

QUESTIONS RAISED DURING THE FEBRUARY 2009 WEBINAR SESSIONS

Related To	Question and Answer
1. Guidance	<p>Q: Will the issued rules effective 2/23/09 and requirements supersede the Site specific Order Response?</p> <p>A: No. The orders will remain in effect until the Commission relaxes the requirements of the orders in whole or in part. In those instances when the rule and an order appear to conflict with one another, the more stringent requirement must be applied.</p>
2. Guidance	<p>Q: If a specific extension is applied for prior to the effective date, will the licensee be in violation of the regulation while NRC is determining if the extension will be granted?</p> <p>A: Yes. Until the exception is granted, the licensee is obligated to comply with the rule.</p>
3. Guidance	<p>Q: Will the designation guide, marking guide, and standard practices and procedures guide be rolled up into the draft reg. guide? If not, why not?</p> <p>A: As a practical matter, the safeguards information designation guide will remain as a stand-alone product. The detail and policies that are addressed in key guidance documents such as the safeguards designation guide, regulatory guide and standard practices and procedures are subject to change as dictated by the Commission or regulatory requirement. Merging the key guidance documents could cause a significant delay when limited changes are required for one component of the composite document. The industry would be better served with the key guidance document existing independently of one another. The determination as to the publishing disposition of the safeguards information marking guide and standard practices and procedures guide are still being evaluated. Given that the documents are in different stages of concurrence, they may be published as stand-alone documents as they are approved. At any rate, the guidance documents will be made available for use to all licensees, applicants and certificate holders.</p>
4. Definition	<p>Q: Ref 73.22(a)(1)(ii) - Please provide criteria associated with the use of the term "easily discernable"?</p> <p>A: The phrase "not easily discernible to members of the public" was added to reflect the aspects of a licensee's or applicant's physical security system that can be readily observed by members of the public are not necessarily considered SGI.</p>
5. Definition	<p>Q: Reference 73.22(1)(xii) - Please identify the criteria associated with use of the term "engineering and safety analysis"?</p> <p>A: The criteria referenced in 10 CFR 73.22(a)(1)(xii) is that the engineering and safety analyses must be security related and is considered to be SGI only if they reveal "site specific details" about the physical protection of the facility or source material, byproduct material, or SNM.</p>

QUESTIONS RAISED DURING THE FEBRUARY 2009 WEBINAR SESSIONS

6. Transportation
- Q: The information in the Federal Register seems to conflict between the guidance and the responses to comments as follows:
- Current Code language in the Federal Register: § 73.23 Protection of Safeguards Information—Modified Handling: Specific Requirements..... ; manufacturers and distributors of items containing source material, or byproduct or special nuclear material in greater than or equal to Category 2 quantities of concern; transportation of more than 1000 Tbq (27,000 Ci) but less than or equal to 100 grams of spent nuclear fuel;..... research
- Comments and Response:
- According to the commenter, it is unclear how the originator of a RAMQC Category 2 will be able to assure that each carrier meets the requirements to handle SGI-M. Response: The Commission has determined that information relating to the transportation of Category 2 RAMQC need not be protected as SGI-M and may be shared on a “need-to-know” basis. Does Cat 2 count as SGI-M or not?
- A: Category 2 security related information is not safeguards information-modified handling. However, Category 2 security related information is considered sensitive information. Licensees are expected to protect such security related information from unauthorized disclosure and limit access to those individuals that have a need to know.
7. Transportation
- Q: Do we need to Safeguard all information utilized in making dry cask movements?
- A: No. The protection of security information for dry cask storage or movements is similar to spent fuel transportation. Many components of dry cask movements are public information or easily observed by the public. The NRC has developed and issued a SGI Designation Guide to assist licensees or other stakeholders in determining what information should be protected as SGI. In short, information that could assist an adversary in developing or carrying out an attack would be considered SGI.
8. Transportation / Access
- Q: Are these non Power Reactor stakeholders going to have a data base such as PADS for us to review to verify status of individuals?
- A.: The NRC does not own, operate nor control the Personnel Access Data System. The Personnel Access Data System is not a tool that’s used to verify access to safeguards information. The Commission has no immediate plans for creating a similar type of database for stakeholders to use to verify the access status of individuals.
-

