

Frequently Asked Questions
About
Safeguards Information -Modified Handling

Agreement State Questions

1. Will Agreement States have access to Safeguards Information (SGI)?
 - A. The Governor of a State or his or her designated State employee representative, the State Radiation Control Program Directors and State Homeland Security Advisors or their designated State employee representatives, and Agreement State employees conducting security inspections on behalf of the NRC under an agreement executed under section 274.i of the Atomic Energy Act (AEA), may have access to SGI. These individuals may have access to SGI provided they have an established "need to know" for the information. As indicated in 10 CFR 73.59 "Relief from Fingerprinting and Criminal History Records Check for Designated Categories of Individuals" (71 FR 33989), these individuals are considered trustworthy and reliable to receive SGI by virtue of their occupational status and have either already undergone a background or criminal history check as a condition of their employment, or are subject to direct oversight by government authorities in their day-to-day job functions. Under the "Fingerprinting Relief" rule, if individuals in the categories described above need to know SGI to perform a job function and are otherwise qualified to receive it under existing Commission regulations and orders, they may have access to SGI without being fingerprinted or undergoing a criminal history check.
2. Are States going to be inspected for SGI-M?
 - A. State handling of SGI-M will be reviewed in some fashion; the details are to be worked out.
3. Can the NRC give Agreement States specific guidance on handling FOIA request for SGI-M? Do the States refer such requests to NRC? Does NRC need to tell FOIA requesters that the material can not be release?
 - A. See the answer to question 4 below.
4. Do States have authority to protect SGI-M? What about States that have no statute to protect SGI-M, how do they protect it from a public request?
 - A. States must protect SGI-M from unauthorized disclosure and otherwise must handle SGI-M in accordance with applicable NRC requirements governing the handling of SGI-M that have been imposed by order. States and State employees are subject to these requirements as a matter of Federal law and may not disclose SGI-M to any person who does not have a "need to know" and who has not been fingerprinted and has had a federal criminal history check and determined to be trustworthy and reliable. States' protection of SGI is not

Enclosure 4

Frequently Asked Questions
About
Safeguards Information -Modified Handling

dependent on State FOIA-type laws or any other State laws. States may not disclose SGI-M in response to FOIA-type laws and requests or any other State laws or requests. States which are granted access to SGI (or SGI-M for the SGI subject to modified handling requirements) must protect it from unauthorized disclosure as a matter of Federal law, and no State law can nullify the AEA's prohibition (and NRC's implementing regulations and orders) against unauthorized disclosures. States and State employees are required by Federal law to protect SGI-M from unauthorized disclosure. It is a violation of the AEA and the NRC Order that will be issued if SGI is not so protected. Willful violations are felonies subject to criminal sanctions, including imprisonment for any person, State employees included, who willfully violates NRC's SGI-M requirements. This prohibition against unauthorized disclosure and the SGI-M handling requirements that will be issued by order apply to States and their employees and do not depend on States having a State law means of protecting SGI-M.

5. Is SGI-M sent over e-mail? We have received e-mail messages marked "Safeguards Advisory"
 - A. SGI-M may be sent by e-mail only if protected by a NIST certified encryption program. Official correspondence to NRC typically is handled via hard copy and through the NRC's document control center. Although NRC has, in response to the changing threat conditions, sent out "Safeguards Advisories," they were not safeguards information.

6. License renewals for Agreement State licensees may contain SGI-M. Will there be guidance for renewal applications containing SGI-M?
 - A. Licensees submitting renewals containing SGI-M must properly identify and protect the information sent to Agreement States and to NRC. SGI-M must be marked and properly packaged prior to being sent. Agreement States should identify those individuals within their organization authorized to receive the SGI-M information as indicated in the final rule for 10 CFR § 73.59 "Relief from Fingerprinting and Criminal History Records Check for Designated Categories of Individuals," (71 FR 33989) . If an Agreement State chooses not to receive SGI-M, the licensee will have to make certain that no SGI-M is contained in the application.

NRC document, DG-SGI-1, "Designation Guide for Safeguards Information" has been developed to provide clearer understanding of what is or is not SGI-M. Generally, licensee's specific design and operational control features, used for health and safety purposes and submitted as part of the license application or renewal process, are not considered SGI-M. Facility specific design and

Enclosure 4

Frequently Asked Questions
About
Safeguards Information -Modified Handling

operational features would be SGI-M when they are identified as being used for security purposes to protect the radioactive material from the theft, diversion, or sabotage. Each Agreement State should develop its own procedures for processing applications containing SGI-M.

7. How are we to handle new applicants - NRC and Agreement State?
 - A. When an NRC or Agreement State license reviewer determines that a license can be issued, notification should be given to the Director, Office of Nuclear Security and Incident Response, U.S. NRC, so that the order imposing the Compensatory Measures can be issued along with the new license. This procedure should be followed unless and until the Compensatory Measures are incorporated into the Code of Federal Regulations.

