

REQUEST REPLY BY: 11/30/05

UNITED STATES
NUCLEAR REGULATORY COMMISSION

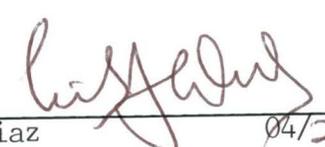
WASHINGTON, D.C. 20555-0001

REVISED VOTE

Disapproved. See attached
comments.

October 26, 2005

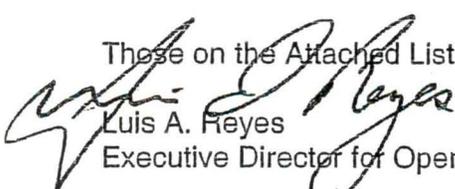
Nils J. Diaz


04/25/06

MEMORANDUM TO:

Those on the Attached List

FROM:


Luis A. Reyes

Executive Director for Operations

SUBJECT:

POLICY REVISION: HANDLING, MARKING, AND
PROTECTING SENSITIVE UNCLASSIFIED NON-SAFEGUARDS
INFORMATION (SUNSI)

In a memorandum to you dated January 19, 2005, I directed that the recommendations of the SUNSI task force be implemented by a staff working group supported by the offices and chaired by the Office of Information Services. The interoffice working group completed the requested work and identified numerous key changes on how the Agency handles SUNSI. All of those changes are identified in the attached Communication Plan, with the significant changes listed below. The new policy:

- Eliminates the need for all cover sheets except for Allegation Information and Investigation Information;
- Requires marking of header and footer for each type of SUNSI;
- Determines that portion marking of documents is not required; and
- Notes that SUNSI must be encrypted when transmitted electronically.

I am implementing the new policy and procedures effective on the date of this memorandum. The attached "NRC Policy for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information" describes the new policy and procedures which will be incorporated in the next revision of Management Directive 12.6. Additionally, over the next four months, SUNSI awareness training sessions will be held in the Auditorium. Staff should take advantage of these training sessions to become familiar with the new policy. Further training will be incorporated into the Computer Based Learning (CBT) class on Information Computer Security in the spring of 2006.

Attachments: As stated

Chairman Diaz's Comments – REVISED VOTE – COMSECY-05-0054

Upon further review of the staff's SUNSI policy and additional information, I disapprove the staff's proposed revised policy on Handling, Marking and Protecting Sensitive Unclassified Non-Safeguards Information. As stated in my previous vote, I appreciate the extensive efforts put forth by the staff in revising the policy. However, I believe that a more reasonable approach is to develop a simplified policy (including a two-tiered handling regime) that incorporates the existing SUNSI categories.

In reexamining the SUNSI policy, staff should review the handling requirements in all 14 areas to determine their adequacy with a two-tiered system, taking the following comments into consideration:

- For documents not requiring either a cover sheet or mandatory marking, the staff should evaluate if it is necessary for such documents to be considered SUNSI at all.
- Cover sheets should continue to be used for Allegation, Investigation, and Security-Related Information. Staff should follow other Federal agencies' requirements governing the use of cover sheets for sensitive information originating in those agencies.
- The use of SUNSI should be avoided while traveling on public conveyances.
- The use of encrypted email should be deferred until the Executive Branch standardizes a federal government policy.
- The current policy on destruction of material should be reexamined.

I understand the staff will be creating an eighth group of SUNSI to address the Department of Energy's Unclassified Nuclear Control Information (UCNI) and Naval Nuclear Propulsion Information (NNPI), that will be subject to more restrictive handling and marking requirements. I approve of this action.

Once the new policy is in place, training should be mandatory for all NRC agency personnel and offered to external stakeholders.



REQUEST REPLY BY: 11/30/05

UNITED STATES
NUCLEAR REGULATORY COMMISSION

WASHINGTON, D.C. 20555-0001

Approve with comments and edits.

October 26, 2005

[Signature]
Nils J. Diaz 12/8/05

MEMORANDUM TO: Those on the Attached List
FROM: *[Signature]*
Luis A. Reyes
Executive Director for Operations
SUBJECT: POLICY REVISION: HANDLING, MARKING, AND
PROTECTING SENSITIVE UNCLASSIFIED NON-SAFEGUARDS
INFORMATION (SUNSI)

In a memorandum to you dated January 19, 2005, I directed that the recommendations of the SUNSI task force be implemented by a staff working group supported by the offices and chaired by the Office of Information Services. The interoffice working group completed the requested work and identified numerous key changes on how the Agency handles SUNSI. All of those changes are identified in the attached Communication Plan, with the significant changes listed below. The new policy:

- Eliminates the need for all cover sheets except for Allegation Information and Investigation Information;
- Requires marking of header and footer for each type of SUNSI;
- Determines that portion marking of documents is not required; and
- Notes that SUNSI must be encrypted when transmitted electronically.

I am implementing the new policy and procedures effective on the date of this memorandum. The attached "NRC Policy for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information" describes the new policy and procedures which will be incorporated in the next revision of Management Directive 12.6. Additionally, over the next four months, SUNSI awareness training sessions will be held in the Auditorium. Staff should take advantage of these training sessions to become familiar with the new policy. Further training will be incorporated into the Computer Based Learning (CBT) class on Information Computer Security in the spring of 2006.

Attachments: As stated

OS NOV 15 PM 3:30
COMMUNICATIONS SECTION

Chairman Diaz' Comments on COMSECY-05-0054

I approve the revised policy on Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information, with the exception of the elimination of cover sheets for all but Allegation and Investigation Information. I understand that the staff will be creating an eighth group of SUNSI, to address the Department of Energy's Unclassified Nuclear Control Information ("UCNI") and Naval Nuclear Propulsion Information ("NNPI"), that will be subject to more restrictive handling and marking requirements. I approve of this action. I also believe that use of cover sheets should be retained for security-related information and the proposed eighth group. The use of cover sheets for these two categories, as well as Allegation and Investigation Information, will serve to distinguish particularly sensitive information from other documents and provide an additional layer of protection for that information. Finally, the staff should follow other Federal agencies' requirements governing the use of cover sheets for sensitive information originating in those agencies.

I appreciate the hard work the SUNSI task force has invested in this effort and believe that the new policy will be more effective. I also want to stress the importance of staff taking advantage of the training sessions that are available to agency personnel, to familiarize themselves with the new policy. The staff should also make the noted edits to the Communications Plan.



COMMUNICATION PLAN ANNOUNCING NEW POLICY FOR HANDLING SENSITIVE UNCLASSIFIED NON- SAFEGUARDS INFORMATION (SUNSI)

PURPOSE

The purpose of this communication plan is to address the rollout initiatives planned for implementing the new policy and simplified process for handling sensitive unclassified non-safeguards information (SUNSI) to achieve the agency's goal of preventing the inadvertent release of information to the public. SUNSI is defined as any information of which the loss, misuse, modification, or unauthorized access can reasonably be foreseen to harm the public interest, the commercial or financial interests of the entity or individual to whom the information pertains, the conduct of NRC and Federal Programs, or the personal privacy of individuals.

