POLICY ISSUE
(Notation Vote)

February 14, 2006 SECY-06-0036

FOR: The Commissioners

FROM: Luis A. Reyes
Executive Director for Operations /RA/

SUBJECT: Public Disclosure Options Within the Security Cornerstone of the Reactor Oversight Process

PURPOSE:

To respond to the Staff Requirements Memorandum (SRM) dated August 15, 2005, on "SECY-05-0082 - Revised Assessment Process for the Security Cornerstone of the Reactor Oversight Process," and provide options and a staff recommendation regarding public disclosure of certain security-related information within the security cornerstone of the reactor oversight process (ROP).

SUMMARY:

Based on its evaluation, the staff recommends the Commission maintain the Security Cornerstone within the ROP, continue implementation of the revised security assessment process, and provide more public access to security-related information. This approach would improve the balance between the agency's strategic goal of openness in carrying out the regulatory process, and the protection of sensitive information in order to protect the public and promote the common defense and security. The approach also maintains the current ROP infrastructure to support the Security Cornerstone and the integrity of the revised security assessment process within the ROP, allowing for its continued implementation without significant resource impacts.

CONTACT: Paul W. Harris, NSIR/DNS
(301) 415-1169

BACKGROUND:

On February 5, 2004, the staff provided the Commission a set of options and a full discussion of pertinent issues associated with the treatment of security information under the ROP (SECY-04-0020, “Treatment of Physical Protection Under the Reactor Oversight Process”). The paper presented six options for the Security Cornerstone. The options ranged from the process in place prior to September 11, 2001, to complete removal of the Security Cornerstone from the ROP and complete withholding of all security-related information from the public. In its SRM dated March 29, 2004, the Commission directed the staff to maintain the Security Cornerstone within the ROP, but make no security oversight information publicly available. The staff was directed to develop a separate process to address how security-related inspection findings would be considered when determining appropriate agency response.

Further, the staff was directed to develop a classified report to Congress describing the results of force-on-force exercises, of which an unclassified version would also be submitted to Congress and issued to the public describing general security-related information without revealing any site-specific details. This report was subsequently established as a statutory requirement in the Energy Policy Act of 2005. The staff implemented the Commission decision which was announced to the public on August 4, 2004. The announcement included the Commission commitment to provide pertinent information to State and local officials and other federal agencies.

On May 12, 2005, the staff forwarded to the Commission a revised method for assessing security performance of nuclear power reactor licensees (SECY-05-0082, “Revised Assessment Process for the Security Cornerstone of the Reactor Oversight Process”). The staff described the development and initial implementation of a security assessment process that was similar to, but independent of the Reactor Safety ROP assessment process. The staff’s plan also noted that under the current processes, most security-related information would not be publicly available. Specifically, the following would be withheld from public disclosure: (1) schedules for planned security inspections; (2) inspection findings for security inspections; and (3) security-related NRC Inspection Manual Chapters, Inspection Procedures, and Temporary Instructions. However, to provide as much information to stakeholders as possible and to improve security-related assistance to State and Federal partners who may respond or assist during a security event at a commercial power reactor, the staff added a new action to its Proposed Security Cornerstone Action Matrix entitled "External Communications," in which the staff provides more information to States and other security partners. This action helps ensure that State officials, Department of Homeland Security, Congress, and other federal agencies, as necessary, are appropriately and promptly informed of performance changes in a licensee's security program and enhances the transparency to authorized officials of the security assessment process within the ROP.

In its SRM, dated August 15, 2005, the Commission approved the staff's proposal for assessing the security performance of reactor licensees and also directed the staff to (1) "share with the Commission options for making further progress on openness with the security portion of the reactor oversight process" and, in particular, (2) "recommend whether it is feasible to make

inspection reports publicly available after completion of long-term corrective actions."

