131
Final Rule – 10 CFR Part 73 "Safeguards Information Protection Requirements"

I approve in part and disapprove in part this Final Rule on part 73. I approve of the final rule in the same areas where I approved of the proposed rule – where it clarifies SGI requirements and captures requirements imposed on licensees by Order. As I mentioned in my prior votes on this rule, I continue to disapprove of the use of separate handling requirements for SGI-M as I believe it unnecessarily complicates the issue.

I continue to support the inclusion of a regulatory provision requiring a periodic assessment of whether documents marked as "SGI" or "SGI-M" still meet the requirements of Part 73, and are thus properly marked and protected. The staff originally received comments raising the issue of appealing SGI markings and, in the process of voting on the proposed rule the Commission directed that the staff include a periodic 10-year review requirement. I do not find the rationale for the staff's reluctance to maintain this requirement persuasive. If we intend for SGI to be treated more like classified information, we should then require that it be treated more like classified information. Requiring a periodic review would not require, in practical terms, those in possession of SGI to do anything different than they do with their classified information. And if a ten-year review appears a bit cumbersome, then, at minimum, a twenty-five year review should be required.

I also have some concerns with the final edits to provisions in part 2 of our regulations which dictate the process by which access determinations are reviewed. Specifically, I do not approve of the abuse of discretion standard provided for review by a presiding officer in adjudications of trustworthiness and reliability determinations by the NRC Office of Administration (sections 2.336(f)(1)(iv), 2.704(c)(3)(iv), 2.709(f)(1)(iv) and 2.1010(b)(6)(i)(D)). I believe adding an "abuse of discretion" standard is neither necessary nor efficient. It is a standard that does not appear elsewhere in our Part 2 regulations and introducing it now into a new process creates implementation issues of its own.

Moreover, I believe the agency's Administrative Judges are more than capable of delving into the details of a record on a trustworthiness and reliability determination and making a decision in this regard. I recognize that these determinations are made by Office of Administration employees who rely upon expertise developed through training and experience. But I believe that statement is true of most, if not all, of the staff's decisions which are later subject to review in agency adjudications. The area of enforcement is one that immediately comes to mind, where staff is applying their best judgment, based upon their experience and training, in determining the appropriate enforcement action in a particular situation. Despite the skilled and expert staff making these decisions, the decisions can be challenged in our adjudicatory proceedings and the Licensing Boards are then required to sift through the evidence and determine the appropriateness of the staff action. Many enforcement matters essentially boil down to credibility determinations and the Boards are tasked to resolve those very kinds of issues.

Additionally, I believe the issue of access to information is a fundamental one as it then essentially determines who the participants are going to be and what subject matters will be allowed to be litigated in an NRC adjudicatory proceeding. If we do not require this decision to be made clearly and completely up front in the process, we are only inviting later delays. Thus, the staff should stand ready to defend their decision to a Presiding

Officer in more detail than required by a lenient "abuse of discretion" standard, and that Presiding Officer should have the flexibility in reviewing the information to determine if there is any additional information he or she deems necessary in order to best resolve the dispute and have the ultimate decision clearly reflected on the record. I believe the Office of Administration will thoroughly perform its required role in reviewing requests for access to SGI, and thus, allowing a Presiding Officer to have broader review authority over its decisions should not create any additional work for the NRC staff. Instead, it will allow the staff an opportunity to fully explain its rationale.

While the current draft of the *Federal Register* notice infers that there are concerns with additional time delays if the Presiding Officer has to conduct a full-fledged fact-finding, "mini-hearing" in the context of the larger hearing, I believe the opposite to be true. If the abuse of discretion standard remains and the Presiding Officer is limited to this very high level review aimed at catching only egregious errors, their role is essentially perfunctory and is, in itself, a waste of time. An intervenor who continues to be denied access to the information will file an interlocutory appeal to the Commission under the proposed final section 2.311 revisions. Then the Commission will have to review the issue and if, in fact, there is a question about the staff's decision, the Commission will have to look into the issue in more detail. Historically, the Commission has tasked these types of activities to a Presiding Officer. This then brings us full circle. Time is actually saved by eliminating the "abuse of discretion" standard and ensuring the appropriate review is conducted thoroughly at the beginning of the process. The subsequent request for Commission interlocutory review will then be informed by an already-established and complete record. Therefore, I would propose the rule language, and the response to comments in this regard, be edited to remove the abuse of discretion standard for a Presiding Officer review of adverse trustworthiness and reliability determinations.