Previously, there were about 23 categories of information disseminated in the agency which sometimes led to confusion and inefficiencies in the marking and handling of this large number of documents. In December 2003, a task force was established to address the handling of sensitive unclassified non-safeguards information. The task force submitted its recommendation in November 2004. This communication plan explains the major changes in the policy and the communication efforts associated with these changes.

The complete SUNSI policy is currently available on the internal web, at: <http://www.internal.nrc.gov/sunsi/pdf/SUNSI-Policy-Procedures.pdf> and will be incorporated in the next revision of Management Directive 12.6.

BACKGROUND

The revised policy condenses 23 categories of information of SUNSI into seven groups. It also establishes handling requirements in 14 different areas for each of the seven SUNSI groups. The policy and handling requirements **do not** apply to sensitive or classified information.

Safeguards



KEY CHANGES/MESSAGES FROM NEW POLICY

- Simplified process for handling SUNSI to prevent the inadvertent release of information to the public.
- The previous 23 categories of SUNSI have been condensed into the following seven groups:

Allegation information
Investigation information
Security-related information
Proprietary information
Privacy Act information
Federal-, State-, foreign government- and international agency-controlled information
Sensitive internal information

Other major changes are:

separate



- Elimination of the "Official Use Only" category and its associated green cover sheet. Also, the elimination of the yellow "Proprietary Information" cover sheet (although the Proprietary category remains). Only Allegation and Investigation Information must be protected by a cover sheet, and dedicated forms exist for this purpose.
- Elimination of the requirement to add a FOIA Exemption Box to sensitive unclassified agency documents.
- Imposition of a broad page-marking requirement for documents in most SUNSI groups. If marking is required, the top and bottom of each page in the document must bear a marking (e.g., a header and footer) stating the ~~sensitivity of the information and identifying the applicable document category.~~ *SUNSI group and type of information*
- Creation of tools to help staff properly mark electronic files containing SUNSI. Extension of the NRC's "no comment" policy to questions from the public about the unauthorized release of SUNSI.
- When more than one SUNSI group applies to information, the most restrictive handling requirement of the applicable groups should be applied.
- NRC employees, consultants and contractors are responsible for ensuring the procedures specified in this announcement are ~~allowed~~ *followed* to protect SUNSI.
- The web address for SUNSI handling requirements are published on the internal web, at: <http://www.internal.nrc.gov/sunsi/>. They contain detailed requirements for areas such as applicable document categories, authority to designate, access, marking, cover sheet, reproduction, processing on electronic systems, use at home, use while traveling, physical and electronic copy transmission, storage, destruction and decontrol authority.
- Each document containing SUNSI must be properly and fully marked when such markings are required.
- No person should have access to SUNSI unless they have a need-to-know.
- Replaces Sensitive Information Screening Project (SISP) review process.
- Does not impact policies and procedures governing safeguards information (SGI) and classified information.

AUDIENCE

NRC management and staff at Headquarters and the Regions
Administrative staff responsible for processing, marking, and handling documents

REQUEST REPLY BY: 11/30/05

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

October 26, 2005

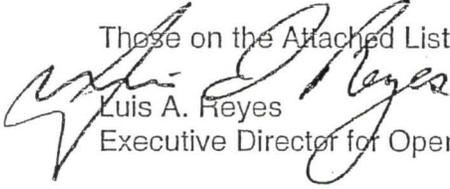
REVISED VOTE— 4/17/06

Disapproved. See attached comments.



Edward McGaffigan, Jr.

MEMORANDUM TO: Those on the Attached List

FROM: 
 Luis A. Reyes
 Executive Director for Operations

SUBJECT: POLICY REVISION: HANDLING, MARKING, AND
 PROTECTING SENSITIVE UNCLASSIFIED NON-SAFEGUARDS
 INFORMATION (SUNSI)

In a memorandum to you dated January 19, 2005, I directed that the recommendations of the SUNSI task force be implemented by a staff working group supported by the offices and chaired by the Office of Information Services. The interoffice working group completed the requested work and identified numerous key changes on how the Agency handles SUNSI. All of those changes are identified in the attached Communication Plan, with the significant changes listed below. The new policy:

- Eliminates the need for all cover sheets except for Allegation Information and Investigation Information;
- Requires marking of header and footer for each type of SUNSI;
- Determines that portion marking of documents is not required; and
- Notes that SUNSI must be encrypted when transmitted electronically.

I am implementing the new policy and procedures effective on the date of this memorandum. The attached "NRC Policy for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information" describes the new policy and procedures which will be incorporated in the next revision of Management Directive 12.6. Additionally, over the next four months, SUNSI awareness training sessions will be held in the Auditorium. Staff should take advantage of these training sessions to become familiar with the new policy. Further training will be incorporated into the Computer Based Learning (CBT) class on Information Computer Security in the spring of 2006.

Attachments: As stated

Commissioner McGaffigan's Comments - REVISED VOTE - COMSECY-05-0054

In light of recent developments and new information, I find that I must now disapprove the staff's proposed revised policy on Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information that was implemented without prior Commission review. Recent White House directives addressing the handling of sensitive but unclassified information, insights gained from the staff's briefing of the Commission, and the flaws and implementation difficulties with the current policy that have become evident, require that I modify my prior vote. I do not take this action lightly, but I no longer believe the current path is a prudent course of action. Instead, I believe the staff should develop and implement a simplified policy that will use the current SUNSI categories created by the SUNSI Task Force. In the interim, while the staff develops and implements a simplified policy, it will need to continue using the policy it chose to put in place prior to seeking Commission direction, with the exception of email encryption. As such, while it quickly works to create a simplified alternative for Commission approval, the staff should continue to train based on the existing SUNSI handling requirements and guidance. I would note that I have seen little evidence that guidance is being followed, and little training on it.

I believe the fundamental flaw in the existing policy is its complexity. The current system proposed by the staff utilizes seven categories of SUNSI, each with its own handling requirements. While many of these requirements are similar or identical among different categories of SUNSI, subtle differences require the staff to learn several sets of requirements tied to each specific category. This is an untenable system. Instead, the staff should consider developing a simplified two-tiered handling regime. This will necessitate some information being protected to a slightly higher extent than it currently is, and other requirements being relaxed. I do not believe relaxing some of these requirements poses a problem as the staff's proposal seeks to overprotect some information, imposing unworkable conditions and restrictions that the staff should reconsider in developing the new policy. Each handling regime should be given a designation noting whether the information is protected under tier "1" or "2" protection requirements. Each of the seven categories of SUNSI would be assigned to one of the two tiers (some exceptions may be necessary for a particular subset of the SUNSI categories should it require unique treatment separate from the rest of the information contained in that category). In large part I believe the staff could develop a structure in which almost all of SUNSI is handled in a consistent manner (e.g., tier "1"), with Allegations and Investigation information and certain other limited categories, such as Trade Secrets and possibly Naval Nuclear Propulsion Information, requiring a higher level of protection (e.g., tier "2").