QUESTIONS RAISED DURING THE FEBRUARY 2009 WEBINAR SESSIONS

9. Access Q: Under the new rule, can anyone establish an SGI program without obtaining NRC approval?
- A: Yes, anyone can establish a safeguards information program, but the establishment of that program does not mean that it complies with the requirements of the rule, nor that it meets the rigors of NRC requirements. The establishment of a safeguards information program is merely one component that must be complimented with a need-to-know determination, and satisfactory completion of all elements of the background check requirement before one gains access to safeguards information.
10. Access Q: What is the durability of the newly required background checks required per 73.22(b)(2), is it required on some recurring basis?
- A: The rule does not mandate a reinvestigation. However, the background check must be sufficient to support the trustworthiness and reliability determination so that the person performing the check and the Commission have assurance that granting the individual access to SGI does not constitute an unreasonable risk to the public health and safety or common defense.
11. Access Q: If you already have prints on file and have verified that individual's identity, can you have them fill out the PHQ from NEI and not have to re-verify their ID at that time. (I have some individuals who are not in the immediate area and they would have to travel to verify their ID.)
- A: If the fingerprints on file have previously been submitted to the FBI, through the NRC, then you need not re-accomplish that element of the background check requirement. Use of the PHQ from NEI is permissible and will satisfy the other elements of the background check requirement.
12. Access Q: If an individual was badged in PADS for UAA, can we use that information to grant SGI and use the Re-investigation due date from PADS?
- A: Yes you can, but the rule does not prescribe a reinvestigation requirement for access to safeguards information.
13. Access Q: If the re-investigation is set up on a 5 year basis and I had printed someone for SGI 2 years ago, do I need to reprint now or 5 years from the original fingerprint date?
- A: You do not need to reprint now. The rule does not prescribe a reinvestigation requirement for access to safeguards information.
14. Access Q: What about psychological screening?
- A: Psychological screening is not a prerequisite for access to SGI.

QUESTIONS RAISED DURING THE FEBRUARY 2009 WEBINAR SESSIONS

15. Access Q: What adjudication standards are to be used when reviewing FBI Criminal History report?
- A: 10 CFR 73.57(c) states the prohibition for use of information received from the FBI when it is used to determine access to a nuclear power facility or access to safeguards information. There are no stated disqualifying criteria, for access to safeguards information, stated in the rule. Reviewing officials however, must be judicious in their application of the trustworthiness and reliability determination such that disclosing safeguards information to the individual (i.e. the subject of the trustworthiness and reliability determination) does not constitute an unreasonable risk to the public health and safety or common defense and security.
16. Access Q: Is there a requirement for developed references or just personal references provided by the individuals.
- A: The rule does not differentiate between stated personal references and developed references. The person performing the check and reviewing official must have a level of assurance that the procedures used to complete the elements of the background check are sufficient to make an informed trustworthiness and reliability determination.
17. Access Q: Will individuals with existing government issued security clearances, such as DOE or USNRC, be exempt from the background investigation requirement? If so, what will be the expected documentation to be maintained to support this exception?
- A: No, they will not be exempt from meeting the background check requirement, but no additional fingerprinting is required for access to safeguards information. The fact that they have an active Federal security clearance can be used to meet the fingerprint and other elements of the background check requirement as prescribed by 10 CFR 73.22 and 73.23. When an active Federal security clearance is used to meet the fingerprinting and other elements of the background check requirement, the Reviewing official must maintain a record of official notification stating that the individual possesses an active Federal security clearance.
18. Access Q: Plant employees not granted access to SGI are not considered "Public"?
- A: No, they are merely employees without access to safeguards information. Employees typically undergo some form of an employment screening process and that differentiates them from "Public" members; if that is what you're referencing in your question. Nonetheless, the implemented of the information protection system must be sufficiently applied so as to deny SGI access to those personnel not authorized access to safeguards information.