Finally, I believe that the presiding officer assigned to rule on the matters of access to information should in no case be the presiding officer assigned to rule on the hearing matters themselves. Instead, the rule as currently drafted allows for it to be one and the same presiding officer unless a person requests a different presiding officer. I believe this change is important not because I lack confidence in the ability of the presiding officers to remain fair and impartial even if they serve both functions, but instead, because I do not believe it would be fair to put the presiding officers in that position in the first place. The presiding officers work hard to gain the confidence of all the parties to a proceeding. This is a difficult job and not one I believe we should make any more difficult. Thus, the rule and response to comments should make it clear that if a proceeding has commenced, a different presiding officer will be appointed to review any adverse trustworthiness and reliability decisions.

Gregory B. Jaczko 1/25/08

Date

AFFIRMATION ITEM

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

FROM: COMMISSIONER LYONS

SUBJECT: SECY-07-0131 - FINAL RULE - 10 CFR PART 73 "SAFEGUARDS INFORMATION PROTECTION REQUIREMENTS" (RIN 3150 - AH57)

Approved X Disapproved _____ Abstain _____

Not Participating _____

COMMENTS: Below___ Attached X None ___

Peter Lyons
SIGNATURE

10/15/07
DATE

Entered on "STARS" Yes X No ___

Commissioner Lyons' Comments on SECY-07-0131

I approve the staff's recommendation that the Commission publish the final rule that amends the Safeguards Information protection requirements in 10 CFR Part 73 and makes conforming changes to other provisions of the regulations. I appreciate the effort that the staff has undertaken in this endeavor and thank the staff for its work. My specific comments on the final rule are set forth below, and my edits to the *Federal Register* notice and to the draft supplemental material are attached.

The staff did not include a 10-year SGI decontrol review requirement in proposed 10 CFR 73.22(h) and 73.23(h), which would have required holders of SGI to perform a review every 10 years of SGI-designated documents in their possession that are 10 years or older. I agree that the costs of performing the review would not be justified by the benefits. The current requirement states that documents containing SGI "shall be removed from the Safeguards Information category whenever the information no longer meets the criteria contained in this section." 10 CFR 73.23(i). It is my understanding that persons subject to this SGI protection requirement may comply with it by evaluating each document at the time that it is removed from storage. The 10-year requirement would mandate that all documents be evaluated, irrespective of their storage state, at 10-year increments from the effective date of the rule. I do not believe that the cost of a comprehensive review of all SGI in an entity's possession is justified by the intangible benefit of having confidence that at least once every 10 years all documents bearing SGI markings contain SGI. I further doubt that an appreciable increase in documents would make its way into the public domain should the 10-year provision be required.

In the response to comments, the *Federal Register* notice states that information contained in licensing documents on the possession limits for radionuclides generally would not meet the definition of SGI, but that the information may be withheld if disclosure could raise "safety concerns." See *Federal Register* p. 13. The staff should provide an example of such a circumstance in the *Federal Register* notice.