I do not propose significantly modifying the current seven SUNSI categories (though I believe some reassessment and modification is necessary, as noted below), and believe that current training should continue to delineate the types of information that fall within each category. This two-tiered handling designation would be in addition to the designation of the applicable SUNSI category. Thus, for example, a document would be marked "Sensitive - Privacy Act Information - 1". This would note the type of information and which of the two handling regimes applies. I believe this system would also allow for simplification in training by organizing the issues into discrete subjects. Training would continue to explain and provide examples of the types of information that fall within the different existing SUNSI categories. The training would then focus on the two tiers of handling requirements, and significant differences between the tiers. Finally, these two concepts would be combined by clearly and simply stating which tier applies to each category (noting any unique exceptions to the general rule). Determining the type of information, and thus the associated handling tier designation, would be the responsibility of the originator or persons primarily responsible for handling the information. Proper initial designation of information will be of paramount importance as it will set the system of protection that will be followed by others in the agency with regard to the document. Thus, should an individual handle a document corresponding to a SUNSI category they are not familiar with, they will still know exactly what handling requirements apply.

Other slight modifications or exceptions to the two tiered system may be necessary. For instance, the policy should note that Federal, state, foreign government and international agency controlled information retains the originating agency's cover sheets and marking (though it will still be assigned a tier designation noting what additional handling requirements apply and be marked with that designation number). Those cover sheets may necessitate tier "2" designation, even if the information would otherwise be considered tier "1" if originated at NRC. Another potential problem the staff must address in its policy and training is information that qualifies under two SUNSI categories. If overlap cannot be prevented, for protection purposes, information that falls within two or more categories should be assigned the higher handling tier designation to ensure adequate protection. I believe such overlap could result in the possible over-application or misuse of the 'sensitive' label to information that should not be categorized as sensitive. The staff should reassess the SUNSI category definitions to see if they can be tightened to prevent overlap and eliminate any categories or subsets of information that should not be considered sensitive under SUNSI. The category I believe that requires the most work and reassessment is the circularly defined Sensitive Internal information (defined, in part, as "information submitted to the Commission marked Sensitive"). A document should not be marked sensitive simply because it is not yet publicly available.

In crafting this or an alternative simplified program, the staff should reexamine some of the requirements of their current policy. I believe that in some cases the staff has set requirements for protection too high, or have failed to address the implications of their proposed policy.

- **Destruction:** The destruction requirements currently envisioned in the staff's proposed policy would require the majority of SUNSI to be destroyed in such a manner as to prevent reconstruction or by placing the document in the Classified and Sensitive Unclassified Waste Disposal containers. I question whether all of the documents currently within the SUNSI rubric truly require such protections. For instance, the sensitivity of the circularly defined Sensitive Internal Information (e.g. predecisional information) is uniquely tied to timing. The staff should reassess whether the destruction requirements currently in place are in fact necessary for all types of SUNSI, and whether they need to be modified to take into account the unique nature of some documents. I also believe the staff has not properly addressed the implications of their current proposal. I believe it is unlikely that the staff will have the time or capability to tear each document into ½ inch squares, burn, pulverize or chemically decompose the documents, and thus they will likely resort to placing the documents in the Classified and Sensitive Unclassified Waste Disposal containers. This raises the question of whether the agency has the requisite resources in place to deal with the increased volume of properly disposed documents. As such, the staff should reevaluate whether the current destruction methods and requirements are in fact necessary, and address the resource needs of the agency to handle actual implementation and compliance with its destruction procedures.
- **Cover Sheets:** I continue to believe that Cover Sheets serve as a valuable reminder of the need to carefully protect sensitive information from intentional or inadvertent unauthorized disclosure. As such, the staff should reexamine their current policy addressing the need and scope of use of Cover Sheets. This is a simple method to ensure a high level of protection against inadvertent disclosure and mishandling, and if the staff determines that such measures are unnecessary, then I question the sensitive status of the information. At the very least, the staff should maintain Cover Sheets for types of information the inadvertent or willful unauthorized disclosure of which carries with it civil and/or criminal penalties. That may force some SUNSI subcategories into tier "2". The staff should also look to create exceptions necessary to prevent burdensome restrictions where the risk is minimal. For instance, Privacy Act information that may contain social security numbers, when used within a system (like the payroll system) where all those involved are familiar with the sensitivity of the information, may

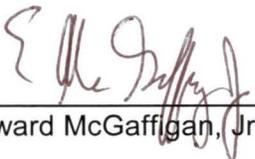
not require a cover sheet or tier "2" status. However, when such information is sent outside that system, e.g. a report on pay of particular individuals for a particular quarter, a cover sheet should be used.

- **Marking:** Mandatory marking of SUNSI documents may provide a simple tool to prevent inadvertent mishandling. A document without any markings could be disseminated throughout the agency and wind up in the hands of an individual who is unaware of its inherent sensitivity, thereby potentially leading to inadvertent release. However, as with Cover Sheets, some information (e.g. Privacy Act information) when used within a particular system where those involved are familiar with the sensitivity of the information, may not require marking. However, if the information is sent outside of the system marking should be added. Therefore, the staff should reevaluate the use of markings denoting sensitivity and the SUNSI designation, and consider whether they should be mandatory for all categories of SUNSI, or whether non-burdensome exceptions could be created for narrowly tailored situations.
- **Use At Home:** The staff should reassess the policy governing use of SUNSI at home and determine whether the restrictions currently in place, and the presumption that employees are prohibited from routinely using the information at their residences, are in fact necessary for all types of SUNSI, especially for tier "1" documents. I believe that with minimal common sense safeguards, SUNSI could be used and stored at home without undue risk to inadvertent disclosure. The current measures make little sense with some of the categories of information, such as Sensitive Internal information (e.g. the vast array of predecisional information). To apply such restrictive measures would discourage or prevent people from working with documents that have minimal associated risk. Such measures are also inconsistent with the government's efforts to encourage telecommuting and the government's contingency preparations for events such as pandemic.
- **Use On Travel:** Many of the travel restrictions (i.e. restrictions on hand carrying, storage in hotel security facilities) also seem overprotective and burdensome, especially for tier "1" documents. If the documents are kept under the control of the individual or stored out of sight with some element of safeguarding (i.e. in briefcase or closed drawer), that should be sufficient. As with use at home, I believe that overly-restrictive requirements will discourage and prevent individuals from working with documents that do not require a heightened level of protection beyond that which common sense would dictate.
- **Releasability of Sensitive Internal Information:** The staff should develop more descriptive labels for documents considered Sensitive Internal information that would establish whether the staff considers that the document should be withheld indefinitely or the document can be released at a certain time.
- **"No Comment" Policy:** In cases where NRC employees are contacted about SUNSI that appears in the public domain, the staff has applied the 'no comment' policy, noting that if there are any questions, the employee should consult with his or her supervisor or the originator of the information. Some documents, such as the EDO's June 14, 2005 memo on GSI-189 or the annual decommissioning report, were considered sensitive by certain staff for certain time periods, but should not have been. In these cases we should not adopt a "no comment" policy, but instead need to address whether the document should have been released, and, if so, then comment on it appropriately.
- **Periodic Review:** The staff should address the benefits and disadvantages of a periodic review (i.e., every five years), for documents designated as "Sensitive Internal information" with due