DISCUSSION:

The staff has implemented previous Commission direction, including steps to reduce public access to information from the security oversight program for nuclear power plants, fuel cycle facilities, and other licensed activities. Within prescribed limitations, the staff has met with external stakeholders in different forums since the March 29, 2004, SRM was issued, including activities such as the Regulatory Information Conference and two security public meetings. Feedback during these public meetings, combined with direct correspondence with stakeholders, and that provided from the external ROP survey, have provided the NRC with insights regarding improving the openness of the security assessment process within the ROP and an appropriate balance between openness and the need to protect sensitive information. In these interactions, the staff has received numerous comments from non-governmental stakeholders describing their dissatisfaction with the level of public information available concerning licensees' performance in the security area.

Restricting the public access to security performance information has made it difficult for the staff to achieve the NRC's goal of openness in the area of security. Equally important is that this lack of transparency restricts public access and involvement in regulatory decisions necessary to ensure the secure use and management of radioactive materials, as well as the public's awareness of NRC's efforts in this area.

The staff would make appropriate determinations to assure that the information released will not be useful to a potential adversary. These staff evaluations will be consistent, in part, with the framework for making decisions on withholding information established in the Staff Requirements Memorandum for SECY-04-0191, "Withholding Sensitive Unclassified Information Concerning Nuclear Power Reactors from Public Disclosure," dated November 9, 2004, for SECY-05-0101, "Withholding from Disclosure Sensitive Unclassified Intermation Concerning Materials Licensees and Certificate Holds," dated October 7, 2005, and the October 26, 2005 NRC Policy for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information. The staff has developed the following options for Commission consideration. The alternatives described below provide a range of approaches that could be implemented if the Commission decides to revise the current practice.

OPTIONS:

***Option 1*: Maintain the status quo. No security-related information will be made publicly available pursuant to SRM SECY-04-0020, March 29, 2004.**

In this option, the staff continues to use the Physical Protection Significance Determination Process (PPSDP), and provide stand-alone security inspection reports to licensees and affected States[1] (consistent with Chairman Diaz's letter to Governors dated May 28, 2004, and the staff's May 2005 letter to the States), and withhold security-related oversight information from the public. The licensee would be able to provide additional information on more significant inspection findings at a Regulatory Conference which would not be open to the public. Security-related Plant Issues Matrix (PIM) entries, inspection schedules, color designations of findings, and performance indicator (PI) data would not be available to the public. Security-related discussions would not be provided in the periodic assessment letters and during the annual assessment public meetings. Further, the results of the Security Cornerstone PIs and inspection findings would not be integrated into the ROP Action Matrix. Inspection procedures, temporary instructions, and inspection schedules would be maintained as safeguards or security-related information and be exempt from public disclosure. If the NRC receives a Freedom of Information Act (FOIA) request for security-related information, the NRC will carefully review the records under the FOIA legal standard. The Security Cornerstone would remain within the ROP and security-related inspection findings would be assessed separately using the Physical Protection Significance Determination Process within the security assessment process.

Pursuant to the SRM dated March 29, 2004, and Section 170D of the Energy Policy Act of 2005, the staff continues to develop classified and unclassified reports for Congress describing the results of force-on-force exercises and other security oversight activities. The unclassified version will also be provided to the public describing general security-related information without revealing any site-specific or generic details.

Advantages:

- Maintains the status quo with no change to budgeted resources.
- Provides the highest level of information security control.

Disadvantages:

- Emphasizing information security control, this option may be perceived to

[1]As used here, "affected States" refers to those States in which the commercial power reactor facility resides and those States whose boundary is intersected by the reactor facility's 10 mile emergency planning zone. This definition also applies to those States who have an NRC-recognized commitment to provide contingency response resources to preclude or mitigate a security event at the subject site.

improperly balance the agency's general goal of openness in carrying out the regulatory process, and the need to protect sensitive information in order to protect the public health and safety and promote common defense and security.