In the response to comments, the *Federal Register* notice addresses civil penalties for violations of protective orders in adjudications and later addresses criminal penalties for violations of protective orders in adjudications. See *Federal Register* p. 35-37. With respect to civil penalties, the notice states that only those violations of orders that result in unauthorized disclosure should be sanctionable by civil penalty (as opposed to violations of orders that result in, for example, not disclosing information, which would be treated as violations of adjudicatory orders within the adjudicatory context). With respect to criminal penalties, the notice takes the opposite tack, stating that criminal penalties would be applied to the "order as a whole" and that the problem would not come up often since criminal penalties are uncommon. I do not support this view since it is inconsistent with the logic provided with respect to civil penalties and since it recognizes that the paramount harm is the unauthorized disclosure of information. The staff should change the response on page 37 and should revise proposed §§ 2.336(f)(6), 2.705(c)(7), 2.709(f)(6) and 2.1010(b)(6)(vi), as necessary, to make the provisions applying to criminal penalties consistent with the provisions applying to civil penalties.

In the response to comments, the *Federal Register* notice addresses a comment that the

phrase "or other means approved by the Commission" be deleted from the requirement found in 73.22(b)(2) and 73.23(b)(2) that to be granted access, a person must be trustworthy and reliable, "based on a background check or other means approved by the Commission." See *Federal Register* pp. 46-47. The response to the comment suggests that the phrase is meant to apply to relief from the obligations imposed by the section. The staff should, in addition to the discussion of the Commission's authority to relieve persons from criminal records requirements, provide a discussion that addresses the authority of the Commission to impose additional requirements to the extent that the phrase is considered to allow for more conservative protections.

The Commission recently received a paper (SECY-07-0163) regarding vulnerabilities in computer systems due to the use of peer-to-peer software. The *Federal Register* notice on page 141 and 152 addresses processing SGI on electronic systems. The requirements should make it clear that computer systems that have been used to process SGI, prior to being returned to nonexclusive use, must be free of recoverable SGI in order to preclude any access to SGI.

Peter B. Lyons 10/15/07
Peter B. Lyons Date

III. Purpose of Rulemaking

NRC staff review of the SGI regulatory program indicates that changes in the regulations are needed to address issues such as access to SGI, types of security information to be protected, and handling and storage requirements.

This rulemaking will:

(1) Revise the definition of "need to know" in 10 CFR 73.2;

(2) Implement expanded fingerprinting and criminal history records check procedures for broader categories of individuals who will have access to SGI unless exempt from those requirements;

(3) Implement a requirement for background checks to determine trustworthiness and reliability for individuals who will have access to SGI or SGI-M unless exempt from those requirements;

(4) Implement generally applicable requirements for SGI and SGI-M that are similar to requirements imposed by the orders;

(5) Expand the scope of part 73 to include additional categories of licensees (e.g., source and byproduct material licensees, research and test reactors not previously covered, and fuel cycle facilities not previously covered). As expanded, vendors, applicants and certificate holders are also within the scope of the rule;

(6) Expand the types of security information covered by the definition of SGI in § 73.2 and the information categories described in §§ 73.22 and 73.23 to include detailed security

measures for the physical protection of byproduct, source, and special nuclear material; emergency planning scenarios and implementing procedures; uncorrected vulnerabilities or weaknesses in a security system; and certain training and qualification information;

(7) Clarify requirements for obtaining access to SGI in the context of adjudications and clarify the appeal procedures available;

(8) Modify the original proposed rule to align it with the final rule in 10 CFR 73.59 granting relief from the fingerprinting, identification and criminal history records checks and background checks for designated categories of individuals; and

(9) Modify 10 CFR 73.59 to make it consistent with the language and structure of the proposed SGI rule.

In the development of the rule, a graded approach based on the risks and consequences of information disclosure was used to determine which category of licensee or type of information would be subject to certain protection requirements. This graded approach was applied to issues such as the type of information to be protected, the classes of licensees subject to the rule, and the level of handling requirements necessary for the various licensees. For example, the graded approach will allow certain licensees to employ the modified-handling procedures introduced in recent orders and now set forth in the SGI-M provisions of this final rule.