consideration to the recommendations due to the President pursuant to Section 2.c. (iii) of the "Guidelines and Requirements in Support of the Information Sharing Environment."

- Additions and Expansions of SUNSI: The staff should address creation of an additional category of SUNSI, to address the Department of Energy's Unclassified Nuclear Control Information ("UCNI") and Naval Nuclear Propulsion Information ("NNPI"). Proposed additions to the SUNSI groups or an expansion of the applicable document categories within a SUNSI group should be carefully considered and brought to the Commission's attention.
- Performance-Based Approach: Most importantly, as part of the simplification of this policy, the staff should consider implementing handling requirements that are more performance based, relying on the common sense of agency personnel to provide a certain level of protection. For example, instead of mandating specific requirements for use of SUNSI at home, a requirement could simply note that while using or storing SUNSI at your residence it should be stored in such a manner as to limit access and prevent inadvertent disclosure.

In developing the simplified policy, the staff should particularly take notice of the recent Presidential "Memorandum for the Heads of Executive Departments and Agencies" dated December 16, 2005. This memorandum states that acquisition, access, retention, production, use, management, and sharing of sensitive but unclassified information must be standardized across the Federal Government. This may ultimately necessitate additional changes to the SUNSI guidance and training. As such, the staff should consider crafting a policy that is similar to that used by other Federal agencies. This could lead to an easier transition should the White House's directive result in greater standardization of control over sensitive but unclassified information. To this end, the staff should examine its SUNSI categories to see if we are being over-inclusive in the types of information that we are seeking to characterize as sensitive. The staff should determine whether our sensitivity determination is consistent with other federal agencies and provide the Commission with an analysis and comparison of our SUNSI policy to what other agencies withhold as sensitive. The staff should also provide a recommendation of how to best mirror the types of information labeled by other agencies as sensitive, or explain why our policy should remain distinct. I question why the NRC should be taking the lead in making such sensitivity determinations, and wonder if we instead should be looking to other sectors of the Federal government for direction. It is for this precise reason that I firmly believe the Agency should not implement a secure e-mail procedure at this time, but should wait for the Executive Branch to formulate government-wide practices, including those for e-mail encryption.



 Edward McGaffigan, Jr.

4/17/06

 (Date)

REQUEST REPLY BY: 11/30/05

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

October 26, 2005

*Approved, subject to
 the attached comments*

*Elle Jeffrey
 12/14/05*

MEMORANDUM TO: Those on the Attached List

FROM: *Luis A. Reyes*
 Luis A. Reyes
 Executive Director for Operations

SUBJECT: POLICY REVISION: HANDLING, MARKING, AND
 PROTECTING SENSITIVE UNCLASSIFIED NON-SAFEGUARDS
 INFORMATION (SUNSI)

In a memorandum to you dated January 19, 2005, I directed that the recommendations of the SUNSI task force be implemented by a staff working group supported by the offices and chaired by the Office of Information Services. The interoffice working group completed the requested work and identified numerous key changes on how the Agency handles SUNSI. All of those changes are identified in the attached Communication Plan, with the significant changes listed below. The new policy:

- Eliminates the need for all cover sheets except for Allegation Information and Investigation Information;
- Requires marking of header and footer for each type of SUNSI;
- Determines that portion marking of documents is not required; and
- Notes that SUNSI must be encrypted when transmitted electronically.

I am implementing the new policy and procedures effective on the date of this memorandum. The attached "NRC Policy for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information" describes the new policy and procedures which will be incorporated in the next revision of Management Directive 12.6. Additionally, over the next four months, SUNSI awareness training sessions will be held in the Auditorium. Staff should take advantage of these training sessions to become familiar with the new policy. Further training will be incorporated into the Computer Based Learning (CBT) class on Information Computer Security in the spring of 2006.

Attachments: As stated

Commissioner McGaffigan's Comments on COMSECY-05-0054

I approve of the staff's revised policy on Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information, subject to the following comments. I believe the staff has done a good job in attempting to clarify the requirements and guidance for dealing with SUNSI, but would note that this is only the first step in creating an efficient, cohesive and coherent policy for protecting SUNSI. Additional modifications to the policy will be necessary to include new categories of information, such as UCNI and NNPI that will be subject to more restrictive requirements as noted in the Chairman's vote, and to incorporate comments from the staff's training sessions and lessons learned through actual practice.

I agree with the Chairman's vote that the staff should not eliminate the use of cover sheets for all but Allegations and Investigation Information. Cover sheets serve as a valuable reminder of the need to carefully protect sensitive information from intentional or inadvertent unauthorized disclosure. Therefore, cover sheets should remain in use for sensitive information, the unauthorized disclosure of which could result in civil or criminal penalties. At a minimum this would add a Proprietary Information cover sheet. The cover sheet should include a discussion of the potential civil or criminal penalties for unauthorized disclosure. I also agree with the Chairman's vote to follow other Federal agencies' requirements governing the use of cover sheets for sensitive information originating in those agencies.

It should also be noted that the staff continually refers to the 'requirements' for handling, marking and protecting the various categories of SUNSI. However, in some cases these are not in fact requirements, but are internal procedures or guidance provided by the staff as a means to prevent unauthorized disclosure. In order to avoid any potential confusion amongst the public and other agencies, the staff should review and revise this policy, and any future modifications to the policy, to clearly distinguish those provisions for handling, marking, and protecting SUNSI that are in fact requirements, derived from statutory or regulatory authority, as distinct from guidance or internal procedures.

I share the concern of Commissioner Jaczko regarding the potential inconsistent application of the 'sensitive' label for predecisional information, and would go further to emphasize the overall necessity of consistent implementation of this SUNSI policy, in particular assiduously categorizing and labeling documents.