8. Is it an automatic assumption that government employees are deemed trustworthy by virtue of their position?
 - A. As indicated in 10 CFR 73.59 "Relief from Fingerprinting and Criminal History Records Check for Designated Categories of Individuals" (71 FR 33989), these individuals are considered trustworthy and reliable to receive SGI by virtue of their occupational status and have either already undergone a background or criminal history check as a condition of their employment, or are subject to direct oversight by government authorities in their day-to-day job functions. Such employees must also, however, be knowledgeable of the specific requirements for protecting SGI-M, have the use of a lockable storage container, and have an employment specific need-to-know.

9. Will licensees have to send their responses to the Orders to the Agreement States also? or will NRC send copies of the responses?
 - A. Each licensee will be instructed to respond directly to NRC. For each Agreement State licensee, NRC will provide the State with a copy of the Order, CMs, and the licensee's response.

10. Will the Agreement States get copies of the CMs and responses?
 - A. Each licensee will be instructed to respond directly to NRC. For each Agreement State licensee, NRC will provide the State with a copy of the Order, CMs, and the licensee's response.

Enclosure 4

Frequently Asked Questions
About
Safeguards Information -Modified Handling

11. Who will the Order be mailed to in the Agreement States?
- A. All SGI-M material transmitted from NRC to a State program will be addressed to the Program Director (presuming the program chooses to receive SGI-M) and the State Liaison Officer. The Program Director may authorize other State program staff to have access to the SGI-M, however, to effectively control the distribution from NRC, it will be addressed only the Director.
12. Will NRC have to “clear” (authorize) individuals from each Agreement State?
- A. The Governor of a State or his or her designated State employee representative, the State Radiation Control Program Directors and State Homeland Security Advisors or their designated State employee representatives, and Agreement State employees conducting security inspections on behalf of the NRC under an agreement executed under section 274.i of the AEA, may have access to SGI. These individuals may have access to SGI provided they have an established "need to know" for the information. As indicated in 10 CFR 73.59 “Relief from Fingerprinting and Criminal History Records Check for Designated Categories of Individuals” (71 FR 33989), these individuals are considered trustworthy and reliable to receive SGI by virtue of their occupational status and have either already undergone a background or criminal history check as a condition of their employment, or are subject to direct oversight by government authorities in their day-to-day job functions.
13. What is the role of Agreement State with regard to SGI-M? How will they get SGI-M materials.
- A. The Agreement States may choose their role: participate or not participate. If a State program chooses to participate, it will get SGI-M from NRC and the licensees. It may also generate SGI-M during inspections, licensing reviews, etc.

Enclosure 4

Frequently Asked Questions
About
Safeguards Information -Modified Handling

14. What documentation will the Non-Agreement States receive in the future? Of particular interest at this time is the list of licensees that is described as "sensitive information."
- A. Since the Non-Agreement States do not have regulatory responsibility for health and safety of AEA materials licensees, their "need-to-know" SGI-M may be difficult to establish. However, if situations arise where Non-Agreement States request SGI-M determining their "need-to-know" will necessarily be addressed on a case-by-case basis with the same overall common defense and security objectives as for AEA materials licensees.
- As indicated in 10 CFR 73.59 "Relief from Fingerprinting and Criminal History Records Check for Designated Categories of Individuals" (71 FR 33989), the individuals identified in the rule are considered trustworthy and reliable to receive SGI by virtue of their occupational status and have either already undergone a background or criminal history check as a condition of their employment, or are subject to direct oversight by government authorities in their day-to-day job functions.
15. Who is going to inspect the implementation of Compensatory Measures? What frequency?
- A. Since the CMs are requirements for the common defense and security of the United States, inspection and enforcement are NRC's responsibilities. Nevertheless, given the closer relationship between the Agreement States and their licensees, it was decided, in order to be more efficient and effective, for the States to inspect them. Some states have accomplished this under an Agreement pursuant to section 274i of the AEA (the "standard" Agreements, for protecting public health and safety, are authorized by section 274b of the AEA). A temporary instruction (TI) for the initial inspection of Compensatory Measure implementation has been developed. Generally, when a TI is completed, it is evaluated for incorporation into the routine inspection program.
16. For the States that do the Compensatory Measure inspections for the NRC, will it become part of the IMPEP review?
- A. No. IMPEP is designed only to evaluate the performance of a regulatory program acting under its own authority. Inspections of CM compliance by State inspectors will be conducted as designees of NRC, acting under NRC authority. The NRC Regional Offices will evaluate the state inspections.