The requirements set forth in this final rule are the minimum restrictions the Commission finds necessary to protect SGI and SGI-M against inadvertent release or unauthorized disclosure which might compromise the health and safety of the public or the common defense and security. The final rule would cover those facilities and materials the Commission has already determined need to be protected against theft or sabotage. The categories of

information constituting SGI and SGI-M relate to the types of facilities and the quantities of special nuclear material, source material and byproduct material determined by the Commission to be significant and therefore subject to protection against unauthorized disclosure pursuant to Section 147 of the AEA. Unauthorized release of SGI could reduce the deterrence value of systems and measures used to protect nuclear facilities and materials and allow for the possible compromise of those facilities and materials. Such disclosures could also facilitate advance planning by an adversary intent on committing acts of theft or sabotage against the facilities and materials within the scope of this rule. Further, the Commission has determined, pursuant to Section 147a.(3)(B) of the AEA, that the unauthorized disclosure of SGI, including SGI-M, 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 nuclear material or a facility.

IV. Discussion

A. *Resolution of public comments on the revised proposed rule.*

1. Overview of comments on the revised proposed rule.

On February 11, 2005 (70 FR 7196), the Commission published a proposed rule and requested public comments. On October 31, 2006 (71 FR 64004), the Commission published a revised version of the proposed rule that responded to comments on the original proposed rule.

criminal penalties for unauthorized disclosure of SGI documents. The commenter also believes that it is too burdensome for intervenors to determine whether the engineering and safety analyses they generate to support a contention are SGI. The commenter believes that in light of the above difficulties, parties should be allowed to file documents marked "may contain safeguards information," which would be treated as SGI pending a determination by NRC staff members not involved in the adjudicatory proceeding. Although it is not entirely clear from the comment letter, the commenter might also be requesting that intervenors not be potentially subject to criminal and civil penalties for violating SGI requirements.

Response: In response to a comment on the first proposed rule, the Commission acknowledged that there is a tendency to "err on the safe side" in making SGI designations, and stated that it might make appropriate changes if over-designating documents as SGI arises as a problem in practice. *See* 71 FR 64020-21. Eliminating criminal and civil sanctions for violating SGI requirements, however, would not be among these appropriate changes. The Commission believes that criminal and civil sanctions serve a worthwhile purpose in securing compliance with SGI provisions, and that these sanctions should apply equally to all parties. The AEA explicitly authorizes criminal sanctions for willful violations of SGI provisions. *See* 42 U.S.C. §§ 2167 and 2273.

The Commission does not accept the commenter's suggestion to allow parties to mark pleadings as possibly containing SGI awaiting a determination by the Staff; the Commission thinks it fair that parties be responsible for determining whether the analyses they generate contain SGI. A party that is litigating a security contention presumably possesses the requisite

competence in security matters to make SGI determinations, and a party in possession of SGI must have already been determined to possess competence in security matters to satisfy the "need to know" requirement. Also, the commenter's suggestion, if implemented, would allow parties to file documents labeled "may contain Safeguards Information" without doing a careful analysis. The potential for over-designating SGI would be much greater under the commenter's suggested regime than under the rule as proposed. Until the Staff review was complete, there would likely be a much larger number of documents subject to SGI handling than would be the case under the proposed rule. If a party needs assistance, however, in determining whether the materials it creates contain SGI, the Staff will be available to provide advice if requested.

Comment: An agreement state commenter asserts that proposed § 73.22(h) allows the decontrol of SGI-marked documents only by, or with the approval of, the NRC, and suggests that a mechanism be established allowing intervenors to request the NRC staff to decontrol documents, or portions thereof. The commenter believes that such a process would benefit intervenors by removing from them the burden of having to control and store a large mass of documents as SGI. The commenter states that destruction might not be a viable option for an intervenor to reduce its burdens because of that intervenor's internal document retention procedures.