The staff should clarify the meaning of 'need to know' required for access to various categories of SUNSI. The staff should determine whether this is the same need to know determination that would be used in gaining access to Safeguards Information under Part 73. I doubt it is for many SUNSI categories. In particular, the staff notes that for access to SGI, an individual must (1) have an authorized need to know, and (2) the information is for the conduct of official agency business. The staff should clarify whether the second requirement, that the information is for the conduct of official agency business, is in fact an element of the need to know determination and is thus redundant. Furthermore, the staff should clarify responsibility for making this need to know determination, i.e. the originator of the document.

In cases where there is doubt about granting access to SUNSI originating from outside the NRC, the staff should clarify whether the consultation suggested by the staff is for the purpose of mere notification or involves an element of deference to an originating agency's determination whether to grant access. If the staff is suggesting deference be given to the

originating agency's determination on access, the staff should clarify the level of deference it proposes. These same concerns also apply to the policy that other Government and International agencies be consulted before documents bearing restrictive markings or containing SUNSI of primary interest to them are released to the public. Again, the staff should clarify whether this consultation is for notification purposes, or whether the determinations of other Government and International agencies should be given some deference in making our own determination on granting access.

In cases where NRC employees are contacted about SUNSI that appears in the public domain, the staff has applied the 'no comment' policy, noting that if there are any questions, the employee should consult with his or her supervisor or the originator of the information. I am not sure that this is the right policy for at least one of the categories of SUNSI, the "sensitive internal information" category. We have had documents, such as the EDO's June 14, 2005 memo on GSI-189 or the annual decommissioning plan, that were considered sensitive, but should not have been. To try and impose a "no comment" policy in cases where the right answer is that the document should have been released, may lead to the agency just looking silly.

Finally, I join with the Chairman in encouraging participation in the staff's SUNSI training, noting that the comments in response to the training may prove a valuable resource in assisting in additional revisions to this policy. In addition the staff should make the necessary edits to the Communication Plan proposed by the Chairman.



Edward McGaffigan, Jr.

12/14/05

(Date)

REQUEST REPLY BY:11/30/05

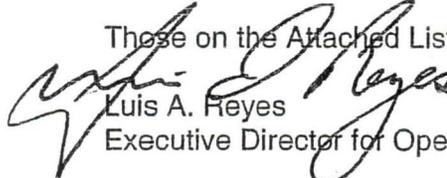
UNITED STATES
NUCLEAR REGULATORY COMMISSION
 WASHINGTON, D.C. 20555-0001

October 26, 2005

Approved.


 11/30/05


MEMORANDUM TO: Those on the Attached List

FROM: 
 Luis A. Reyes
 Executive Director for Operations

SUBJECT: POLICY REVISION: HANDLING, MARKING, AND
 PROTECTING SENSITIVE UNCLASSIFIED NON-SAFEGUARDS
 INFORMATION (SUNSI)

In a memorandum to you dated January 19, 2005, I directed that the recommendations of the SUNSI task force be implemented by a staff working group supported by the offices and chaired by the Office of Information Services. The interoffice working group completed the requested work and identified numerous key changes on how the Agency handles SUNSI. All of those changes are identified in the attached Communication Plan, with the significant changes listed below. The new policy:

- Eliminates the need for all cover sheets except for Allegation Information and Investigation Information;
- Requires marking of header and footer for each type of SUNSI;
- Determines that portion marking of documents is not required; and
- Notes that SUNSI must be encrypted when transmitted electronically.

I am implementing the new policy and procedures effective on the date of this memorandum. The attached "NRC Policy for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information" describes the new policy and procedures which will be incorporated in the next revision of Management Directive 12.6. Additionally, over the next four months, SUNSI awareness training sessions will be held in the Auditorium. Staff should take advantage of these training sessions to become familiar with the new policy. Further training will be incorporated into the Computer Based Learning (CBT) class on Information Computer Security in the spring of 2006.

Attachments: As stated

REQUEST REPLY BY: 11/30/05

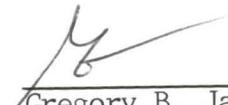
UNITED STATES
NUCLEAR REGULATORY COMMISSION
 WASHINGTON, D.C. 20555-0001

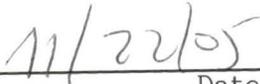
October 26, 2005

Approved. See attached comments.

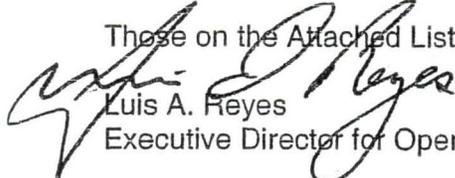
MEMORANDUM TO:

Those on the Attached List


 Gregory B. Jaczko


 Date

FROM:


 Luis A. Reyes

Executive Director for Operations

SUBJECT:

POLICY REVISION: HANDLING, MARKING, AND
 PROTECTING SENSITIVE UNCLASSIFIED NON-SAFEGUARDS
 INFORMATION (SUNSI)

In a memorandum to you dated January 19, 2005, I directed that the recommendations of the SUNSI task force be implemented by a staff working group supported by the offices and chaired by the Office of Information Services. The interoffice working group completed the requested work and identified numerous key changes on how the Agency handles SUNSI. All of those changes are identified in the attached Communication Plan, with the significant changes listed below. The new policy:

- Eliminates the need for all cover sheets except for Allegation Information and Investigation Information;
- Requires marking of header and footer for each type of SUNSI;
- Determines that portion marking of documents is not required; and
- Notes that SUNSI must be encrypted when transmitted electronically.

I am implementing the new policy and procedures effective on the date of this memorandum. The attached "NRC Policy for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information" describes the new policy and procedures which will be incorporated in the next revision of Management Directive 12.6. Additionally, over the next four months, SUNSI awareness training sessions will be held in the Auditorium. Staff should take advantage of these training sessions to become familiar with the new policy. Further training will be incorporated into the Computer Based Learning (CBT) class on Information Computer Security in the spring of 2006.

Attachments: As stated

**Commissioner Jaczko's Comments on COMSECY-05-0054
Policy Revision: Handling, Marking, and Protecting Sensitive Unclassified
Non-Safeguards Information (SUNSI)**

There are a variety of reasons I felt that Commission involvement in the Sensitive Unclassified Non-Safeguards Information (SUNSI) project was necessary. First, as I have often stated, public confidence is critical to this agency's success and impossible to garner without transparency and openness. Thus, any project which has as its premise the idea of limiting the public's access to information warrants detailed scrutiny.

Moreover, the Commission has recently provided its perspective on various information screening projects by establishing a recent Task Force to report on the public disclosure of security-related information and through voting on the Sensitive Information Screening Process (SISP). The Commission has not, however, provided its views on the broad policy issues associated with limiting from public availability unclassified, non-safeguards information. Because this is such an important issue, and in light of the Commission's prior involvement in related matters, the staff needs and deserves to have the Commission provide clarity on how it should proceed with this new SUNSI initiative.

