Public Comments and Staff Responses
Draft Regulatory Guide (DG) 5034, "Protection of Safeguards Information"

1. **Public Comment**: In providing acceptable means in carrying out the requirements of the Rule, the Regulatory Guide should be careful to avoid adding or inferring requirements that do not appear in the rule.

Public Suggested Revision: None.

NRC Response: The staff did not find evidence of inferred regulatory requirements within the Regulatory Guide. Recommended processes are prefaced with "should" or "may" and where appropriate, regulatory requirements are prefaced with the word "must" or "shall." The Regulatory Guide describes methods that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable for implementing general performance requirements as stated in 10 Code of Federal Regulations (CFR) 73.21, 73.22 and 73.23.

2. **Public Comment**: The Regulatory Guide should be consistent in the use of language (e.g., must, shall, should, may, etc.) with other Part 73 Regulatory Guides.

Public Suggested Revision: None.

NRC Response: With no specific reference to perceived inconsistencies within this Regulatory Guide and other Part 73 Regulatory Guides, as it relates to the use of must, shall, should, may etc., the staff is unable to address any particular concerns that the commenter may have. The staff has reviewed the Regulatory Guide thoroughly, and compared it with other Part 73 Regulatory Guides, and find no instances of inconsistency with the use of must, shall, should, may, etc. as it relates to methods that can be used to comply with the guidance in 10 CFR 73.21, 73.22 and 73.23.

3. **Public Comment**: Consistent with the other Part 73 Regulatory Guide format, the guidance should be provided in the same order as the requirements in the Rule.

Public Suggested Revision: None.

NRC Response: To aid in the readability of the document, the Regulatory Guide will be reformatted to ensure that the order of guidance is consistent with the order of the requirements as stated in the Regulation.

4. **Public Comment**: As worded/organized it's difficult to understand exactly when the Regulatory Guide is referring to either Safeguards Information (SGI) or Safeguards Information-Modified Handling (SGI-M) or both.

Public Suggested Revision: None.

NRC Response: Except where specifically stated, the guidance in the Regulatory Guide should be interpreted as being applicable to both SGI and SGI-M requirements. The "Introduction" of the Regulatory Guide has been modified to make that point explicitly clear.

5. Public Comment: Page 2, Paragraph 3; not all categories of licensees are listed that are subject to the provisions of 10 CFR 73 for the protection of SGI.

Public Suggested Revision: Include fuel fabrication facilities, Uranium enrichment facilities, UF6 production and conversion facilities, etc.

NRC Response: The categories of licensees referenced in Section B of the Regulatory Guide were not intended to be all inclusive. Section B, of the Regulatory Guide, states the categories of licensees referenced are "examples of the categories of licensees currently subject to the provisions of 10 CFR Part 73." The Regulatory Guide is intended to compliment the guidance of 10 CFR Part 73. The staff made a concerted effort to limit the frequency with which the text of the CFR was reiterated, so no reference was made to the fact that the identified categories of licensee were not all inclusive. Stakeholders and other interested parties should, as a matter of practice, familiarize themselves with the CFR before referring to the Regulatory Guide for implementation guidance. Where appropriate, the Regulatory Guide references and quotes particular sections of the CFR when necessary to place the intended regulatory guidance in the appropriate context. The suggested revision was not adopted.

6. Public Comment: Page 3, Paragraph 2; the text states that since the NRC didn't incorporate all Order requirements into the rule, licensees must comply with both and determine which regulatory document contains more stringent requirements and comply. This approach is not effective regulation and could lead to confusion and non-compliance.

Public's Suggested Revision: (1) Place guidance in the Regulatory Guide for all Order requirements that are not in the Rule. (2) Rescind Orders that are duplicative of the Rule.

NRC Response: The recipients of the applicable Orders are in compliance with both the spirit and intent of those Orders. Placing guidance within the Regulatory Guide, on those applicable Orders, would not assist those that are currently complying with those Orders. As to the second portion of the suggestion, the staff has initiated the process of reviewing relevant SGI Orders and upon completion of that review, will make its recommendation to management. In the interim, the Orders will remain in effect and Order recipients are obliged to comply with both the rule and the applicable Orders, in those few instances where the Orders impose more stringent requirements than the rule.

7. Public Comment: Page 4, Section 2; the term "System" is confusing. "Program" is more appropriate.

Public Suggested Revision: Replace "system" with "program" throughout the Regulatory Guide as appropriate.

NRC Response: The terminology used within the Regulatory Guide must be consistent with the terminology used within the Regulation itself so as not to cause confusion. The Regulatory Guide appropriately uses the term "system" when referring to the tool that licensees, certificate holders, applicants, or others persons that are subject to the rule must establish, implement and maintain with respect to protection of SGI performance requirements. The suggested revision to the Regulatory Guide would cause its terminology to be inconsistent with the terminology used within the regulation itself, and therefore was not adopted.

8. Public Comment: Page 4, Section 2(a); section C.2 (a): Don't understand what this means "document activities and commitments regarding the local procedures."

Public Suggested Revision: Delete (a). It is redundant to (g).

NRC Response: The referenced section should be interpreted to mean that the Information Protection System, that is required by 10 CFR 73.21 (a), should be formally documented so as to be available for use and review by interested parties. Section C.2 (g), of the Regulatory Guide, guidance differs from that of C.2 (a) in that it recommends the establishment of a training program that is geared toward the identification and protection of SGI. While the suggested revision was not adopted, the section in question will be modified so as to provide better clarity.

9. Public Comment: Page 4, Section 2(b); section C.2 (b): Identification by role or by name?

Public Suggested Revision: Delete (b). It is covered in procedures developed per (g).

NRC Response: Section C.2 (b) is not covered by the recommended guidance in C.2 (g). Section C.2 (b) recommends that the Stakeholder identify, in a manner that is best suited for the Stakeholder, key personnel with responsibilities for the implementation of the Information Protection System. Section C.2 (g) recommends the establishment of a training program that is geared toward the identification and protection of SGI. The suggested revision was not adopted.

10. Public Comment: Page 4, Section 2(c); the rule does not require an annual independent audit of the Safeguards Information program and the periodicity is inconsistent with established programs.

Public Suggested Revision: Delete the annual requirement or make it consistent with other security program audits.

NRC Response: The commenter is correct, the regulation does not specifically call for an annual independent audit and likewise, the staff has not mandated such a requirement. The Regulatory Guide is a guidance document and provided to Stakeholders to set forth one acceptable way of complying with the NRC's regulatory requirements. The regulation does require that an Information Protection System be established, implemented and maintained. The staff believes that a periodic audit of the effectiveness of the Information Protection System is a valuable tool that licensees and other stakeholders should use in the maintenance

of their Information Protection System. A 12 month cycle is consistent with other inspection and audit requirements referenced in Part 73.

11. Public Comment: Page 4, Section 2(e); this is both a Rule and PSP requirement. C.2 states "The system should do the following:" however, (e) is a "shall" versus "should."