Response: Contrary to the commenter's understanding, § 73.22(h) allows an SGI document to be decontrolled in consultation with the person or organization making the original SGI determination, as well as by the NRC or with the NRC's approval. The language of

Response: The Commission believes that an abuse of discretion standard is appropriate for presiding officer review in adjudications of adverse trustworthiness and reliability determinations made by the Office of Administration. The Commission chose the abuse of discretion standard primarily because trustworthiness and reliability determinations rely upon expertise developed through training and experience. Office of Administration employees who make these determinations possess specialized training and experience in evaluating similar information for NRC employee security clearances. Because of the Office of Administration's expertise, the Commission believes that the office's trustworthiness and reliability determinations will generally be sound. A searching, *de novo* review by the presiding officer, therefore, would not be warranted. This is especially the case because presiding officer review of adverse trustworthiness and reliability determinations will not involve witness testimony or other procedures that might arguably put the presiding officer in a better position to assess the evidence underlying a trustworthiness and reliability determination.[9]

The following four numbered paragraphs respond in order to the four numbered reasons given in the comment above:

(1) The commenter's comparison of the review of Office of Administration trustworthiness and reliability determinations to the review of Staff safety evaluations is invalid. The commenter is mistaken in stating that the Staff's safety evaluations are subject to review in contested licensing proceedings. Well-established Commission precedent provides that the license application, and not the Staff's safety review, is the subject of a contested licensing

[9] To be clear, the Commission does not believe that setting up a "mini-hearing" within a hearing by taking witness testimony and using other trial-type procedures is justified to resolve what is, at heart, a discovery dispute over whether certain individuals in a party's litigation team can have access to SGI.

officer will not be conducting a trial-type hearing and will not be performing a searching, *de novo* review of the evidence. Rather, the presiding officer will be reviewing for abuse of discretion and will base this review on a record compiled by the Office of Administration as supplemented by one round of pleadings from the parties. The Commission believes that fifteen days is sufficient time for this review and that providing a longer period would unnecessarily delay proceedings without compensating benefit.

The commenter's analogy relating the time needed for the presiding officer's decision to the time needed for the initial determination by the NRC staff's Office of Administration's is not apt. In order to make its decision, the Office of Administration must first collect information that originates from a variety of sources. This process takes time, and the speed of information collection depends upon the time taken by the providers of the information. As explained in the preceding paragraph, a presiding officer's review of an adverse trustworthiness and reliability determination would involve review only for an abuse of discretion and would not involve the presiding officer independently gathering information for that determination.

Comment: An agreement state asserts that if the Commission were unwilling to entertain appeals of presiding-officer-reviewed access determinations on a timely basis, the proposed changes to part 2 would lead to a denial of parties' rights to a fair hearing and the assistance of counsel. The commenter asserts that lack of timely Commission review would give the Staff, as a party in an adjudicatory hearing, broad discretion to deprive an opposing party of both expert witnesses and legal counsel needed to present its case. According to the commenter, this situation would be a violation of section 555 of the APA, 5 U.S.C. § 555.

SGI-M requirements to ensure proper handling and protection of SGI to avoid unauthorized disclosure. The commenter states that § 73.21(a)(1)(i) conflicts with the previous order by requiring uranium enrichment facilities to modify their protection strategy from SGI-M to SGI. This provision, in the commenter's opinion, imposes an unnecessary regulatory burden without providing commensurate benefit, and could result in the two facilities being governed by different SGI handling requirements even though they are located within the same physical boundary and will ultimately share common infrastructure.

Response: An order issued on October 4, 2006, and published in the Federal Register on October 24, 2006 (71 FR 62318), required the United States Enrichment Corporation (USEC) to protect certain information relating to its uranium enrichment test and demonstration facility (Lead Cascade Facility). Specifically, the order required USEC and other persons to employ the modified handling requirements for SGI-M relating to the interim measures to enhance security at the Lead Cascade Facility. As reflected in § 73.21(a)(1), the Commission later determined that the type of information described above should be subject to the requirements for SGI. Interim security measures relating to the other facility located onsite with the Lead Cascade Facility (the American Centrifuge Plant) are also designated as SGI. Therefore, there is no longer a discrepancy with respect to the information protection requirements for the two facilities.

destroyed pursuant to final §§ 73.22(i) and 73.23(i). This would probably amount to roughly half of the SGI-designated documents ten years or older.