Regarding the specifics of the staff's SUNSI proposal, I believe that the staff has, overall, forged a useful approach on a difficult issue, but I am concerned that the current guidance will not ensure consistent implementation. While the SUNSI Policy does an excellent job of reducing the overall number of categories of SUNSI information, I am not convinced that the description of each category will provide the individual authoring the document (and making the SUNSI determination) enough information to appropriately and consistently do so. For example, in the category of "Sensitive Internal Information," one identified document category is "Information submitted to the Commission marked 'sensitive'". The author of a paper for Commission review does not appear to be given any additional guidance on what information should be marked "sensitive", but only that if she marks the document "sensitive" it then falls under this SUNSI category. Defining a category to be anything marked with the category label is unhelpful and confusing.

I find this particularly troubling given that the current SUNSI process provides the author of the document the labeling authority with no established supervisory review of that decision. This makes the clarity and ease of use of the SUNSI handling requirements absolutely essential. **Thus, the staff, in consultation with OGC, should review the definition of SUNSI and the document categories to ensure that the SUNSI handling requirements are written in such a fashion that they are clear, concise and able to be consistently applied. Furthermore, the staff should establish a committee charged with periodically auditing the agency's implementation of SUNSI and reporting to the Commission on an annual basis inconsistencies identified and recommendations to improve the process.**

Furthermore, to the extent this guidance is intended to cover staff documents to the Commission, such as SECY papers, the process should integrate the direction currently outlined in chapter II of the Internal Commission Procedures document. The Commission's procedures explain that if SECY papers involve particularly sensitive matters, they should contain a specific withhold recommendation by the originating office together with supporting justification and the sensitive label. The Commission procedures continue by noting that:

Because the Commission's general policy is to release papers whenever possible, the use of this withholding category should be limited and, when used, requires solid justification for withholding on a case by case basis. The originating office must include in the supporting justification statement reasons which are sufficiently persuasive to set aside the release policy.

(Internal Commission Procedures, pg. II-3.) There does not appear to be integration of this direction into the SUNSI process. **Therefore, this review committee should also ensure that the SUNSI handling requirements effectively capture and integrate the direction provided in the Internal Commission Procedures.**

There is an additional issue regarding documents for Commission review that deserves further thought and clarification in this SUNSI guidance. Staff often marks documents for Commission review with a "sensitive" label simply because the Commission has not acted upon the item and the staff thus considers the documents to be "predecisional." That does not necessarily render the document to be "deliberative". In fact, in many of these instances the staff has no concern with the document being released following Commission action. The current SUNSI guidance does not appear to provide the staff with any alternative, however, except to mark a "predecisional" document as "sensitive." **Therefore, the review committee should address the differing intents of the "predecisional" and "deliberative" labels. For items that are only marked "sensitive" because they are considered "predecisional", the committee should provide the staff with a non-sensitive label that would allow for a more accurate reflection of the staff's intent and trigger the release of the documents upon completion of the Commission's voting process.**

Another aspect of the SUNSI process which merits attention is the lack of a periodic review mechanism to determine the continued need for protection of SUNSI. Classified documents, which are legally protected from disclosure even upon request, are either automatically declassified after a period of time or, at a minimum, periodically reviewed for declassification. I find it puzzling that unclassified NRC documents marked sensitive would appear to be eternally protected - without any automatic periodic release established or without even a periodic review to determine the necessity of the marking and protection of the document. Certainly if Classified information is subject to such review, there is little room for argument that SUNSI information should not be subject to, at a minimum, similar reviews. **Therefore, the review committee should also establish and implement an automatic release or review mechanism for documents marked with a sensitive label that ensures release or review at least every two years.**

Finally, I request that the Secretary poll the Commission regarding early release of the COMSECY so that it is made publicly available now, rather than at the end of the voting process.

Gregory B. Jaczko

Date

REQUEST REPLY BY: 11/30/05

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

October 26, 2005

SUPPLEMENTAL VOTE

Disapproved. See attached comments.

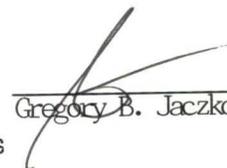
MEMORANDUM TO:

Those on the Attached List

FROM:

Luis A. Reyes

Executive Director for Operations


 Gregory B. Jaczko

 6/20/06
 Date

SUBJECT:

POLICY REVISION: HANDLING, MARKING, AND
 PROTECTING SENSITIVE UNCLASSIFIED NON-SAFEGUARDS
 INFORMATION (SUNSI)

In a memorandum to you dated January 19, 2005, I directed that the recommendations of the SUNSI task force be implemented by a staff working group supported by the offices and chaired by the Office of Information Services. The interoffice working group completed the requested work and identified numerous key changes on how the Agency handles SUNSI. All of those changes are identified in the attached Communication Plan, with the significant changes listed below. The new policy:

- Eliminates the need for all cover sheets except for Allegation Information and Investigation Information;
- Requires marking of header and footer for each type of SUNSI;
- Determines that portion marking of documents is not required; and
- Notes that SUNSI must be encrypted when transmitted electronically.

I am implementing the new policy and procedures effective on the date of this memorandum. The attached "NRC Policy for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information" describes the new policy and procedures which will be incorporated in the next revision of Management Directive 12.6. Additionally, over the next four months, SUNSI awareness training sessions will be held in the Auditorium. Staff should take advantage of these training sessions to become familiar with the new policy. Further training will be incorporated into the Computer Based Learning (CBT) class on Information Computer Security in the spring of 2006.

Attachments: As stated

**Commissioner Jaczko's Comments on COMSECY-05-0054
Supplemental Vote
Policy Revision: Handling, Marking, and Protecting Sensitive Unclassified
Non-Safeguards Information (SUNSI)**

I supplement my original vote on SUNSI only to change my vote from an approval noting my concerns to a disapproval noting the same concerns.

All of my original concerns with the proposed SUNSI policy remain and I continue to believe that these concerns must be resolved in order to ensure a consistent and transparent application of the SUNSI policy. Specifically, the staff must provide more descriptive explanations of the types of documents intended to fall within each SUNSI category and provide for a periodic review of documents marked SUNSI - especially those that fall into the "sensitive internal information" and "security-related information" categories. Nothing has changed my view on these issues since my original vote.

What has changed since my original vote is the speed in which the government-wide effort to develop a policy to deal with sensitive but unclassified information throughout the federal government is evolving. Given this multi-agency effort and what will inevitably result in a new policy regarding sensitive but unclassified information, I supplement my vote to disapprove of the SUNSI effort.