Enclosure 4

Frequently Asked Questions
About
Safeguards Information -Modified Handling

17. If the States inspect implementation of the Compensatory Measures, will the NRC inspect the States?
- A. NRC Regional offices evaluate the inspections performed by the Agreement States.
18. Who is responsible for enforcement?
- A. Because the Orders imposing Compensatory Measures are issued by the NRC under its authority for common defense and security, the NRC is responsible for enforcement.
19. NRC sent out a letters to licensees requesting names of individuals to receive SGI-M. Do the Agreement States need to submit similar list of individuals in the States that will receive SGI-M?
- A. No. The Governor of a State or his or her designated State employee representative, the State Radiation Control Program Directors and State Homeland Security Advisors or their designated State employee representatives, and Agreement State employees conducting security inspections on behalf of the NRC under an agreement executed under section 274.i of the AEA, may have access to SGI. These individuals may have access to SGI provided they have an established "need to know" for the information. As indicated in 10 CFR 73.59 "Relief from Fingerprinting and Criminal History Records Check for Designated Categories of Individuals" (71 FR 33989), these individuals are considered trustworthy and reliable to receive SGI by virtue of their occupational status and have either already undergone a background or criminal history check as a condition of their employment, or are subject to direct oversight by government authorities in their day-to-day job functions.
20. Do the Agreement States have to pass the same rules for protecting SGI-M as required by Orders for the irradiator and manufacturing and distribution licensees?
- A. Program directors should consult their agency legal advisor for their State's requirements. See the answer to question 4 above.

Enclosure 4

Frequently Asked Questions
About
Safeguards Information -Modified Handling

21. Will NRC issue licenses to all the Agreement State Licensees?
- A. No. If a person holds a license issued by an Agreement State to acquire, possess, and use source, byproduct or special nuclear material, that person is subject to the jurisdiction of the NRC for the purposes of common defense and security. No additional license document is required.
22. What happens if a state licensee, or the state program itself for that matter, is unwilling or unable to accept and protect SGI-M?
- A. There are two questions:
(1) What happens if a State licensee is unwilling or unable to accept and protect SGI-M?
(2) What happens if a State program is unwilling or unable to accept and protect SGI-M?
- In either case, the party will not be given the SGI-M, or authorized by NRC to receive it from anyone else. Since the Compensatory Measures are SGI-M, the party will not be able to receive them. For a licensee, this means that the licensee will be unable to comply with the Compensatory Measure requirements. NRC will issue an order prohibiting the licensee to engage in licensed activities requiring Compensatory Measures. For a State program, this means that the program will be unable to participate in evaluation of licensee response to the Compensatory Measure orders, or in the inspection of licensee compliance with the orders. The program will be unable to receive SGI-M information from the licensee related to any interaction between the licensees Compensatory Measure requirements and their health and safety requirements. Otherwise, the State will continue to regulate the licensee's health and safety program. In any case, if either a licensee or State employee willfully violates the order, they are subject to criminal prosecution and imprisonment. They should read with the utmost care the "Modified Handling Requirements for the Protection of Certain Safeguards Information (SGI-M)," which is provided to every licensee with the Order and NRC Regulatory Issue Summary 2003-08, "Protection of Safeguards Information from Unauthorized Disclosure," April 30, 2003.

Safeguards Information (General)

23. The definition of Safeguards Information does not mention licensees, applicants or Agreement States.
- A. No, the definition applies to security information, that if disclosed could adversely increase the risk of a malevolent act. It applies to all who have access to the information.

Enclosure 4

Frequently Asked Questions
About
Safeguards Information -Modified Handling

24. Can foreign nationals have access to SGI-M?

A. Yes, there is no prohibition against foreign nationals having access to SGI-M.

However if the foreign nationals are employees of the State, they may have access to SGI provided they have an established "need to know" for the information. As indicated in 10 CFR 73.59 "Relief from Fingerprinting and Criminal History Records Check for Designated Categories of Individuals" (71 FR 33989), these individuals are considered trustworthy and reliable to receive SGI by virtue of their occupational status and have either already undergone a background or criminal history check as a condition of their employment, or are subject to direct oversight by government authorities in their day-to-day job functions. Under the final rule, if individuals in the categories described above need to know SGI to perform a job function and are otherwise qualified to receive it under existing Commission regulations and orders, they may have access to SGI without being fingerprinted or undergoing a criminal history check.

However, if the foreign national is an employee of the licensee, all other requirements for need-to-know access to SGI-M and a determination of trustworthiness, in accordance with the order, including fingerprinting and a federal criminal history check, must be followed.

25. Are there sample programs for control of Safeguards Information (other than irradiators) which the irradiator licensees can build upon?

A. Other NRC licensees, such as commercial power reactors, have programs in place for the protection of Safeguards Information. However, the handling and storage requirements for these licensees are more stringent than required for irradiator licensees. The "Modified Handling Requirements for the Protection of Certain Safeguards Information (SGI-M)," issued with the Order, outlines the basic concepts of a fundamentally sound program for protection of SGI-M. NRC will be developing specific guidance for licensees to use in developing their programs for control of SGI-M.