Public Suggested Revision: Modify the Regulatory Guide language or delete in entirety.

NRC Response: The commenter has incorrectly associated physical security program requirements, various mandated records retention guidance prescribed by 10 CFR 73.55, with information security requirements as prescribed by 10 CFR 73.22 and 73.23. In an effort to remove any misconceptions as to the appropriate application that the guidance of section C.2 addresses, (C)(2)(e) will be modified to indicate that the referenced system of records review, are related to SGI records.

12. Public Comment: Page 4, Section 2(f); this is both a Rule and PSP requirement. C.2 states "The system should do the following:" however, (f) is a "shall" versus "should."

Public Suggested Revision: Modify the Regulatory Guide language or delete in entirety.

NRC Response: The commenter has incorrectly associated physical security program requirements, as prescribed by 10 CFR 73.55, with information security requirements prescribed by 10 CFR 73.22 and 73.23. Section (C)(2)(f) will be modified to add specificity in that the procedures to address security violations will specifically state "establish procedures to describe information security violation and appropriate corrective actions."

13. Public Comment: Page 4, Section 3; there is no requirement for the training program in the Rule. There is a requirement that personnel receiving access to SGI be knowledgeable of requirements for protection of the information. This can be accomplished through individual briefings, general employee training, or other methodologies at the discretion of the licensee without the implementation of a formal training program.

Public Suggested Revision: Eliminate inference of a formal training program and provide instead, a general statement such as, "Provide training of individuals authorized access to SGI on the procedures and guidance for identification and protection of SGI."

NRC Response: The Commenter is correct; there is no stated regulatory requirement for a SGI training program within 10 CFR 73.21, 73.22 and 73.23. Likewise, there is no stated requirement for a SGI training program within the regulatory guide. The recommended areas for inclusion, within the information protection system, are not all inclusive, nor are they mandatory requirements that must be evident in every Information Protection System. The regulatory guide will be revised as the commenter suggested. The revised text will read as follows: "Provide training to individuals authorized access to SGI on the procedures and guidance for task geared toward the identification and protection of SGI."

14. Public Comment: Page 4, Section 3; the wording in the second paragraph is confusing. Intent appears to be to treat information in a conservative manner until classification is reliably determined.

Public Suggested Revision: Clarify wording and provide examples as necessary. Delete second paragraph and insert: "If the information is questionably labeled as SGI, treat it as SGI and confirm as soon as possible with the originating organization that made the determination of the SGI."

NRC Response: The Commenter is correct in that the referenced paragraph does direct the reader to treat inappropriately marked or non-marked information, that may warrant SGI designation, in a conservative manner until the document can be assessed and its true designation determined by an authorized SGI Designator. The paragraph will be modified to clarify its intent and remove the possibility for misunderstanding or misinterpretation. The modified text will read as follows: "If information is thought to be SGI, but not marked as such and it is not clear whether the requirements of 10 CFR 73.22 or 10 CFR 73.23 apply, the possessor should apply the protection provisions of 10 CFR 73.22(b) through (i) (excluding 73.22(d) and 73.23(d)), and obtain clarification from the originator as soon as practicable, so that the information can be protected at the appropriate level. If it is determined that the information is SGI, the appropriate SGI markings must be applied to the document as prescribed by 10 CFR 73.22(d). Additionally, the Licensee should initiate an inquiry if the information in question is believed to have been viewed or otherwise obtained by personnel not authorized access to SGI."

15. Public Comment: Page 4, Section 4; (a) through (e) set performance expectations for law enforcement to meet the requirements of 73.21. These expectations are not located in the rule and imply that there would be some audit to assure they are in place before SGI is shared with LLEA. This is impractical and has the potential for negative relations that NRC referred to with their stakeholders.

Public Suggested Revision: Revise Section 4 as follows: "Law enforcement agencies are presumed by NRC in accordance with 73.21(a)(2) to meet performance requirements of 73.21(a)(1). However, licensees should inform Federal, State, and local law enforcement agencies of the SGI requirements before transferring SGI, so that these agencies are fully aware of the protection requirements for SGI and the potential for civil and criminal sanctions against any person that discloses SGI in an unauthorized manner."

NRC Response: The information in Section C (4)(a) through C (4)(e) should not be viewed as the NRC's creation of performance expectations for Law Enforcement agencies as a condition for access to SGI, but rather the recognition and acknowledgement of the day-to-day performance requirements evident at Law Enforcement agencies. Those stated performance requirements were taken into consideration when both 10 CFR 73.21(a)(2) and 10 CFR 73.59 were written and therefore should not be interpreted as implying a need to audit for an assurance of their existence. The potential for "negative relations" that may occur as a result of the precautionary measures that are taken in concert with third party sharing is outweighed by the benefit of improved situational awareness, with respect to rule compliance and acknowledgment of the penalties associated with unauthorized or unlawful

disclosure. The Regulatory Guide will be modified to plainly state that it is assumed that law enforcement agencies meet the performance requirement that are outlined within that section of the Regulatory Guide. That modification should remove the perception that the NRC has set a performance expectation for Law Enforcement agencies within the Regulatory Guide.

16. Public Comment: Page 5, Section 4; this section states that "written or oral confirmation" of understanding of SGI handling is required before the sharing SGI by the possessor. Transfer by transfer re-validation is excessive and unnecessary if the individual is included in an approved SGI handling program.

Public Suggested Revision: None.

NRC Response: Persons possessing SGI have an obligation to protect it from unauthorized disclosure. Within the context of the guidance stated within section 4, page 4 of the Regulatory Guide, persons possessing SGI and intending to share it with a third party recipient, i.e., Federal, State, or local law enforcement agency, have a responsibility to ensure that the intended recipient is aware that the information is SGI and that it must be protected from unauthorized disclosure in accordance with 10 CFR 73.21(a). The Regulatory Guide does not mandate obtaining written or oral confirmation that the recipient understands the protection and handling requirements associated with SGI, but rather presents written or oral confirmation as one possible means of assuring that a third party recipient of SGI is aware that the information warrants protection.

17. Public Comment: Page 5, Section 5; the Designation Guide is referred to as an additional guidance document for the determination of SGI. Although the guide was provided to licensees for information purposes, it is not official guidance for licensees and should not be referenced as such in the Regulatory Guide. The Designation Guide is not a publicly commented document and is an internal NRC document.

Public Suggested Revision: Eliminate reference to Designation Guide from the Regulatory Guide and insert necessary information from the Designation Guide into Regulatory Guide language.

NRC Response: The SGI Designation Guide is identified, within the Regulatory Guide, as a valuable tool that provides further examples of what constitutes SGI and SGI-M. The staff was careful to include guidance within the Regulatory Guide to state that 10 CFR 73.21 and Commission Orders set forth the criteria for whether information is SGI or SGI-M. It was never our intent to infer or imply that the SGI Designation Guide was "additional guidance." As suggested, reference to the SGI Designation Guide, as an official guidance document, will be removed from the listed references within the Reference section of the Regulatory Guide.