QUESTIONS RAISED DURING THE FEBRUARY 2009 WEBINAR SESSIONS

19. Access Q: Is a credit check a necessary part of a "reliability and trustworthiness" determination under 73.22(b)(2)?
- A: No. The basic requirement for a background check is based upon a Federal Bureau of Investigation criminal history records check (including verification of identity based on fingerprinting), employment history, education, and personal references. The trustworthiness and reliability determination takes into account the results of the background check and the individual characteristics of the individual.
20. Access Q: May the Industry utilize PADS to store and track SGI Background Checks and FBI Criminal History Checks (this would be for those personnel who have not applied for Unescorted Access)?
- A: The NRC can not make policy for a database that it does not own nor operate.
21. Access Q: You mentioned acceptance of confirmation of fingerprints or background information transferred from other agencies for credit towards background investigations. Are e-mails from NRC, DHS, DOE, FBI, State Police, PADS coordinator, other licensees, etc. sufficient for confirmation, in lieu of letterhead memo? For example, if I get an e-mail from NRC ADM/DFS/PSB, it should suffice to confirm and credit for whether they have fingerprints on record, or what kind of current clearance they have, etc. It may even be on a spreadsheet attachment, etc.
- A: Confirmation of an active Federal security clearance may be made in several forms. The manner in which that confirmation is transmitted and/or received is dependant upon the organization or agency that is communicating the information. Typically, Federal Agencies do not rely upon the use of emails to confirm active Federal security clearances. Compliance with guidelines associated with the protection of privacy act information must always be at the forefront when sharing such sensitive data.
22. Access Q: 2 forms of photo ID are restrictive with respect to most individuals. What other forms of government-issued ID (other than driver's license) would be acceptable?
- A: That would depend on the purpose for the identification verification. Since no indicate was stated for the purpose of the identification verification, the assumption is that the effort is related to a fingerprinting initiative. Jurisdictions across the country have various requirements for identification as it relates to fingerprinting. Typically, they rely upon government issued credentials that state physical characteristics such as a driver's license, a passport or a Federal, State or Tribal issued identification card. Some jurisdictions may have an expansive list of identifications credentials that are accepted for the purpose of fingerprinting while others may be very restrictive in what can be accepted.

QUESTIONS RAISED DURING THE FEBRUARY 2009 WEBINAR SESSIONS

23. Access

Q: If an SGI cleared employee changes employers i.e. Moves from licensee to licensee or from NRC to licensee or licensee to NEI, for example, do they have to go through the process again, or take credit for previous SGI requirements having been met?

A: The lapse in time between employment must be taken into consideration, as should information as to whether the access was terminated under favorable condition, before a decision is made to accept the trustworthiness and reliability determination from a previous employer. 10 CFR 73.57(b)(5) makes allowance for the acceptance of fingerprints of an employee of a licensee, contractor, manufacturer, or supplier that has been granted access to a nuclear power facility or to safeguards information if that access is based in part on a criminal history records check. The criminal history check file may be transferred to the gaining licensee in accordance with the provision of 10 CFR 73.57(f)(3). The reviewing official must verify that all elements of a background check have been conducted and make a trustworthiness and reliability determination based upon the information made available to him or her.

24. Access

Q: If an employee has been with the same employer for a number of years, say 8 or 10 yrs and was SGI cleared under the old Rule, was finger printed many years ago; what new activity is expected, that needs to be done to meet the new Rule requirements?

A: If the employee has not been the subject of a background check as prescribed by 10 CFR 73.22(b) and 73.23(b), he or she would have to undergo a background check to meet the SGI access requirements, but is not required to resubmit fingerprints to NRC.

25. Access

Q: Was the intent of the Regulator to follow the current AA model?

A: No. The staff believes that the requirements for unescorted access within a commercial nuclear power plant or unescorted access to highly irradiated nuclear fuel should be more stringent than the access requirements for SGI. The prerequisites for access to safeguards information is considerably less stringent than those used to determine unescorted access authority. The staff does not intend for the two access requirements to conflict or cause an unnecessary burden on licensees.

26. Access

Q: There is no specific or implied expiration or required update to these background checks. What value is there in doing this SGI background once and not doing it again at some period? The way this reads I could do a background once and carry it on the books indefinitely.

A: There is no follow-up requirement for additional background or fingerprint checks required by the regulation. Rulemaking and regulatory oversight for information security requirements, is a continuing and on-going initiative. If there is any requirement for a periodic or follow-up background check, it would be subject of future rulemaking.

QUESTIONS RAISED DURING THE FEBRUARY 2009 WEBINAR SESSIONS

27. Access

Q: The other problem is the verification of "education". Access Authorization is only required to do this when it is claimed as part of the 5 year history to complete a UA background. Why does access to SGI seem to be different?

A: The background check portion for access to SGI requires that a person's education be verified as part of the trustworthiness and reliability determination. The suitability of a person's education to their job responsibilities is considered a key attribute in determining a person's trustworthiness and reliability.

28. Access

Q: At FENOC we are using the current Access Authorization requirements for unescorted access to meet this background requirement. How are others in the industry going to meet and document this if they are not using the Access Authorization group at their Sites?

A: The background check requirements for access to Safeguards Information (SGI) were not intended to be more comprehensive or restrictive than what is required for unescorted access to a commercial nuclear power plant. We will review the access requirements for both SGI and unescorted access to ensure that SGI access is not more cumbersome or restrictive. The regulation requires that SGI access records/documentation be maintained by the licensee granting such access.

29. Protection while in use or storage

Q: Why would the NRC consider additional controls for thumb drives that contain encrypted information when the same information is allowed to be transmitted electronically (i.e., encrypted)?