Gregory B. Jaczko

9/20/06

Date

REQUEST REPLY BY: 11/30/05

UNITED STATES
NUCLEAR REGULATORY COMMISSION

WASHINGTON, D.C. 20555-0001

October 26, 2005

Approved w/ comments + edits
[Signature] 12/13/05

MEMORANDUM TO: *[Signature]* Those on the Attached List

FROM: Luis A. Reyes
Executive Director for Operations

SUBJECT: POLICY REVISION: HANDLING, MARKING, AND
PROTECTING SENSITIVE UNCLASSIFIED NON-SAFEGUARDS
INFORMATION (SUNSI)

In a memorandum to you dated January 19, 2005, I directed that the recommendations of the SUNSI task force be implemented by a staff working group supported by the offices and chaired by the Office of Information Services. The interoffice working group completed the requested work and identified numerous key changes on how the Agency handles SUNSI. All of those changes are identified in the attached Communication Plan, with the significant changes listed below. The new policy:

- Eliminates the need for all cover sheets except for Allegation Information and Investigation Information;
- Requires marking of header and footer for each type of SUNSI;
- Determines that portion marking of documents is not required; and
- Notes that SUNSI must be encrypted when transmitted electronically.

I am implementing the new policy and procedures effective on the date of this memorandum. The attached "NRC Policy for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information" describes the new policy and procedures which will be incorporated in the next revision of Management Directive 12.6. Additionally, over the next four months, SUNSI awareness training sessions will be held in the Auditorium. Staff should take advantage of these training sessions to become familiar with the new policy. Further training will be incorporated into the Computer Based Learning (CBT) class on Information Computer Security in the spring of 2006.

Attachments: As stated

Commissioner Lyons' Comments on COMSECY-05-0054

I approve the NRC Policy for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information (SUNSI), subject to the attached edits. The policy simplifies the process for handling SUNSI and condenses 23 categories of information of SUNSI into seven groups. Future proposed additions to the SUNSI groups or an expansion of the applicable document categories within a SUNSI group should be carefully considered and brought to the Commission's attention should the total number of groups meet or exceed ten.

I agree with Commissioner Jaczko that there is a lack of a periodic review mechanism to determine the continued need for the SUNSI designations of documents. The staff should institute a review process that re-assesses the SUNSI designation of documents on a periodic basis. In addition, I agree with Commissioner Jaczko's concerns regarding the treatment of predecisional documents as sensitive. The staff should consider the development of a process for certain predecisional documents that would allow for the release of documents that could be made public following Commission voting.



12/13/05

COMMUNICATION PLAN
ANNOUNCING NEW POLICY FOR HANDLING SENSITIVE UNCLASSIFIED NON-SAFEGUARDS INFORMATION (SUNSI)

PURPOSE

The purpose of this communication plan is to address the rollout initiatives planned for implementing the new policy and simplified process for handling sensitive unclassified non-safeguards information (SUNSI) to achieve the agency's goal of preventing the inadvertent release of information to the public. SUNSI is defined as any information of which the loss, misuse, modification, or unauthorized access can reasonably be foreseen to harm the public interest, the commercial or financial interests of the entity or individual to whom the information pertains, the conduct of NRC and Federal Programs, or the personal privacy of individuals.

Previously, there were about 23 categories of information disseminated in the agency which sometimes led to confusion and inefficiencies in the marking and handling of this large number of documents. In December 2003, a task force was established to address the handling of sensitive unclassified non-safeguards information. The task force submitted its recommendation in November 2004. This communication plan explains the major changes in the policy and the communication efforts associated with these changes.

The complete SUNSI policy is currently available on the internal web, at: <http://www.internal.nrc.gov/sunsi/pdf/SUNSI-Policy-Procedures.pdf> and will be incorporated in the next revision of Management Directive 12.6.

BACKGROUND

The revised policy condenses 23 categories of information of SUNSI into seven groups. It also establishes handling requirements in 14 different areas for each of the seven SUNSI groups. The policy and handling requirements **do not** apply to sensitive or classified information. X

KEY CHANGES/MESSAGES FROM NEW POLICY

- Simplified process for handling SUNSI to prevent the inadvertent release of information to the public.
- The previous 23 categories of SUNSI have been condensed into the following seven groups:

Allegation information
Investigation information
Security-related information
Proprietary information
Privacy Act information
Federal-, State-, foreign government- and international agency-controlled information
Sensitive internal information

Other major changes are:

- Elimination of the "Official Use Only" category and its associated green cover sheet. Also, the elimination of the yellow "Proprietary Information" cover sheet (although the Proprietary category remains). Only Allegation and Investigation Information must be protected by a cover sheet, and dedicated forms exist for this purpose.
- Elimination of the requirement to add a FOIA Exemption Box to sensitive unclassified agency documents.
- Imposition of a broad page-marking requirement for documents in most SUNSI groups. If marking is required, the top and bottom of each page in the document must bear a marking (e.g., a header and footer) stating the sensitivity of the information and identifying the applicable document category.
- Creation of tools to help staff properly mark electronic files containing SUNSI. Extension of the NRC's "no comment" policy to questions from the public about the unauthorized release of SUNSI.
- When more than one SUNSI group applies to information, the most restrictive handling requirement of the applicable groups should be applied.
- NRC employees, consultants and contractors are responsible for ensuring the procedures specified in this announcement are allowed to protect SUNSI.
- The web address for SUNSI handling requirements are published on the internal web, at: <http://www.internal.nrc.gov/sunsi/>. They contain detailed requirements for areas such as applicable document categories, authority to designate, access, marking, cover sheet, reproduction, processing on electronic systems, use at home, use while traveling, physical and electronic copy transmission, storage, destruction and decontrol authority.
- Each document containing SUNSI must be properly and fully marked when such markings are required.
- No person should have access to SUNSI unless they have a need-to-know.
- Replaces Sensitive Information Screening Project (SISP) review process.
- Does not impact policies and procedures governing safeguards information (SGI) and classified information.

AUDIENCE

NRC management and staff at Headquarters and the Regions
Administrative staff responsible for processing, marking, and handling documents

person has an authorized need to know, and (2) the information is for the conduct of official agency business.

If doubt exists in any particular case whether it is proper to grant access to SUNSI originating from outside the NRC, consult with the originating party, the party, or other source from which the information was derived.

3. Ensuring legible markings on copies

All copies must clearly show the protective markings on the original document. Markings on documents submitted for reproduction should be in black or red and dark enough to be reproduced legibly.

4. Packaging SUNSI for Transmission

Material used for packaging SUNSI for physical transmission must be opaque and of such strength and durability as to provide secure protection for the document in transit, prevent items from breaking out of the container, and facilitate the detection of any tampering with the container.

5. Profiling SUNSI in ADAMS

When a document containing SUNSI is authorized to be entered into the Agencywide Documents Access and Management System (ADAMS), personnel entering the document must ensure that one of the sensitive values (Sensitive or Sensitive-Copyright, as appropriate) is marked in the "Document Sensitivity" profile property and that the "Availability" profile property is marked as "Non-Publicly Available." Identifying the appropriate document sensitivity and availability along with the markings on the documents will aid in protecting SUNSI. It will also alert staff to the sensitivity of the document when it is requested under Freedom of Information Act or the Privacy Act, thus ensuring that the document is properly reviewed under FOIA and Privacy Act exemptions standards.