18. Public Comment: Page 5, Section 5; Regulatory Guide language infers new requirements not in language of the Rule and related to compilation of multiple non-SGI material into SGI classification.

Public Suggested Revision: Delete last sentence of the fourth paragraph of this section.

NRC Response: Concern for compilation of information should always be at the forefront of any information protection system. The Regulatory Guide does not infer a new requirement, but rather draws distinct attention to the possibility for a compilation issue to occur. 10 CFR 73.21(a)(1)(iii) directs the reader to protect information in accordance with the requirements of 10 CFR 73.22 if the SGI (i.e., information that meets the criteria for SGI designation) is not described in paragraphs 10 CFR 73.21(a)(1)(i) and 10 CFR 73.21(a)(1)(ii).

19. Public Comment: Page 5, Section 5; Regulatory Guide language needs to be restructured for clarity.

Public Suggested Revision: Replace the fifth paragraph language with the following: "Information of a general nature and not specific to a particular facility is usually not SGI unless, for example, it concerns studies of the impact of postulated security events on nuclear facilities or radioactive materials or is information that discloses generic consequences to a class of facilities or material users. When classifying material in accordance with 10 CFR 73.22(a)(1)(xii) and 73.23(a)(1(x), licensees should consider the specificity of the information and its usefulness in defeating security measures at a particular facility. The overall measure for the designation of SGI is the usefulness of the information to an adversary in planning or attempting an act of radiological sabotage."

NRC Response: The suggested revision is very close to reiterating the draft text that is currently in the Regulatory Guide with minor exceptions. It is those minor exceptions that if accepted by the staff, would deliver a message that is contrary to the intended guidance currently within the Regulatory Guide. The suggested revision mistakenly uses the term "classifying" with respect to SGI designation. Classifying a document is an action that's reserved exclusively for National Security Information. Additionally, the suggested revision would restrict the focus of what should be considered for SGI designation to only that which is intentionally and possibly narrowly considered under 10 CFR 73.22(a)(1)(xii) and 73.23(a)(1)(x). The intention of the referenced guidance, as currently written in the draft Regulatory Guide, is for the reader to expand or not limit its level of awareness for the possibility that engineering or construction drawings containing a degree of specificity of information that could be advantageous to an adversary, must be designated as SGI in accordance with 10 CFR 73.22(a)(1)(xii) and 73.23(a)(1)(x). The overall measure for designation is not limited, as stated in the suggested revision, to the usefulness of the information to an adversary in planning or attempting an act of radiological sabotage. The overall measure for designation of SGI is its significance to the public's health and safety or common defense and security and is not limited, exclusively, to "acts of radiological sabotage." If the unauthorized disclosure of the information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of sabotage or theft or diversion of source, byproduct, or special nuclear material (a malevolent act), the information must be designated as SGI.

20. Public Comment: Page 6, Section 6; the requirement for access to SGI regarding verification of education exceeds requirements for UAA. For UAA, education is only used in lieu of work history. The education element of the background investigation for SGI

should be consistent with UAA. A process also needs to be developed to specify adjudication criteria for SGI access BI.

Public Suggested Revision: Remove the following sentence: "The verification of a person's stated level of education is considered a key attribute in determining a person's trustworthiness and reliability."

Insert the following: "The trustworthiness and reliability determination is based upon verification of identity, employment history, education, criminal history records check, and appropriate reference checks as defined by "background check" in 10 CFR 73.2.

For access to SGI, the background investigation elements should consist of the following: "Verification of identity – Compare a valid (not expired) official photo identification (e.g., driver's license; passport; government identification; State, Province, or country issued certificate of birth; etc.") with physical characteristics of the individual."

Employment history – Verify employment/unemployment history for the past 3-year period, or since age 18, whichever is shorter.

Education in lieu of employment – Conduct a suitable inquiry of an educational institution for the appropriate timeframe.

Criminal history record check – Conduct FBI fingerprint screening.

Reference checks – Conduct reference checks with co-workers, neighbors, or friends. Either personal references or developed references may be used when collecting information to make a trustworthiness and reliability determination. Background investigations performed for UAA and/or UA exceed the requirements for background investigation for access to SGI."

NRC Response: 10 CFR 73.22(b) does not call for a verification of education nor does the Regulatory Guide. The education element of the background check that must be accomplished as a pre-condition for access to SGI, is consistent with the requirement that must be accomplished for unescorted access authorization (UAA). The depth of the inquiry, on the education element of the background check, is subject to the requirements established by the Licensee or the organization that is completing the background check. Verification of stated information, education or otherwise, is a key attribute in determining a person's trustworthiness and reliability. As the Commission explained in the 2006 Revised Proposed Rule (71 FR 6404, 64014), an individual that has successfully completed a background investigation and been granted UAA, should be considered suitable for access to SGI, if the individual has a need-to-know. The NRC does not intend for the two access requirements to conflict or cause an unnecessary burden on licensees.

10 CFR 73.22 and 73.23 do not contain background check adjudication standards, and it would be improper for the staff to infer that such a regulatory standard exist. At a minimum, the criteria used to adjudicate the results of the FBI criminal history records check and other elements of the background check must not conflict with the prohibitive practices stated in 10

CFR 73.57(c). As stated in the Regulatory Guide, the NRC expects Licensees to use their best judgment and experience in determining which individuals are trustworthy and reliable and therefore suitable for access to SGI. Whichever adjudication standard is adopted by the licensee or organization, it should be capable of supporting a character determination.

21. Public Comment: Page 6, Section 6; there is no reinvestigation requirement in the regulation. The draft Regulatory Guide is expanding the stated meaning of the rule by stating, "This implies that there is a continuing obligation for licensees and others responsible for allowing access to SGI to make reasonable efforts and use their best judgment to ensure that person with access to SGI remain trustworthy and reliable."

Public Suggested Revision: Delete the following language: "This implies that there is a continuing obligation for licensees and others responsible for allowing access to SGI to make reasonable efforts and use their best judgment to ensure that persons with access to SGI remain trustworthy and reliable."

NRC Response: As explained by the Commission in the 2006 Revised Proposed Rule (71 FR 6404, 64014), there is no requirement in the rule, or the Regulatory Guide, that states an individual, determined to be trustworthy and reliable, undergo a periodic background check to confirm or monitor trustworthiness and reliability. As suggested, the Regulatory Guide will be revised to read as follows: "If a licensee, applicant or certificate holder (responsible party) learns of information that would reasonably call into question the trustworthiness and reliability of an individual already authorized access to SGI or SGI–M, the responsible party should re-evaluate that individual's access authorization". 10 CFR 73.22(b)(2) and 73.23((b)(2) make individual trustworthiness and reliability a condition for access to SGI.