A. Removable magnetic medium, used to store Safeguards Information, must be properly marked and stored in a security storage container when not in use. The rule makes no distinction between the marking and safekeeping requirement for encrypted safeguards information on removable magnetic media devices and the marking and safekeeping requirements for unencrypted safeguards information on removable magnetic media devices.

30. Marking

Q: What is roll of the designation guide? Is this enforceable to licensees or does it continue to be internal to the NRC?

A: The safeguards information designation guide is and will continue to be a valuable key guidance document available for use by the nuclear industry. The safeguards designation guide will not be used to support an enforcement action. All persons that have access to safeguards information have a continuing obligation to protect it against inadvertent release and unauthorized disclosure. As such, the safeguards information designation guide is intended to aid personnel in properly identifying and designating safeguards information that they are obligated to protect.

QUESTIONS RAISED DURING THE FEBRUARY 2009 WEBINAR SESSIONS

31. Marking

Q: What now is the status of the NRC Designation Guide for Safeguards Information? Have the applicable portions to the industry been incorporated into the forth coming Reg Guidance on SGI? Are we as an industry going to be obligated by this guide over and above all this new SGI regulation

A: The safeguards information designation guide continues to be a key guidance document used by NRC and shared with industry. The new rule has not incorporated all of the guidance of the designation guide and no, industry is not obligated to use the designation guide, but is responsible for the proper identification, marking and safekeeping and storage of safeguards information.

32. Marking

Q: The addition of marking 1st page of SGI document, how is that being applied to historical documents that are vaulted as for example previous revision to PSP's?

A: The Commission noted, in the statements of consideration of the final rule, that it does not expect licensees or applicants to 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 10 CFR 73.22(d)(1). Historical documents that are vaulted need not be removed from the vault solely for the purpose of meeting the marking requirement. As those documents are removed from the vault for use, i.e. transmitted, modified or used as an attachment, they must be marked as required by 10 CFR 73.22(d)(1).

33. Marking

Q: It appears that the portion marking requirement, in the new rule, is limited to transmittal documents, is that an accurate assessment?

A: Yes. The new rule has relaxed the portion marking requirements that were evident in the previous version of the rule. Portion marking is only required for correspondence to and from the NRC (i.e. cover letters, but not attachments) that contain safeguards information.

34. Marking

Q: 73.22 (d)(1)(i) - (iii) requirements are to be applied to the first page of the SGI document. What is the expectation for electronic media bearing these markings?

A: The rule makes no distinction, with respect to the marking of electronic documents and hardcopy documents or other matter containing safeguards information. Documents or other matter containing safeguards information must be marked according to 10 CFR 73.22(d) and 73.23(d).

QUESTIONS RAISED DURING THE FEBRUARY 2009 WEBINAR SESSIONS

35. Marking

Q: For engineering information determined to be SGI. At what point would engineering design for security systems be considered SGI? And would the employees of the design firm then need to be screened and granted access to SGI? Thank You.

A: The rule doesn't address engineering designs. It does however state that detailed security related site-specific drawings, diagrams, sketches etc. that substantially represent the final design feature of the physical security system are considered safeguards information. Engineering and safety analyses (that are security related) and revealing site-specific details of the facility or material and that can reasonably be expected to aid an adversary, must be protected from unauthorized disclosure.

36. Marking

Q: Must the new marking requirements be contained on the first page of the document containing SGI data; or may it be placed on a cover page which is attached to the SGI document?

A: The marking requirements, as stated in the rule, must be conspicuously placed on the first page of the document. If the first page of the document is the cover page, then the required markings would be conspicuously placed on the cover page/first page. When a transmittal letter is attached to a safeguards information document, and not a permanent part of the document, the actual first page of the safeguards information document itself must be marked according to 10 CFR 73.22(d) and 73.23(d).

37. Marking

Q: Is it possible for a materials licensee (such as an M&D) to mark information as SGI-M that should be labeled as SGI?

A: Material licensees, such as Manufacturers and distributors of items that are addressed in 73.23, can not err by marking that type of information as safeguards information-modified handling. Only that information as referenced in 10 CFR 73.22 meet the requirement for safeguards information.

38. Marking

Q: Containers cannot be identified as containing SGI...what about rooms, individuals carrying SGI (currently we require those with SGI to keep it in bright pink folders and to wear a badge indicating they have possession of SGI. These are visual reminders to assist the individual in maintaining control).

A: Security storage containers can not be marked to indicate that they house safeguards information. Marking locked security storage containers to indicate they contain SGI may assist in identifying the location of SGI. If a room has security storage containers and those security storage containers house safeguards information, the marking of the room to indicate that it holds safeguards information would violate the spirit and intent of the rule and should not be done. The use of devices that strengthen day-to-day information security awareness, such as the use of bright pink folders or the wearing of a particular badge is permissible and should be viewed as a security enhancer.