Comment: A commenter asserts that it is impractical to have the NRC approve the decontrol of documents generated by other agencies and that sometimes the individual in an organization who made the original SGI determination is unavailable. The commenter suggests that the proposed text of §§ 73.22(h) and 73.23(h) be modified to allow other authorized individuals within the organization that made the original SGI determination to decontrol the document. Another commenter echoes this request.

Response: In response to these comments, the Commission is clarifying the text in §§ 73.22(h) and 73.23(h) to state that the authority to determine that documents originally containing SGI or SGI-M must be removed from the SGI or SGI-M category may be exercised by the NRC, with the approval of the NRC, or in consultation with the individual or organization that made the original determination.

Section 73.23.

Comment: A commenter asserts that for shipments of Category 1 materials, which are not routine, schedules and itineraries of a shipment constitute information that, if disclosed, could reduce the security of the shipment. For the more routine Category 2 RAMQC shipments, the commenter states that it is not clear from the proposed rule that relevant

Section 73.59.

Comment: One commenter stated that § 73.59 should be revised to permit a licensee to recognize a background check conducted in accordance with the final rule by another NRC or Agreement State licensee. The commenter believes that this change would help allow a licensee to sub-contract work to other licensees where it may be necessary to divulge SGI to the contracted licensee in order for the maintenance activity to be performed safely. The commenter's suggested revision would state that an "employee of an NRC or Agreement State licensee who has undergone criminal history and background checks in accordance with or equivalent to those required by 10 CFR 73.22(b) or 73.23(b)."

Response: Section 73.59 of the rule provides relief from the fingerprinting and criminal history records check requirements set forth in Section 149 of the AEA for limited categories of individuals set forth in § 73.59(1) through (9). Those categories of individuals are considered to be trustworthy and reliable by virtue of their occupational status and have either already undergone a background check or criminal history records check as a condition of their employment, or are subject to direct oversight by government authorities in their day-to-day job functions. The categories of individuals specified in § 73.59 include governmental employees at the federal, state or local level or certain NRC-certified representatives of the International Atomic Energy Agency. In addition, any agent, contractor, or consultant of those categories of individuals are also exempt if they have undergone equivalent criminal history and background checks to those required by §§ 73.22(b) or 73.23(b). The Commission has determined not to

a document containing SGI, but only marked with DOT markings, were transmitted to another individual, that individual would not know that SGI requirements apply to the document. Because DOT and SGI requirements differ, the recipient of the document containing SGI would likely not comply with all of the SGI handling requirements. The benefits of using NRC markings surely need not be quantified.

The Commission also does not consider it a useful measure to quantify how much additional material protected under the rule has historically been released to the public because of the lack of the rule's requirements. First, a relatively small quantity of SGI obtained by one determined individual for nefarious purposes could be more dangerous than a larger quantity of material obtained by several people with peaceful intentions. Second, the request misses the point that security orders issued since September 11, 2001, have imposed SGI protection requirements above and beyond those imposed by the current rule. There is no recent experience with the current rule as a baseline from which to make the requested calculation, even if such a calculation produced a useful measure.

Finally, with respect to a quantitative analysis of benefits in a backfit analysis, the Commission has determined that a backfit analysis is not necessary for this rule, as explained in the response to the previous comment.

B. *Analysis of changes made in the final rule to the text of the revised proposed rule.*

Change from "criminal history check" to "criminal history records check."

Throughout the rule, references to "criminal history check" have been revised to read

Minor change in terminology.

The phrase "delegate of the Executive Director for Operations" in § 2.709(f)(1) will be changed to "delegee of the Executive Director for Operations" to conform with the usage throughout the rest of § 2.709.

Section by section analysis of remaining changes to the proposed rule text.

Section 30.4 Definitions.

A definition of "quantities of concern" is added, which is identical to the definition of that term in parts 2 and 73. Defining that term in part 30 will assist licensees, applicants, and other persons subject to part 30 in determining the applicability to their activities of the requirements for the protection of SGI and SGI-M in part 73.