22. Public Comment: Page 6, Section 6; this is a good provision, however, it is currently very difficult to verify federal security clearances by the private sector. It should be noted that only the Facility Security Officer (FSO) has the authority to retain this record IAW the U.S. Nuclear Regulatory Commission Notification of Access Authorization Form. For visitors, since we do not have access to the Joint Clearance Access Verification System (JCAVS), we have to request the visitor's FSO provide that information to us prior to us granting them SGI access.

Public Suggested Revision: The industry request that NRC assistance in developing a process for the validation of clearances and add language to this effect in the Regulatory Guide.

NRC Response: The Regulatory Guide cannot be revised to prescribe a manner of practice for meeting the requirements of the regulation. When relying upon an active Federal security clearance to meet SGI access requirements, Licensees should contact the Facility Security Officer or the Organization's designated representative to obtain security clearance verification for the SGI access requesting individual.

Licensees may establish, implement and maintain their Information Protection System as they deem appropriate to support their day-to-day mission while complying with regulatory requirements. Industry may make a formal request for assistance with interpretation of the rule or guidance in meeting regulatory requirements. However, such a request made through

the Public Comment process for a Regulatory Guide is inconsistent with NRC standard operating procedures and can not be addressed in this forum.

23. Public Comment: Page 6, Section 6; the NRC should provide additional clarification that a determination of trustworthiness and reliability may be based on such determination from other previous entities performing such determinations. i.e., no requirement to redundantly review FBI fingerprint records or other background information.

Public Suggested Revision: Revise the draft guidance appropriately.

NRC Response: The guidance that the commenter suggested already exists within the Regulatory Guide, see Section C, Page 9, Paragraph 12. Access to SGI must always be based upon need to know, a trustworthiness and reliability determination as prescribed by 10 CFR 73.22(b) and 73.23(b). In keeping with 10 CFR 73.57(f)(3), licensees may obtain the personal information of a previous criminal history records check from another licensee provided the information transfer is in accordance with regulatory requirements. Whether the SGI access determination was based upon an active Federal security clearance, or a re-dissemination of personal information from another licensee, the Regulatory Guide makes it clear that each individual record of those requesting SGI access should contain documentation from the reviewing official that briefly explains or identifies the basis for granting or denying the request. Given that the guidance suggested by the commenter already exist within the Regulation, 10 CFR 73.22 and 10 CFR 73.23, the suggested revision will not be adopted.

24. Public Comment: Page 6, Section 6; the term "originator of the SGI" is inappropriate as used on page 7 in the sentence, "For persons participating in an NRC adjudicatory proceeding, the originator of the SGI must make the need to know…"

Public Suggested Revision: Replace "originator of the SGI" with "originating organization that made the determination of the SGI."

NRC Response: The text currently in the Regulatory Guide reiterates the regulatory guidance as it is written in 10 CFR 73.22(b)(4) and 73.23(b)(4). As such, the guidance can not be changed as suggested.

25. Public Comment: Page 8, Section 8; reviewing official should already have access to SGI or unescorted access to designated facility.

Public Suggested Revision: Replace "the designated reviewing official must be an individual seeking access to SGI" with "the designated reviewing official, if utilized, should be currently granted access to SGI or have UAA to a designated facility."

NRC Response: The recommended revision does not afford licensees the opportunity to designate someone currently without access to SGI to be the reviewing official. The staff believes that licensees should have the latitude to appoint the best person for the job of reviewing official. The guidance within the Regulatory Guide is consistent with previously issued NRC orders, in that Licensees and others are given the latitude to nominate any

individual currently authorized access to SGI, or is otherwise seeking access to SGI. The Commenter's recommendation would limit the pool of potential candidates and could possibly place an undue burden on the licensee and/or the person selected as reviewing official. For those reasons, the suggested revision will not be adopted.

26. Public Comment: Page 8, Section 9; the provision prevents the transfer of SGI access as stipulated in C.12 and the use of National Security Clearances in lieu of additional fingerprinting.

Public Suggested Revision: (1) Fingerprint each individual who requires access to SGI and submit the fingerprints to the NRC for transmission to the FBI in accordance with 10 CFR 73.22(b) and 73.23(b) or,

(2) Verify a current National Security Clearance exists or,

(3) Accept the fingerprinting, background check, and trustworthiness and reliability determination performed by another licensee through the SGI or UAA process.

NRC Response: The guidance in the Regulatory Guide does not prevent the transfer of SGI access; doing so would be contrary to 10 CFR 73.57(f)(2) and the referenced section of the Regulatory Guide e.g., Section C paragraph 12. The Regulatory Guide (See Section C, Page 6, Paragraph 6) does not require additional fingerprinting for those personnel possessing an active Federal security clearance. Accordingly, the suggested revision was not adopted.

27. Public Comment: Page 8, Section 9; the reference to NEI 03-01 is too general.

Public Suggested Revision: The reference should be "to applicable elements of the NEI 03-01 Personnel History Questionnaire" as discussed in Item 6.

NRC Response: The NRC has endorsed the Nuclear Energy Institute document, NEI 03-01, "Nuclear Power Plant Access Authorization Program" and considers the procedures that are outlined in it to be an acceptable means for licensees to use when making a trustworthiness and reliability determination. The suggested revision will be adopted and the Regulatory Guide revised to state: "The NRC has accepted certain industry standards, such as those found in the applicable elements of Nuclear Energy Institute document, NEI 03-01, "Personal History Questionnaire," and considers them an acceptable means for licensees to use when making a trustworthiness and reliability determination"

The message that inherently must be communicated here is that the NRC has found NEI 03-01, "Nuclear Power Plant Access Authorization Program" to be an adequate tool when making a trustworthiness and reliability determination.

28. Public Comment: Page 9, Section 11; the bases for granting SGI access are the criminal history and background records relied upon for the granting of access. An explanation should only be necessary where the request for access to SGI is denied to explain why the request was denied.

Public Suggested Revision: Each individual record of those requesting SGI access should contain the basis, i.e., the documents relied upon, for granting or denial of access to SGI. Where the access is denied a brief explanation of the reason for denial should also be provided.

NRC Response: The recommended change will be adopted and the Regulatory Guide revised to state that each individual record of those requesting SGI access should contain the documentation relied upon for granting or denial of access to SGI. In those instances where the SGI access is denied, a brief explanation of the reason for the denial should also be made a part of the individual's record. The record must be retained for one (1) year after termination of employment or denial of access to SGI in accordance with 10 CFR 73.57(f)(5).

29. Public Comment: Page 9, Section 10; the requirement for document retention is not in the Rule. This Regulatory Guide is transferring requirements from 73.57 to 73.21 without appropriate Rulemaking process. Rule language in 10 CFR 73.57(f)(5) does not include other elements of the background investigation process used for granting access to SGI such as education verification, employment verification, etc.

Public Suggested Revision: Clarify guidance to address other elements of background investigation process.