26. Why don't individuals need security clearances for access to SGI-M like is required for SECRET information?

A. SECRET information is government classified information that requires government background checks as mandated by law. Safeguards Information is covered by the Atomic Energy Act of 1954, as amended, and authorizes the NRC to determine what types of security information for radioactive materials are considered under the AEA. Since the information covered by Section 147 of the

Enclosure 4

Frequently Asked Questions
About
Safeguards Information -Modified Handling

AEA does not rise to the level of National Security Information or Restricted Data, a government security clearance is not required. However, a government security clearance can be used as the basis for determining the trustworthiness of an individual for authorizing access to SGI-M.

27. Does §73.21 apply to Irradiator Licensees?
- A. No. However, the proposed rule for 10 CFR 73.22 is proposing that the NRC amend its regulations for the protection of SGI to protect SGI from inadvertent release and unauthorized disclosure which might compromise the security of nuclear facilities and materials. The amendments would affect certain licensees, information, and materials not currently subject to SGI regulations, but which are within the scope of Commission authority under AEA, as amended. As required in Section 147 of the Atomic Energy Act of 1954, as amended, the Commission is prescribing, by Order, that the security measures for the protection of byproduct material, used in panoramic and underwater irradiators, be protected from unauthorized disclosure.
28. Is all this discussion about SGI-M a decided issue or is the idea in a formative stage
- A. The Commission has determined that the information about security measures for byproduct materials, in quantities used in panoramic and underwater irradiators, should be protected from unauthorized disclosure as safeguards information. Because §73.21 does not apply to these licensees, the minimum restrictions needed to protect safeguards information, appropriate to irradiator licensees, have been formulated and are being issued with the Order. The marking "Safeguards Information - Modified Handling" (SGI-M) is being used to distinguish safeguards information for irradiator and other materials licensees from safeguards information that must be protected in accordance with 10 CFR 73.21. However, the Order regarding "Safeguards Information - Modified Handling" (SGI-M) will be superseded when NRC's proposed 10 CFR § 73.22 is made final.
29. How are our corporate headquarters kept informed about SGI-M and the Orders?
- A. NRC headquarters will keep licensee corporate headquarters informed. Orders and measures will be sent directly to sites and corporate headquarters copied if the licensee has requested headquarters personnel to have access to SGI-M and the NRC has authorized. If not, then copies of the orders without SGI-M will be sent to licensee headquarters as a means to keep them informed.

Enclosure 4

Frequently Asked Questions
About
Safeguards Information -Modified Handling

30. Why are we doing all this protecting of information, when there are the same types of facilities in other countries that are not protecting there design and operational information.
- A. While there are many irradiator facilities worldwide that have similar design and operational features used to comply with health and safety licensing requirements, these features do not have to be protected from unauthorized disclosure. When a specific design or operational feature of a facility is used as a security measure to protect the byproduct material against theft, diversion, or sabotage, then, that fact and the particular details or capabilities of how a feature is used for security become safeguards information and must me protected from unauthorized disclosure.
31. Do you recommend having SGI-M in a separable document (for a licensing document)?
- A. Yes. While this is not a requirement, there are many efficiencies that are gained in placing safeguards information in a separate attachment or enclosure to other licensing or business related information. It is up to the individual licensee whether or not to combine SGI-M in an otherwise uncontrolled document. However, many licensees send separate transmittal letters with attachments enclosing SGI-M. This allows licensees to issue non-SGI-M documents publicly or to those within the corporation who do not have access to SGI-M.
32. Is there an annual review to “reclassify” SGI-M?
- A. No. There is no annual review of SGI-M information.
33. Does SGI-M material need to be inventoried periodically? Do you need to keep track of the number of copies made?
- A. No. There is no inventory requirement for material marked as SGI-M. Individuals authorized access to SGI-M can make as many copies as may be needed. However, the number of copies should be kept to the minimum required. All copies must be protected from unauthorized disclosure.
34. Will the NRC inspect how licensees handle and protect SGI-M?
- A. Yes.