Section 30.32 Application for specific licenses.

In paragraph (j), the references to §§ 73.21 and 73.23 are modified to read "§ 73.21, 73.22, and/or 73.23, as applicable." This change correctly denotes the applicable sections of part 73 relating to a part 30 licensee's or applicant's protection against unauthorized disclosure of SGI and/or SGI-M. In addition, the phrase "subject to the requirements of part 73 of this chapter" is being deleted because byproduct material licensees are not subject to part 73 other

select a commercially available encryption system that the National Institute of Standards and Technology (NIST) has validated as conforming to Federal Information Processing Standards (FIPS). Safeguards Information designated as Safeguards Information-Modified Handling files shall be properly labeled to indicate the presence of Safeguards Information with modified handling requirements and saved to removable matter and stored in a locked file drawer or cabinet.

(3) A mobile device (such as a laptop computer) may also be used for the processing of Safeguards Information designated as Safeguards Information-Modified Handling provided the device is secured in an appropriate locked storage container when not in use. Other systems may be used if approved for security by the appropriate NRC office.

(h) *Removal from Safeguards Information-Modified Handling category.* Documents or other matter 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. Care must be exercised to ensure that any document or other matter 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 or other matter may be decontrolled will only be exercised by the NRC, with NRC approval, or in consultation with the individual or organization that made the original determination.

(i) *Destruction of matter containing Safeguards Information designated as Safeguards Information-Modified Handling.* Documents or other matter containing Safeguards Information shall be destroyed when no longer needed. The information can be destroyed by burning,

OPA PRESS RELEASE (DRAFT)

NRC ISSUES FINAL RULE AMENDING DESIGNATION AND HANDLING OF SAFEGUARDS INFORMATION

The Nuclear Regulatory Commission is issuing a final rule today that will amend its regulations on the designation and handling of security-related information known as "Safeguards Information," or SGI. SGI is a special category of sensitive unclassified information authorized under the Atomic Energy Act.

The rule, published in the *Federal Register* today, will be effective in ~~90~~ 120 days.

The final rule reflects changes in the threat environment since Sept. 11th, 2001, and the need to protect as SGI additional types of security information held by a broader group of licenses. The final rule incorporates public comments and new authority granted to the NRC by the Energy Policy Act of 2005. An original version of the proposed rule was published in February 2005, and a revised version was published for additional comment in October 2006.

Individuals provided access to SGI must have a valid "need to know" the information, and an authorization for access based on a background check for trustworthiness and reliability. Since the unauthorized release of SGI could harm the country's nuclear power plants and other facilities and materials regulated by the NRC, SGI must be protected from unauthorized disclosure and physically controlled. Inadvertent release and unauthorized disclosure may result in civil penalties while willful violation of SGI regulations is a felony.

###

Note: Draft prepared by OPA in coordination with Lead Program Office (OGC); still subject to EDO/Chairman approval.

Assurance That These Are the Minimum Restrictions Needed to Protect the Health and Safety of the Public or the Common Defense and Security

The requirements set forth in this final rule are the minimum restrictions the Commission finds necessary to protect SGI and SGI-M against inadvertent release or unauthorized disclosure which might compromise the health and safety of the public or the common defense and security. The final rule would cover those facilities and materials the Commission has already determined by regulation or order need to be protected against theft or sabotage. The categories of information constituting SGI and SGI-M relate to the types of facilities and the quantities of special nuclear material, source material and byproduct material determined by the Commission to be significant and therefore subject to protection against unauthorized disclosure pursuant to Section 147 of the AEA. Unauthorized release of SGI could reduce the deterrence value of systems and measures used to protect nuclear facilities and materials and allow for the possible compromise of those facilities and materials. Such disclosures could also facilitate advance planning by an adversary intent on committing acts of theft or sabotage against the facilities and materials within the scope of this rule. Further, the Commission has determined, pursuant to Section 147a.(3)(B) of the AEA, that the unauthorized disclosure of SGI, including SGI-M, 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 nuclear material or a facility.