6. Removal of Markings

Normally a document will retain its markings until the agency decides that the document will be made public either on its own discretion, or in response to a FOIA request. Before releasing a document with a SUNSI marking, the marking on the copy to be released should preferably be blackened out, or at a minimum, marked through in such a way that it conveys that the marking is no longer applicable to the document. This should be done on each page containing a marking.

REQUEST REPLY BY: 11/30/05

UNITED STATES
NUCLEAR REGULATORY COMMISSION

WASHINGTON, D.C. 20555-0001

October 26, 2005

Disapproved. See attached
comments.

Peter B. Lyons 5/12/06
Peter B. Lyons Date

MEMORANDUM TO: Those on the Attached List

FROM: *Luis A. Reyes*
Luis A. Reyes
Executive Director for Operations

SUBJECT: POLICY REVISION: HANDLING, MARKING, AND
PROTECTING SENSITIVE UNCLASSIFIED NON-SAFEGUARDS
INFORMATION (SUNSI)

In a memorandum to you dated January 19, 2005, I directed that the recommendations of the SUNSI task force be implemented by a staff working group supported by the offices and chaired by the Office of Information Services. The interoffice working group completed the requested work and identified numerous key changes on how the Agency handles SUNSI. All of those changes are identified in the attached Communication Plan, with the significant changes listed below. The new policy:

- Eliminates the need for all cover sheets except for Allegation Information and Investigation Information;
- Requires marking of header and footer for each type of SUNSI;
- Determines that portion marking of documents is not required; and
- Notes that SUNSI must be encrypted when transmitted electronically.

I am implementing the new policy and procedures effective on the date of this memorandum. The attached "NRC Policy for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information" describes the new policy and procedures which will be incorporated in the next revision of Management Directive 12.6. Additionally, over the next four months, SUNSI awareness training sessions will be held in the Auditorium. Staff should take advantage of these training sessions to become familiar with the new policy. Further training will be incorporated into the Computer Based Learning (CBT) class on Information Computer Security in the spring of 2006.

Attachments: As stated

Commissioner Lyons' Comments - - Revised Vote - - COMSECY-05-0054

I am revising my vote with respect to the NRC Policy for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information (SUNSI) in light of suggested improvements to the SUNSI policy that would simplify the overall policy. The SUNSI policy should be as simple as possible to follow while still achieving the goal of protecting certain information from inappropriate release. In this respect, I believe that the staff did a good job in condensing 23 categories of information of SUNSI into seven groups. The Chairman and Commissioner McGaffigan's revised votes on this matter further simplify the SUNSI handling designations, and I agree with the proposal to establish a two-tiered handling system.

To summarize, each of the seven SUNSI categories would be assigned a protection level designation: Tier 1 or Tier 2. Almost all of the SUNSI would be designated as Tier 1 and would be handled in a consistent manner. SUNSI that may merit more handling control, such as Allegation and Investigation information and other limited SUNSI categories, would be designated as Tier 2.

I believe that basic SUNSI handling provisions should be reasonable and allow the staff flexibility in the manner in which documents are protected. The overall goal should be to heighten individuals' sensitivity to SUNSI documents such that a person knows to exercise more caution with respect to these documents. As Commissioner McGaffigan said, the goal should be to rely primarily on the common sense of agency personnel to provide protection. The following are my suggestions:

What should Tier 1 handling look like?

Under the current policy, there are many categories of handling provisions for each of the SUNSI groups. I believe that Tier 1 handling should have the following attributes for the various categories of handling provisions:

Access

NRC and contractor personnel who need the material for official purposes.

Marking

All pages of a SUNSI document should be marked, with the exception of Privacy Act information that is stored and used solely by agency personnel who work primarily with Privacy Act information. The staff may identify other similar sets of voluminous material that would not require marking because it remains in the exclusive control of an office group.

Cover sheets

Cover sheets are not needed for Tier 1 SUNSI information.

Reproduction

Reproduction should only be done to the extent necessary for official purposes, and markings (if present) should remain visible on any copies.

Use at home

While using or storing SUNSI at an employee's or contractor's residence, the SUNSI should be stored in such a manner as to limit access and prevent inadvertent disclosure.

Use while traveling or commuting

The use of SUNSI is acceptable while in transit provided that the information cannot be seen by persons not authorized access. Particular care should be taken where others may be sitting or standing in close proximity to where the information is being used. SUNSI material should be kept under the control of the traveler or stored out of sight, such as in a closed drawer or briefcase (for example, if left alone in a locked hotel room).

Hard copy transmission

SUNSI may be transmitted within the agency by hand carrying or by using a messenger envelope for interoffice mail.

Opaque envelopes should be used for transmission outside of the agency, unless a document is carried with a person who has access.

Electronic copy transmission

The agency should not implement a secure e-mail procedure at this time but should wait for the Executive Branch to formulate government-wide practices.

Storage

SUNSI material to be stored at an NRC office may be stored openly. SUNSI material to be stored outside of an NRC office should be stored in a file cabinet or storage container.

Destruction

SUNSI material to be disposed of at an NRC office may be placed in a recycling bin. SUNSI material to be disposed of outside of an NRC office should be torn into ½ inch squares, burned, pulverized, or chemically decomposed to render it illegible.

Decontrol

The staff should consider options for decontrolling SUNSI designations, which take into account resource implications. The staff should consider as one option the following process:

SUNSI users (staff and contractors) would receive an announcement every year to evaluate the SUNSI material in their possession to verify that the material continues to fall within a current SUNSI designation. If not, the document would no longer be treated as SUNSI. Recognizing that the same document could be treated in an inconsistent fashion, this furthers the goal of relying on the common sense of agency personnel.

Material deemed to be SUNSI, but only for a limited period of time, would bear a calendar date on which it can be safely assumed that the document would no longer be deemed to be SUNSI. If no calendar date can be derived, the document would be designated SUNSI without expiration and should be decontrolled during the annual review (see previous paragraph).

What SUNSI categories should be designated as Tier 1?

I believe that the bulk of SUNSI should be designated as Tier 1: Security-related information; Proprietary information; Privacy Act information; Sensitive internal information; and External-government information (Federal, State, foreign - unless the originator has other handling requirements).

DOE's Unclassified Nuclear Control Information and Naval Nuclear Propulsion Information should be added as an eighth SUNSI category and designated Tier 2. Allegation Information and Investigation Information should be Tier 2.

Tier 2 handling procedures should provide a greater level of protection than those for Tier 1. The staff should develop handling procedures for Tier 2, using Tier 1 procedures as a starting point.

J. Lee Lyon
5/12/06