Enclosure 4

Frequently Asked Questions
About
Safeguards Information -Modified Handling

Marking of SGI-M documents/material

35. Does the last blank page on a SGI-M document have to be “stamped” (marked SGI-M)?
- A. No. All pages of a SGI-M document must be marked. The back of the last page, if blank, is not required to be marked as containing SGI-M. However, this is a good practice. If a document containing SGI-M is turned face-down, it may be desirable to mark both front and back of a document.
36. How do you change the markings on a document that has been decontrolled?
- A. If a document has been appropriately decontrolled, the individual responsible for decontrol of the document should mark through the SGI-M markings to indicate it no longer contains SGI-M or it has been removed from the attached SGI-M document. Lining out SGI-M serves two purposes: 1) it shows that someone deliberately changed the marking of the document in an obvious way; and 2) it indicates that the document contained additional information of a sensitive nature transmitted to authorized parties only.
37. Does security information already sent to the police and/or fire departments over a year ago need to be retrieved and marked as SGI-M?
- A. No. SGI-M information provided to police and fire departments subsequent to the Order must be appropriately marked. Information containing SGI-M sent over a year ago to the police would not have to be marked by the police organization as SGI-M. If the licensee determines that information in the possession of the police contains SGI-M, it would be incumbent on the licensee to identify such information to the police so that it can be protected appropriately.
- Local fire departments rarely require access to SGI-M since their role is primarily geared towards health and safety and not the security of the material licensee’s facility. If the licensee determines that a fire department must have access to SGI-M in order to complete their support mission, the licensee must ensure that appropriate security protection measures are in place.
38. Does information provided to liability carriers, in the last year, have to be retrieved and marked SGI-M?
- A. Not necessarily, it is up to the discretion of each licensee as to whether to identify and reclaim such information. In some cases, it is detrimental to publicly identify sensitive information and may be counterproductive. However, if the licensee identifies certain information as containing SGI-M to the insurance or reliability carrier, then proper protection standards must be in place.

Enclosure 4

Frequently Asked Questions
About
Safeguards Information -Modified Handling

39. Do the SGI-M instructions require a cover sheet?
- A. A cover sheet is not required, but is considered good practice. The requirement is that the licensee properly identify SGI-M and protect it as such.

Authorized access to SGI-M (need to know & trustworthiness)

40. Can a never opened SGI-M package be left with an “uncleared” (not authorized) person? (e.g., leaving the SGI-M package with the secretary of the person to which it is being delivered)
- A. Yes, if the double wrapped package does not indicate the presence of SGI-M on the outer envelope and the individual leaving the package does not indicate the presence of SGI-M within the package. The inside envelope must be marked as containing SGI-M and be packaged so as to indicate potential tampering.
41. Do personnel in mail rooms that open mail need to be authorized access to SGI-M?
- A. Yes, individuals who open mail would require access to SGI-M for the purpose of handling documents pursuant to their job as mail room attendants. The uncontrolled access to SGI-M information requires a need-to-know access and verification of trustworthiness which includes fingerprinting and a federal criminal history check.
42. If we sent SGI-M security plan information (ie., how to turn off alarms, where the guards are, weapons etc.) to the police department, do licensees need to verify that there is someone “cleared” (authorized) to receive it?
- A. No. However, when sending such information to the police department, licensees should have a single point of contact such as the local Chief of Police. Such contacts should always be verified prior to sending of the document. When dealing with larger organizations, the licensee must ensure that the intended recipient is still in the position and is aware that SGI-M information is being sent. Information should not be sent to a position such as “project manager” or “police department supervisor”.
43. Can a contractor develop a clearance (access control?) program?
- A. Yes, however, the responsibility for ensuring the program meets the requirements belongs to the licensee.

Enclosure 4

Frequently Asked Questions
About
Safeguards Information -Modified Handling

44. Do customers have a need to know when they do their QA audits?
- A. If the licensee determines that the auditor or other individual requires access to SGI-M in order to perform their job function, then the requirements for determining trustworthiness must also be met.
45. How is trustworthiness determined? Define trustworthiness!
- A. In so far as trustworthiness relates to SGI-M and radioactive material, licensees must have reasonable assurance that individuals granted access do not constitute an unreasonable risk for theft, diversion, or sabotage of the radioactive material. Licensees in their employing practices should have in place a process by which they determine that an individual is worthy of employment and placed in a position of confidence. Trustworthiness for access to SGI-M will be governed by the Compensatory Measures imposed by the Order.
46. Will there be provisions for grand-fathering the trustworthiness of current employees?
- A. All employees who wish to have access to SGI-M must have an established “need-to-know” and must have a trustworthiness and reliability check, which includes fingerprinting and federal criminal history check. Licensees must have a basis for establishing trustworthiness for all employees that they subsequently authorize access to SGI-M. The Compensatory Measures and Implementing Guidance related to establishing trustworthiness distinguish between new employees and current employees.

Storage Containers

47. Does the SGI-M storage container have to be in a secure area?
- A. The SGI-M storage container must be located in an area that can physically separate (e.g., locks, personnel access controls, escorts,) public areas from areas where employees have work related functions.
48. Does the SGI-M storage container need to be marked that it contains SGI-M material?
- A. No. The container should not be marked or in any other way indicate the presence of the material contained within.
49. Does the SGI-M storage box/container have to be immovable?
- A. No. The SGI-M container or storage box does not have to be an immovable container or secured to the wall/floor in any other way. Security measures or

Enclosure 4

Frequently Asked Questions
About
Safeguards Information -Modified Handling

other access controls must be in place to ensure a high level of confidence that the material will be protected.