NRC Response: The Commenter is correct with the statement that the NRC is transferring requirements from 10 CFR 73.57 to 73.21 without the appropriate rulemaking process. The regulation specifically requires adherence to the requirements of 10 CFR 73.57 as they relate to the procedures for undergoing a Federal Bureau of Investigation (FBI) criminal history records check and the retention of those records. There is no regulatory requirement for Licensees to retain the documentation, other than the criminal history records check data, used in making a trustworthiness and reliability determination. The section in question will be revised to read as follows:

"Licensees shall inform individuals requesting SGI access that their fingerprints will be used to obtain information about their criminal history and that they have the right to obtain or review the content of their record to ensure that correct and complete information is used during the adjudication process as prescribed by 10 CFR 73.57(b)(3). Consistent with the requirements of 10 CFR 73.57(f)(5), the Licensees shall retain the fingerprint and criminal history records received from the FBI for a period of 1 year from the date that the individual's employment was terminated or that the individual was denied access to SGI. Additionally, Licensees should also retain documented information used to support of deny the trustworthiness and reliability determination."

30. Public Comment: Page 9, Section 12; this paragraph limits transfer of information to criminal history records and does not address other elements of the Background Investigation that need to be considered.

Public Suggested Revision: Revise the language as follows: "The determination of SGI access may be transferred to another..."

NRC Response: The language currently in the Regulatory Guide does not limit the personal information that may be re-disseminated or transferred from one licensee to another. Any limitation that may be placed upon the information that can or will be re-disseminated or transferred by a particular licensee is dependent upon the varying content of internal policies and standard operating procedures for a given licensee. The Regulatory Guide, in this context, identifies the minimal standard that must be incorporated into every internal policy and standard operating procedures that addresses or governs day-to-day procedures related to the safekeeping and storage of files containing personal information related to criminal history records.

31. Public Comment: Page 9, Section 13; the second paragraph at the end refers to Note 2. However, Note 2 doesn't apply. If more appropriate, it should be tagged to the entire Regulatory Guide since SGI and SGI-M are lumped together as just SGI. It would be less confusing if the discussions are split up into SGI and SGI-M requirements even though it will result in some redundancy.

Public Suggested Revision: Clarify or remove Note 2.

NRC Response: Throughout the Regulatory Guide, where appropriate, distinctions between SGI and SGI-M protection requirements are identified. Note two (2) may unintentionally give the impression that absent a similar footnote on other pages, a distinction in protection requirements do not exist. For that reason, the footnote referenced by the Commenter, has been removed.

32. Public Comment: Page 9, Section 13; these sections state that encrypted files containing SGI must be secured in the same manner as unencrypted files. There is no basis for this requirement. Encrypted files can be sent over unsecured email that potentially could be intercepted. These files reside permanently in retrievable electronic media. The encryption is relied upon to provide the necessary protection from unauthorized disclosure. Therefore treating encrypted information in the same manner as unencrypted information is unnecessary and should not be an expectation.

The sentence is the second paragraph starting with "Adequate storage…" should be a new paragraph." In addition, guidance is needed on the acceptability of storing SGI in safes provided in hotel room or other similar situations.

Public Suggested Revision: NEI will submit a White Paper for the handling and storage of encrypted information by October 30, 2009. NEI and the industry stake holders request a follow up meeting to further discuss this topic and review the White Paper.

Begin new paragraph with "Adequate storage…" Provide additional guidance regarding storage of SGI in hotel safes, etc.

NRC Response: While the staff is always open to suggestions for opportunities to make improvements, the Public Comment process, in so far as solicitation for comments to a draft Regulatory Guide is not the proper forum for notification of documents that may be

submitted to the NRC for consideration. Therefore, that portion of the Commenter's suggested revision will not be addressed at this time.

The Commenter is incorrect in stating that the NRC has no basis for pointing out that encrypted files containing SGI must be properly stored in accordance with 10 CFR 73.22(c)(2) and 73.23(c)(2). The regulation makes no distinction between encrypted SGI and unencrypted SGI in so far as the necessary protection requirements while the information is not in use and unattended. Two major concerns dealing with the duration of the encrypted information remaining confidential and the ability of such information to remain available are reasons for usage of secure storage containers as described in 10 CFR 73.22(c)(2) and 73.23(c)(2).

Safeguards Information can exist in one of three states at any given time; it can be: (1) in use; (2) in storage or; (3) in transmission. While in use, it must be under the control of someone that has been authorized access to SGI. When SGI is in storage, it resides within an approved security storage container as defined by 10 CFR 73.2. When SGI is in transmission (physical documents or material), the document or material must be properly packaged as prescribed by 10 CFR 73.22(f)(1) and 73.23(f)(1) and disseminated in a manner consistent with the transmission requirements of 10 CFR 73.22(f)(2) and 73.23(f)(2). When SGI is transmitted electronically, it must be packaged (encrypted) and disseminated in a manner consistent with the requirements stated in 10 CFR 73.22(f)(3) and 73.23(f)(3).

With respect to creating a new paragraph for the sentence in the second paragraph starting with "Adequate storage…," as written, the sentence is a continuation of the current subject which is "storage" and the inclusion of the sentence with the current paragraph provides a natural transition for the subsequent guidance that follows. Regulatory requirements for the safekeeping and storage of SGI have been promulgated and published by the NRC, and licensees in possession of SGI are expected to comply with those regulatory requirements. The staff does not intend to regulate through a Regulatory Guide by prescribing, beyond regulatory requirements, the content or manner of presentation of a licensee's information protection system for the protection of SGI. In those instances when licensees grant authorization for SGI to be taken out of the official storage location, licensees should emphasize that the NRC's regulations on storage of SGI continue to apply.

33. Public Comment: Page 9, Section 13; in several places the term "guard(s)" is used.

Public Suggested Revision: Replace the term "guard(s)" with either the term "security" or "security officer(s)" as appropriate for consistency with other Part 73 Regulatory Guides.

NRC Response: The use of the term "guard(s)" in the Regulatory Guide is consistent with terminology used within 10 CFR 73.22(a)(ix) and 10 CFR 73.23(a)(viii). Several NRC Regulatory Guides rely upon the term "guard(s) to identify the on-duty response force and on occasion, the term is used as a prefix to the location the response force operates from or initiates a response from. To maintain a degree of consistency with the applicable portions of 10 CFR 73.22 and 10 CFR 73.23, the term "guard(s)" will be retained within this Regulatory Guide.

34. Public Comment: Page 10, Section 15; the expectation to change SGI locks and combinations when "…individuals knowledgeable of the combination lose their need to know or access to SGI" is unnecessary and creates a significant burden on licensee without associated benefit. The requirement to change locks and combinations should be related to determining an individual's trustworthiness and reliability is in question. Changing locks and combinations when individuals no longer required access to the information would result in a continuous process.

A record of opening and closing a cabinet provides very little value for the administrative burden involved.

The term "security awareness inspection" is not a term utilized by the industry and such practice is not required.

Public Suggested Revision: Revise section to require combination change when an individual who had access to the combination has been determined not to be trustworthy and reliable.