QUESTIONS RAISED DURING THE FEBRUARY 2009 WEBINAR SESSIONS

39. Marking

Q: 73.22(h) discusses who can decontrol SGI. We are assuming that a licensee can decontrol material they have created or material created by others with their approval.

A: That is correct, but care must be taken to ensure that documents or other matter that are decontrolled not meet the criteria for continued designation as safeguards information and not disclose safeguards information in some other form or be combined with other unprotected information to disclose safeguards information.

40. Safekeeping and Storage

Q: Is the use of an encrypted volume within a stand-alone computer (i.e. double password protected) located within a controlled access area an acceptable alternative to the new rule language?

A: No. The rule is specific in its requirement for the protection of safeguards information as it is stored, processed or produced on electronic systems. Controlled access area is not synonymous with security storage container and the rule makes no assertion that encryption is comparable to or a substitute for security storage containers. A controlled access area can be accredited for open storage of safeguards information, but absent that accreditation by NRC, safeguards information must be stored in a security storage container when not in use.

41. Safekeeping and Storage

Q: Is the practice of carrying encrypted SGI on a flash drive acceptable? Some people understood from the Webinar that this would not be allowed under the new rule which makes little sense with respect to the ability to email encrypted information.

A: Safeguards information may be saved to removable storage medium, and while unattended, that removable storage medium must be stored in a security storage container. When removable storage medium is used to store safeguards information, users must ensure that the medium is properly marked to indicate the presence of safeguards information as prescribed by 10 CFR 73.22(d) and 73.23(d).

42. Safekeeping and Storage

Q: Is the practice of carrying unencrypted SGI on an encrypted volume in a dedicated hard drive acceptable?

A: If your question is with respect to transporting the hard drive from an authorized place of use or storage, the hard drive can be used to transport safeguards information if the hard drive is properly marked and packaged as prescribed by 10 CFR 73.22(f) or 73.23(f).

43. Reproduction

Q: Can we get a list of government approved copier memory purge software good for use?

A: Such a list is unavailable at this time, but we will continue to research this issue and respond to all interested parties as soon as possible.

QUESTIONS RAISED DURING THE FEBRUARY 2009 WEBINAR SESSIONS

44. Transmission Has NRC considered modifying Section 73.22(g) to permit the secure electronic transfer (e-mail) of SGI information from a computer with an internet connection? The requirements of 73.22(f) and 73.22(g) seem to contradict one another. Clarification is needed.
- A: Yes the NRC has considered that initiative and made allowances for such an act to occur. 10 CFR 73.22(f)(3) spells out the requirements for using the internet to securely transmit encrypted safeguards information.
- As to the second part of your question; 10 CFR 73.22(f) states that safeguards information must be transmitted through NRC approved secure electronic devices. It also states that safeguards information may be transmitted through electronic mail provided that the information is compliant with Federal Information Processing Standard [FIPS 140-2] or later encryption that has been approved by NRC.
- 10 CFR 73.22(g) addresses the use of stand-alone computers when safeguards information is stored, processed or produced. Safeguards information that is stored, processed or produced on a stand-alone computer can be encrypted, using NRC approved FIPS 140-2 or later methods, then migrated to an internet connected computer for the purpose of transmission through electronic mail. The internet connected computer is merely a transmission and receipt device for a FIPS 140-2 or later compliant encrypted file.
45. Transmission Q: FIPS 140-2 contains four levels of security. Which level satisfies the requirements of 73.22 and 73.23?
- A: Any level, within FIPS 140-2 or later, may be adopted and that choice communicated to the NRC for approval.
46. Transmission Q: 73.22(f)(2) discusses external transmission of documents. This appears to be discussing transmitting documents outside of our company, not within our company. Does this mean that when we send SGI documents that have been properly sealed in double envelopes within our company, but between our different locations which could be in different cities or states, we have to use these commercial carriers or US mail and cannot use our inner company mail system that does not have individual tracking?
- A: Computer tracking capabilities are necessary to aid in quickly determining the location of the information so that the risk of unauthorized disclosure may be minimized. If the inner company mail system relies upon personnel that are authorized access to safeguards information pursuant to the access requirements of 10 CFR 73.22(b), then you need not rely upon commercial delivery companies that provide service with computer tracking features, U.S. first class, registered, express, or certified mail. The procedures for the external transmission of safeguards information must comply with the requirements of 10 CFR 73.22(f) and 73.23(f).