50. Does the key to the SGI-M storage container have to be kept in a place where only a "cleared" (authorized) individual can get to?
- A. If a key is used to secure a storage container, it must be in a place or position where it is controlled by an individual that has authorized access to SGI-M. For instance, a key could be hanging from a hook in an area continuously occupied by authorized individuals. An unauthorized individual could be in the same area as long as appropriate controls to restrict access were in place.

Use of Computers

51. What does "self contained" computer mean? Can it have e-mail capability?
- A. The term "self-contained" is being removed from current language regarding computer protection controls. New language is being used to address appropriate computer security.
52. Does a corporate firewall afford enough protection to allow connected computers to be used for SGI-M?
- A. A firewall itself does not provide security. A firewall implements specific organizational security policies that specify the services and protocols that will be filtered by the firewall. Dependent upon the protocols used, a firewall can substantially decrease the potential of computer misuse. Additional controls, such as password protection, removal of files from the computer hard drive or server, and file encryption when transmitting a document, provide protection of SGI-M between computers.
53. Is logging off the Internet considered to be the same as "pulling the plug" to make the computer "self contained" before processing SGI-M?
- A. No. Logging off the Internet does not reduce the vulnerability of the computer system.

Enclosure 4

Frequently Asked Questions
About
Safeguards Information -Modified Handling

54. What about Intranet? Or local area networks (LANs)?
- A. Good computer security practices, such as that used to protect company proprietary information, can substantially decrease the potential of computer misuse. Additional controls, such as password protection, removal of files from the computer hard drive or server, and file encryption when transmitting a document, provide protection of SGI-M between computers.
55. If the electronic SGI-M file on a removable diskette is password protected, why does access to the computer have to be password protected, and why does the storage container need to be locked?
- A. The use of a computer password or log-on ID is a standard computer security practice. The requirement to lock a security storage container and the requirement to use a computer password are designed to provide a level of security appropriate for such information. The requirements are designed to, minimize access and, provide an acceptable level of physical protection of the information.
56. Now that newer digital copiers scan & retain images of documents, how must copy machines, used for SGI-M material, be protected?
- A. There is not a single government-wide firewall security policy, so it would be difficult to verify that an organization's firewall policy is adequate. NRC may be able to specify some minimum firewall filtering features, but there may be great costs to some of the licensees to implement that. First, NRC would have to specify if it is acceptable to process the new SGI-M on a network. (This is not currently authorized for current SGI).
- If the copier is retaining SGI-M in memory, the copier needs to be removed from the network. It should also be placed in a location that is cleared and controlled for the authorized processing of SGI-M. Different copiers have different capabilities, including some which come with features that allow the memory to be erased. Each copier would have to be examined from a physical security perspective.
57. If I am working on a SGI-M document on the computer, can I use a password protected screen saver to walk away from the computer for a short time while leaving the electronic document active?
- A. No. SGI-M is not to be left unattended. In this case, the SGI-M document is not under the control of an authorized user, not properly packaged for mailing, not stored in an appropriate storage container, and not encrypted for transmission.

Enclosure 4

Frequently Asked Questions
About
Safeguards Information -Modified Handling

Depending on the operating system version, the password protected screen saver may be reset.

Transmitting/transporting SGI-M documents/material (double wrapping)

58. Guidance is need to identify what emergency conditions would allow free transmittal of SGI-M?
- A. Emergency situations where SGI-M can be transmitted without the use of security controls include instances where the facility has declared a security emergency and requests the assistance of local police or other responding agencies. The need-to-know requirement is still in effect. In each case, the licensee must balance the disclosure of information against the threat being faced and the necessity of response.
59. Can SGI-M be sent through intra-company mail between sites?
- A. Yes. SGI-M can be sent through intra-company mail (opened by addressee only). Use of a single opaque envelope is sufficient as long as the contents are not described on the envelope. If mail room situations dictate opening of envelopes, the licensee needs to address whether access to SGI-M is required for the particular job function. When mailing SGI-M outside of an office to a field site or location, two opaque envelopes must be used.
60. If SGI-M is carried from facility to facility, does the SGI-M need to be double wrapped?
- A. If an authorized individual is carrying SGI-M from facility to facility, the requirement to double-wrap the information does not apply. However, the individual must be able to control access to the information during transport.
61. If the SGI-M material is in a briefcase, can that be considered part of a double wrap?
- A. Yes. The briefcase can act as the outer wrapper. However, if the briefcase is left unattended, it must be capable of ensuring against tampering (i.e., combination lock). Otherwise, the briefcase must remain under the control of an authorized individual.
62. Can a FedEx envelop serve as a second wrapper?