Remove expectation concerning open/close logs.

Remove language regarding "security awareness inspection."

NRC Response: The lock combination to security containers, used to protect SGI, must be limited to a minimum number of personnel for operating purposes. Those personnel knowledgeable of the lock combination must have both a need to know and be authorized access to SGI as prescribed by 10 CFR 73.22(c)(2) and 73.23(c)(2). The Commenter's suggestion to limit lock combination changes to instances when an individual has been determined not to be trustworthy and reliable, or have otherwise not met the requirements for access to SGI, can not be supported because it conflicts with the guidance of the regulation, i.e., personnel knowledgeable of the combination to the security container must have a need to know and be authorized access to SGI. Additionally, 10 CFR 73.22(c)(2) states that "access to lock combinations must be strictly controlled so as to prevent disclosure to an individual not authorized access to SGI."

Record keeping for security container opening and closing isn't required by the regulation, but there is value in the proactive and security conscious measure. As pointed out in the Regulatory Guide, the record can be a valuable tool when conducting an inquiry on a security infraction, such as an unattended and open security container. The existence of a record that reflects opening and closing activity may identify the time frame that the security container was open and may prove to be instrumental when making a damage assessment.

The term "security awareness inspection" may not be a term utilized within the industry and will not be retained within the Regulatory Guide. The term was used to identify the process related to checking security containers and environment immediately surrounding the security container itself for SGI documents and material. The term "security awareness inspection" will be replaced with "security container checks."

35. Public Comment: Page 11, Section 16; the term "ensure" assumes specific standards for sound attenuation which do not exist.

Public Suggested Revision: Delete second paragraph.

NRC Response: The term "ensure" as used in the context of section 16, on page 11, does not imply nor require a standard for sound attenuation. The access requirements for SGI are not limited to instances of access to documents or materials and this section of the Regulatory Guide merely draws attention to that fact. Safeguards Information, in all forms, must be protected from unauthorized disclosure as prescribed by 10 CFR 73.21(a). Personnel in possession of SGI are obligated to put in place or follow established procedures that guard against the unauthorized disclosure of SGI. Safekeeping and handling practices should be purposeful and geared toward preventing unauthorized disclosure of documents, material, conversation and electronic transmissions of SGI. Therefore, no change was made.

36. Public Comment: Page 11, Section 17; guidance related to protection, in section 17 of page 11, is redundant to section 16, second paragraph. Limitations on discussions apply.

Public Suggested Revision: Delete portion of second paragraph regarding protection from sound attenuation.

NRC Response: The guidance in section 17 does reiterate a call for caution as it relates to sound attenuation, but the reiteration is purposeful and not an oversight. It is not unprecedented for someone, involved in a secure or encrypted communication, to mistakenly lose sight of the fact that they may not be in a secure environment that's appropriate for sensitive discussion. The guidance in section 17 is intended to serve as a reminder to the fact that encrypted communication equipment is not always located in an area that lends itself to uninhibited conversation.

37. Public Comment: Page 11, Section 18; wrong reference – (See Section 15 for additional guidance on SGI transmission procedures). Section 15 does not provide SGI transmission guidance as indicated.

Clarification is needed on the term "assigned to the licensee or contractor's facility."

Public Suggested Revision: Change reference to Section 28.

Provide clarification.

NRC Response: The erroneous reference to Section 15 will be corrected.

The requirement that computer systems used to produce, process or store SGI-M be assigned to the licensee or contractor's facility, is mandated by 10 CFR 73.23(g). In the context used within the Regulatory Guide, assigned to the licensee or contractor's facility should be interpreted to mean that the computer system used to produce, process or store SGI-M must be under the cognizance and/or control of a licensee that is accountable for the safekeeping and storage of the SGI-M through direct application and/or oversight.

38. Public Comment: Page 11, Section 19; guidance should use terminology such as "Smartphone or similar portable communication device" instead of brand names. SGI cannot be decrypted on such devices.

Public Suggested Revision: Modify wording as appropriate.

NRC Response: The recommendation to delete the reference to "Blackberry" has been accepted. The Regulatory Guide will be revised accordingly. It should be noted however, Smart Phone technology does provide its user with the capability to decrypt FIPS 140-2 encrypted communication. Guidance within the Regulatory Guide will continue to discourage the use of Smart Phones to process SGI.

39. Public Comment: Page 12, Section 20; the suggested limitation on use of SGI at home is unnecessary and based on assumption that the information is at higher risk to unauthorized disclosure. The requirements for the use and storage of SGI in any location are clearly defined and no further expectations should be set regarding where SGI should be used. There are legitimate reasons for persons to regularly use SGI at locations remote from sites, including at home. Restricting this ability would have a significant negative impact on the ability to conduct legitimate business.

Public Suggested Revision: Delete this section.

NRC Response: In providing guidance on the safekeeping and storage of SGI, while it is away from the licensee's facility, the staff is in no way prescribing a mandate that must be adhered to because of a regulatory requirement. The guidance in this particular section acknowledges that licensee's may authorize the couriering of SGI to one's home or private residence and that the justification for granting or denying such an authorization is licensee dependent. Any time that SGI is removed from a licensee's facility, for whatever reason, the potential for unauthorized or inadvertent disclosure increases. Because of that increased potential for unauthorized or inadvertent disclosure, the staff believes it only prudent that licensee's be reminded to emphasize SGI regulatory requirements when formulating an internal policy that addresses instances when SGI is removed from the licensee's facility.

40. Public Comment: Page 12, Section 22; this section implies that only designated and trained individuals should have the authority to designate a document as SGI. There is no requirement of training of this type.

Item (a) list information to be included on the first page of SGI material. Item (a) states the identification of the generating organization must be included. However, the rule requires that the identification of the organization making the SGI determination is required.

Public Suggested Revision: Replace "only designated and trained individuals" with "any individual authorized access to SGI."

Revise the guidance to be consistent with the Rule and merely require identification of the organization making the SGI determination.

NRC Response: The Regulatory Guide does not mandate any requirements that are not addressed in the Regulation. The referenced section contains no requirement that personnel authorized to make a SGI determination be trained, but rather suggest, through the use of "should" that those empowered personnel be trained on the details of their responsibility as it relates to making an informed SGI determination and the proper marking requirements. 10 CFR 73.22(d)(1)(i) and 73.23(d)(1)(i) require that personnel tasked with making an SGI determination be authorized to do so. Given the sensitivity of SGI and the regulatory requirements associated with both its marking and storage, licensees and others should ensure that those personnel authorized to make SGI determinations, are aware of the detailed requirements associated with that authority. Licensees and others shall establish, implement and maintain their Information Protection System, for the protection of SGI, consistent with the regulatory requirements of 10 CFR 73.21.

As recommended, item (a) in Section 22, will be revised from "the identification of the generating organization" to read "the identification of the organization making the SGI determination."