Enclosure 4

Frequently Asked Questions
About
Safeguards Information -Modified Handling

- A. Yes. The requirements are that the envelope be opaque, not disclose the sensitivity of the contents, and protect against tampering of the interior envelope.
63. If I am transporting a SGI-M document, and security at the airport want to open it as part of the security check, what do you do? Do I need to document that it happened?
- A. Explain to the security checkpoint officials that the material contains Safeguards Information and is protected by NRC regulations. If the package must be opened, it must be done in the presence of the authorized individual. Any unusual circumstances such as copying of the information, removal from the authorized individual, or reading of the information must be immediately reported to the security supervisor and subsequently to the NRC and the individual's security point of contact at the company. If the document cannot be repackaged appropriately, an written explanation is required.

Electronic Transmission (e-mail, Internet, & LANs)

64. Can SGI-M be sent from facility to facility and to NRC via e-mail?
- A. Only if protected with encryption. Official correspondence to NRC typically is handled via hard copy and through the NRC's document control center.
65. What are examples of valid encryption systems that can be used to transmit SGI-M electronically?
- A. National Institute of Standards and Technology (NIST) approved products are listed on their computer security website, <http://csrc.nist.gov/cryptval/140-1/1401val.htm>. (Several licensees and NRC staff use PGP however, NRC has not officially adopted it for routine use - contact NSIR Information Security Section before transmitting SGI-M to NRC).

Decontrolling & Destroying SGI-M

66. If the security plan is upgraded from 5 guards to 7 guards, can the old plan be decontrolled?
- A. In theory, the old plan that no longer contains the current security posture for the facility could be decontrolled. However, in practice it is usually difficult to decontrol such documents since some aspects of an old plan still represent sensitive security information or substantially represent a level of security that would be beneficial to an adversary. Typically, copies of an old plan are

Enclosure 4

Frequently Asked Questions
About
Safeguards Information -Modified Handling

destroyed when no longer necessary or superceded by new plans or commitments.

67. Are commercial shredder companies okay to use for destroying SGI-M documents?
- A. Yes, provided the SGI-M information to be shredded is under the control of an authorized individual at the time of destruction. The information cannot be shipped to a commercial shredder company unless there is a need to know and trustworthiness has been determined.
68. If you want to decontrol a SGI-M document, you need the permission of the individual that originally made the determination. What do you do if that individual is no longer around?
- A. A document can be decontrolled by any individual authorized access to SGI-M with proper need-to-know. Depending upon circumstances, it is not necessary to locate the originator of a document in order to decontrol. Some decontrol instructions are contained on the transmittal letter of a document and are authorized by the originator of the document. Generally, the originator of a document is notified if a document is considered to no longer have SGI-M information since there is probably a need-to-know on the part of that individual. In cases where an individual no longer works in a need-to-know position or has left the company, it is not necessary to locate and inform the individual.

Is It Or Is It Not SGI-M

69. What is safeguards and what is not? Better guidance is needed. When will more guidance be available?
- A. SGI-M is information the disclosure of which 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 materials or facilities subject to NRC jurisdiction. NRC has prepared the DG-SGI-1, "Designation Guide for Safeguards Information" guidance document in order to assist with the determination of what is or is not safeguards.
70. Are you going to give examples of what is SGI-M?
- A. "Safeguards Information-Modified Handling" identifies a licensee's or applicant's security measures for the physical protection of source material or byproduct material. These physical security measures are required in order to protect quantities of nuclear material significant to the health and safety of the public or

Enclosure 4

Frequently Asked Questions
About
Safeguards Information -Modified Handling

common defense and security. The overall measure of consideration of SGI-M is the usefulness of the information (security or otherwise) to a adversary in planning or attempting a malevolent act. The specificity of the information increase the likelihood that it will be useful to an adversary. Examples of SGI-M have been prepared, and can be found in NRC has prepared the DG-SGI-1, "Designation Guide for Safeguards Information" which may be used as guidance by licensees.

71. Is it SGI-M to say "I am resourcing on MM, DD, YYYY"? Days?, AM or PM? Between the hours of 8 AM - 10 AM?
- A. Information for public consumption such as specific dates and times for sensitive transfers should not be made unless a clear case is made for need-to-know. In all cases where the public has a right to know specific health and safety information, the information is not considered SGI-M. Specific dates and times dealing with security vulnerabilities or weaknesses are typically considered SGI-M. Information of a general nature such as a range of times (8am-10am for a 30 minute transfer) with adequate security in place are not considered SGI-M.
72. Is the date when a licensee expects a shipment of radioactive sources and will conduct source change out SGI-M?
- A. No. As long as adequate security is in place, the date of a planned shipment is not SGI-M but is considered sensitive information and should only be shared with individuals who have a "need-to-know".
73. If we need to request money for security equipment do we need to control the requests as SGI-M?
- A. Dependent upon the specificity of the information contained in the request. For example, a request for equipment is not considered SGI-M; however, the location of such equipment may be SGI-M if it is not readily seen by unauthorized individuals (i.e., hidden alarms and their locations). Generally, the request for money would not be SGI-M.
74. Is the fact that there are guards or the exact number of guards that make it SGI-M?
- A. The fact that guards are employed would not be SGI-M. The number of guards on duty at any one time would not be SGI-M. The numbers of responders and their locations in a security emergency would be SGI-M.
75. Telephone calls regarding shipments, do they become SGI-M, and if so how to communicate?

Enclosure 4

Frequently Asked Questions
About
Safeguards Information -Modified Handling

- A. Information regarding the shipments of radioactive materials and their impact on public health and safety are not SGI-M. Specific information regarding the security of a shipment is SGI-M. Route information is not SGI-M, however, route information should be considered sensitive information and should only be shared with individuals who have a “need-to-know”.
76. Examples are needed about what can and cannot be discussed over a phone, radio or radio dispatch system. Can quantities, dates and times of shipments be discussed over the phone? What about security check-in calls during transport?
- A. General statements concerning security are not SGI-M. Health and safety information is not SGI-M. Security check-in calls during transport should use non-specific identifiers (e.g., code green, location five).
77. Operating procedures with response to alarms with calls to LLEA are widely available on computers, will they become SGI-M?
- A. Operating procedures and responses to such are not regarded as SGI-M. However, if the licensee takes credit for the “operating procedure” as a “security procedure” the document will be considered SGI-M. The intent of the marking is to prevent an adversary from identifying security measures, or additional security procedures beyond the operating procedures, at a facility.

Fees

78. Will the Agreement State licensees be assessed fees? At what rate?
- A. The NRC is evaluating this issue.

Orders & Compensatory Measures

79. What is the process of decommissioning or when the licensee falls below the 370 TBq (10kCi) limit on downgrading SGI-M?
- A. In general, if the licensee no longer possess that quantity which requires the Compensatory Measures identified in the orders, the licensee would no longer need to have SGI-M information. The licensee should inform the NRC of the fact it no longer possess those quantities and the intention to relax security measures. The NRC will work with the licensee to help determine if any material is still SGI-M at that time.

Enclosure 4

Frequently Asked Questions
About
Safeguards Information -Modified Handling

However, if the licensee falls below the 370 TBq (10kCi) limit, the licensee may be subject to the Increased Control requirements that would be issued by either the NRC or Agreement State. The Increased Controls do require that sensitive information be protected.

80. What should licensees do when they are less than 370 TBq (10 kCi) but will go above - what will be the time allowed to come into compliance with order?
- A. The NRC expects full compliance 180 days after the initial orders are issued. If a licensee actually possesses less than the 370 TBq (10 kCi), at the time the orders are issued, but does intend to exceed that amount in the future, the licensees will have to be in compliance at the time they possess 370 TBq (10 kCi) or more or at the end of the 180 days from the date when the initial orders are issued, whichever date is longer. Example would be if the orders were issued on May 1, 2003, and a licensee were to meet or exceed 10 kCi before October 28, 2003, they would have to be in compliance by October 28. If they were to exceed 370 TBq (10 kCi) on October 30, they would have to be in compliance by October 30. The NRC would have to be informed either way of the date they would be in compliance with any exceptions or delays explained in a written response to the order.
81. Is the list of irradiators necessary to send out with the order - it is sensitive information that is not needed in the attachments?
- A. It is necessary to identify those licensees that were issued the Order. The Commission has determined that the List of Irradiator Licensees (Attachment 1 to Enclosure 1) should be continue to be designated as sensitive unclassified information for Official Use Only and will be withheld from the public. This information was placed in an attachment so that it could be easily separated from a generic Order that could be made publicly available.
82. Will the Orders be issued based on possession limits or actual material possessed?
- A. The orders will be issued to licensees based on possession limits but if the licensee actually possess less than the 370 TBq (10kCi), an acceptable response to the order is that the licensee does not actually possess those quantities and therefore does not need to implement the Compensatory Measures. As long as the licensee has possession limits at 370 TBq (10kCi) or greater, they have the potential to possess those quantities and therefore need to be aware of the order's requirements and be prepared to meet them if their status changes such that they do possess those quantities (see response to Question 83).

Enclosure 4

Frequently Asked Questions
About
Safeguards Information -Modified Handling

83. Does the NRC want a schedule for completion for each Compensatory Measure?
- A. The NRC needs to know when the licensee is in full compliance so that the inspection effort can be planned. If the licensee is taking exceptions to the measures in the order or the time for completion, those exceptions and or time extensions need to be reviewed and approved by the NRC.