41. Public Comment: Page 12, Section 23; the requirements for marking SGI are clearly defined in the rule. Setting expectations for additional markings or cover sheets is unnecessary. Licensees may choose to add cover sheets or other controls at their discretion to assist in preventing human error, but the regulatory guide should not establish expectations for such measures beyond the rule requirements.

Public Suggested Revision: None

NRC Response: The Regulatory Guide does not mandate any marking requirements or performance expectations that are not otherwise required by regulation. Safeguards Information is at its greatest risk for unauthorized or inadvertent disclosure once it has been removed from an approved security storage container. Because of that increased risk, the staff believes it only prudent that it make recommendations for proactive measures that will assist licensees and others in their efforts to prevent or mitigate the potential for instances of unauthorized disclosure. In keeping with regulatory requirements, SGI markings 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 letters is attached to a SGI document, and is not a permanent part of the document, the actual first page of the SGI document itself must be marked according to 10 CFR 73.22(d) and 73.23(d). Additionally, the rule makes no distinction, with respect to the marking of electronic documents and hardcopy documents or other matter containing SGI. Documents or other matter containing SGI must be marked according to 10 CFR 73.22(d) and 73.23(d). Licensees shall establish, implement and maintain their Information Security System, for the protection of SGI, consistent with the regulatory requirements of 10 CFR 73.22 and 73.23.

42. Public Comment: Page 13, Section 25; this exact sentence is not appropriate for all situations.

Placement of wording at bottom of document exceeds Rule requirement.

Public Suggested Revision: Revise language to say "a statement similar to…"

Delete language regarding placement of wording.

NRC Response: Due to a punctuation placement error, the section in question reads improperly and will be revised. The revised text "When separated from Safeguards Information enclosure(s), this document is decontrolled," must be conspicuously placed at the bottom of the document, when the document contains no other sensitive information, as prescribed by 10 CFR 73.22(d)(2) and 73.23(d)(2)."

Some markings on a document, containing SGI, are well established and mandatory in nature. Other markings on the document are predicated on years of accepted practice throughout the industry and are based, in part, on a NRC attempt to standardize document markings to aid users in the expeditious location of portion markings and warning notices. Every strong and proactively based information security program, rely upon a degree of repetitive and effective procedures. For that reason, the Regulatory Guide text will be revised to state that the warning notice "should" be placed at the bottom of the SGI document.

43. Public Comment: Page 13, Section 25; guidance in this paragraph is contradictory and overly prescriptive and not required by the Rule.

The second paragraph states the individuals who arrange or participate in meetings, conferences, etc, MUST perform the (a) thru (c) actions.

Public Suggested Revision: Delete the first paragraph.

Revise the language to replace "must" with "should."

NRC Response: The guidance should not be viewed as contradictory nor interpreted as overly prescriptive. The guidance is this section, as it relates to proactive security measures, are geared toward planned meetings whereas security measures for the meeting participants can be arranged and easily accommodated. Impromptu and informal discussions routinely take place in a work environment and for that reason, there is an expectation that day-to-day security practices will prevail and those engaged in conversation, will take adequate measures to ensure that their discussion is guarded.

The second paragraph of the section in question is properly worded in that those that arrange or participate in hearings, conferences, or discussion involving SGI "must" take steps to ensure that SGI is protected against unauthorized disclosure as required by 10 CFR 73.21(a)(1).

44. Public Comment: Page 13, Section 26; there is no basis for this in the regulation. Sufficient guidance for the protection from inadvertent disclosure of SGI during conferences or meetings is provided in previous sections.

There is no basis for this in the regulation. Any person authorized for access to SGI should be able to coordinate meetings involving SGI. Limit to first-line managers and above is too restrictive. Classification and marking requirements for SGI have been previously described.

Public Suggested Revision: Delete first paragraph.

Delete second paragraph.

NRC Response: The "previous section" of the Regulatory Guide that the commenter referred to is related to impromptu or informal discussions or meetings. The section in question addresses or provides guidance for those instances where formal or structured meetings are scheduled to take place. Additionally, section 26 of the Regulatory Guide identifies proactive measures that should be taken into consideration when licensees plan conferences that will include SGI discussions.

Licensees shall construct their Information Protection System, for the protection of SGI, consistent with the regulatory requirements of 10 CFR 73.22 and 73.23.

As suggested, the reference to first-line managers and above authorizing conferences involving SGI will be removed. However, it should be noted that first-line managers and above are in the best position to influence the manner and speed with which day-to-day information security procedures are addressed and coordinated with security management.

Transcripts of hearings and meeting minutes that contain SGI, like other SGI documents, must be properly marked as prescribed by 10 CFR 73.22(d)(4) and 73.23(d)(4). While the topic of marking SGI documents had previously been addressed within the Regulatory Guide, the staff wanted to ensure that Licensees and others were mindful that transcripts and meeting minutes, from time-to-time, contain SGI.

45. Public Comment: Page 13, Section 27; recommendation that "Copier machines that have e-mail, fax or remote diagnostic capabilities should not be used to reproduce SGI, nor should facsimile machines be used to reproduce SGI" is too restrictive.

"Copiers that have been designated for the reproduction of SGI must be clearly identified." The word "must" in this sentence indicates this is a rule requirement.

Public Suggested Revision: Delete the restrictive guidance on copier machines.

Replace "must" with "should."

NRC Response: When copier machines, with e-mail, fax and remote diagnostic capability are used, the potential for unauthorized access to SGI increased exponentially. Documents may be electronically transmitted inadvertently and maintenance personnel, not otherwise authorized access to SGI, may gain access to SGI through remote or otherwise undetectable capabilities. For those reasons, the staff believes it only prudent to recommend that licensees

take proactive steps to reduce and/or mitigate risk associated with copiers that posses enhanced capabilities.

Copier machines, used to reproduce SGI, must be evaluated, as prescribed by 10 CFR 73.22(e) and 73.23(e), to ensure that unauthorized individuals cannot access SGI. Absent clear identification of the copier machine that has undergone the required evaluation as a condition for approval, the evaluated copier would be indistinguishable from any other copier that may be present within the work environment. If SGI is to be reproduced on a copier that has been approved for the reproduction of SGI, the user must be aware that he/she is not placing the information at risk for unauthorized disclosure through the mere use of a particular copier.

46. Public Comment: Page 14, Section 28(a); the requirement to double wrap hand-carried SGI is unnecessary as long as the individual maintains personal control of the information to prevent unauthorized disclosure. Also, indicating that hand-carrying information should only be done "as a last resort" is inappropriate. Individual control by an authorized individual is completely adequate protection.

(a) The rule only requires outer wrapper to be opaque. Minor issue but establishes de facto requirement.

(b)(4) Guidance language does not address use of interoffice mail system.

(c) Clarification should be added that NRC approval is required for use of the encryption described.

(d) As previously stated, encryption provides sufficient protection of SGI without additional measures. Taking "affirmative action to remove all traces of the encrypted SGI from the Internet-connected computer processing unit" is unnecessary and impractical.

Public Suggested Revision: (a) Delete requirement to double-wrap hand-carried SGI. Delete statement that indicates hand-carrying as the last resort.

(a) Replace "must" with "should." This comment also applies to (b) below.

(b)(4) Include a provision to use the interoffice mail system to transport SGI between company locations of use or storage.

(c) Add words "approved by the appropriate NRC office."

(d) Delete guidance language related to removing traces of encrypted information from systems.

NRC Response: The requirement to double wrap hand-carried SGI, is appropriate and is regulatory in nature; see 10 CFR 73.22(f)(1) and 73.23(f)(1). The commenter is correct in that the authorized possessor must maintain personal control of the information to prevent unauthorized disclosure. Maintaining control of the information does not preclude nor

negate the requirement that the hand-carried SGI be double wrapped when transmitted or transported outside of an authorized place of use of storage.

10 CFR 73.22(f)(1) and 73.23(f)(1) both state that the outer wrapper, for packages containing SGI, be opaque. The outer wrapper is intended to conceal the fact that the inner package contains sensitive information. The inner package, though marked to indicate the presence of SGI, must also protect the contents from unauthorized or inadvertent disclosure. Persons authorized access to SGI must ensure that it is protected from unauthorized disclosure as prescribed by 10 CFR 73.21(a)(1).

Given the risk associated with the physical transportation of SGI, it is always best to limit, as much as possible, the potential for unauthorized disclosure. Day-to-day operating procedures, as they relate to use of interoffice mail systems, are Licensee specific and dependant upon regulatory requirements and organizational needs. Secure electronic transmission of SGI and properly packaged parcel that is tracked by computer, present the least amount of risk and should be considered the preferred methods of transmission. Licensees shall establish and implement their Information Protection System, for the protection of SGI, consistent with the regulatory requirements of 10 CFR 73.22 and 73.23.

The commenter is incorrect in the assertion that "encryption provides sufficient protection of SGI without additional measures." Encryption provides an acceptable degree of security for SGI that is in transmission (only). Encryption, in and of itself, should only be relied upon for protecting SGI while it is in transmission. Encryption is not an acceptable means for storage of SGI when it is unattended (See 10 CFR 73.22(c)(2) and 73.23.(c)(2)). Taking affirmative action to remove all traces of the encrypted SGI from internet-connected computer processing units should be viewed as both necessary and in keeping with the requirement that both transmitters and receivers, of SGI, implement information handling processes that will provide high assurance that SGI is protected before and after transmission (See 10 CFR 73.22 (f)(3)). Office computer processing units are more susceptible to theft or manipulation than large multi-faceted servers that reside within protected rooms. For that reason, the staff believes that the taking of affirmative actions to remove all traces of encrypted SGI from the internet-connected computer processing unit, decrease the potential for unauthorized personnel to gain access to` the encrypted file.

47. Public Comment: Page 15, Section 29; the treatment of historical documents should be consistent with the guidance provided with respect to markings in Item 23.

It is not practical to identify all known recipients. There is no way of knowing who may have received these documents years before.

Clarify what is meant by the "office that generated the information."

Public Suggested Revision: Revise guidance language accordingly.

Delete the word "All."

NRC Response: The Regulatory Guide will be revised to insert guidance that addresses historical SGI documents that are in storage and the requirements of 10 CFR 73.22 (h) and 73.23(h). Licensees and others are not expected to remove historical documents from storage, solely for the purpose of conducting a review of its content for applicability of continued SGI designation. As historical SGI documents are removed from storage for use, an examination of its content should be conducted to determine the applicability of the SGI designation.

The staff has not mandated a strict SGI document accountability requirement that conflicts with the regulatory requirement of information protection. The Regulatory Guide acknowledges that multiple copies of a given SGI document can exist and as such, recommends that Licensees and others make a reasonable effort to inform all "known" recipients or possessors of that SGI document that it's content, in whole or in part, no longer meet the requirement for SGI designation.

Within the context of Section 29, the use of "office that generated the information" should be interpreted to mean "the office that originally made the SGI determination." The Regulatory Guide will be revised to make the clarification.

48. Public Comment: Page 16, Section 30; the statement "Safeguards Information must be destroyed when no longer needed or required to be maintained as prescribed by 10 CFR 73.22(i) and 73.23(i)" may imply the need to do periodic reviews and purging of files of information "no longer needed or required." Since the information is properly protected, this activity should only be conducted at the licensee's discretion.

Public Suggested Revision: Revise language to clarify that periodic reviews are not expected.

NRC Response: 10 CFR 73.21(a)(i) and (ii) require Licensees and others to establish, implement and maintain an Information Protection System for the protection of SGI. Proactive measures, such as periodic reviews, validate programmatic strengths and identify opportunities for process improvement. However, neither the regulation nor the Regulatory Guide currently prescribe the manner by which an Information Protection System is implemented and maintained. Licensees shall establish, implement and maintain their information protection system, for the protection of SGI, consistent with the regulatory requirements of 10 CFR 73.22 and 73.23.

49. Public Comment: Page 19, Paragraph 2 (Glossary Section); wording regarding "dual possession" statement is too restrictive. As written, it could be interpreted that if NRC is in possession of a copy of any document, that a licensee has, the NRC would have to determine "need to know" before the licensee could share the document with another party, even if the licensee was the originator.

Public Suggested Revision: Clarify language to indicate that a licensee can determine need-to-know regarding all SGI in their possession.

NRC Response: The definition used for "need to know" within the glossary of the Regulatory Guide, was taken from 10 CFR 73.2 and therefore cannot be modified.

50. Public Comment: Page 19, Paragraph 4 (Glossary Section); the definition as written indicates the reviewing official must make the "need to know" determination. The reviewing official is only responsible for determining trustworthiness and reliability for access to SGI. The transferring individual makes the need to know determination.

The definition states that the reviewing official "….independently reviews the results of a background check…" And "…should be an individual with access to SGI…" The reviewing official is only responsibility for determining trustworthiness and reliability for access to SGI. There is no Rule requirement for the individual to have access to SGI.

Public Suggested Revision: Revise language to remove need-to-know from this definition.

Replace "should be an individual with access to SGI" with "should be currently granted access to SGI or have UAA to a designated facility."

A reviewing official may rely upon a favorable determined criminal history/background records check within the last five years, subject to obtaining written confirmation from the previous employer that is subject to the provisions of 10 CFR 73, SGI requirements.

NRC Response: The reviewing official is responsible for making the need to know determination for access to SGI in general as it relates to official duties. Specific access to SGI documents rest with the possessor of that information. The definition for reviewing official will be modified to identify the distinction.

Access to SGI and Unescorted Access Authorization (UAA) are mutually exclusive and will not be used interchangeably in this Regulatory Guide.

The recommended change that has been proposed is procedural in nature i.e. within the licensee's purview, and something that will not be made a part of the reviewing official definition.