***Option 2*: Maintain the Security Cornerstone within the ROP, continue implementation of the revised security assessment process, and provide limited security-related information to the public.**

Similar to Option 1, with the exception that security inspection report cover letters would be publicly available. The information in the cover letter would be limited to a description of the site inspected and the date of the inspection. A standardized summary sentence would also be provided in one of the two sub-option formats:

Sub-option A: The summary sentence would state: Prior to leaving the site, NRC inspectors verified that the licensee was in compliance with applicable security requirements within the scope of this inspection. NRC neither confirms nor denies whether security-related deficiencies were identified during the inspection at a site.

Sub-option B: The summary would state: An NRC inspection was conducted in one or more of the attributes of the Security Cornerstone (e.g., access authorization, access control, physical protection, and/or contingency response). In addition, if the inspection resulted in no findings, this would be stated. If the inspection resulted in one or more findings, a description of the attributes affected would be provided with a statement that the deficiencies were promptly corrected or compensated and that the licensee was in compliance with applicable physical protection and security requirements within the scope of this inspection prior to the inspector leaving the site. Once the significance of the findings has been determined, the staff would assess whether to make this security information available to the public.

The NRC requires licensees to take timely compensatory measures or corrective actions to address identified violations, deficiencies, or vulnerabilities. However, for conditions in which a potential adversary would be able to exploit, circumvent or take advantage of a vulnerability which has only interim compensatory measures employed, these cover letters would not be released. Such examples include significant contingency response or intrusion detection system deficiencies that require immediate compensation that have not yet been permanently corrected by the licensee. In such cases, the inspection would not be disclosed to the public until permanent corrective actions have been completed by the licensee and verified by NRC inspectors. At that time, the NRC would prepare a cover letter for public release. This graded

approach ensures the protection of sensitive information and the common defense while providing appropriate information to the public.

For Sub-option A or B, no discussion would be provided regarding an overall assessment of licensee security performance, inspection periodicity, or any other sensitive information.

Option 2 would promptly inform the public that an NRC inspection was conducted at a particular licensee and maintains appropriate control over the details associated with the scope of the inspection, potential vulnerabilities, and the overall licensee performance assessment in the Security Cornerstone. This option would protect sensitive security information and improve openness and transparency in a controlled and graded manner. It would also provide additional incentive for licensees to improve performance, because this option provides timely non-sensitive security-related information to the public, enhancing public awareness and confidence in NRC's independent role to protect public health and safety and promote the common defense and security. This would likely contribute to improving public awareness and involvement in the NRC regulatory process.

Although public dissemination of Option 2B information could result in rudimentary performance trending on a nationwide and site-specific basis, wrongful use of this information should not reasonably contribute to exploitation of vulnerabilities nor does it challenge the secure use and management of radioactive material. However, for conditions in which a potential adversary may be able to exploit a vulnerability which has only been compensated, these cover letters would not be released until permanent corrective actions have been implemented by the licensee and verified by NRC inspectors.

The staff would maintain control of site-specific safeguards information or industry weaknesses or vulnerabilities. The staff would not develop a standardized PIM entry (available through the NRC’s public web site) regarding the color designation of any finding or statement that the deficiency was corrected/compensated, or periodic assessment letters. However, the staff would continue to assess the level of openness and website public access to security information utilizing a graded approach.

Option 2A:

Advantages:

- Improves the balance between the agency's general goal of openness in carrying out the regulatory process, and the need to protect sensitive information in order to preserve the public health and safety.

- As compared to Option 1, Option 2A, better informs the public of NRC inspection activities in the Security Cornerstone.

- Maintains the current ROP infrastructure to support the Security Cornerstone.

- Maintains the integrity of the revised security assessment process within the ROP.
- No impact on budgeted resources.

Disadvantage:

- Provides little to no information regarding licensee security performance.

Option 2B

Advantages:

- Improves the balance between the agency's strategic goal of openness in carrying out the regulatory process, and the need to protect sensitive information in order to preserve the public health and safety.
- Implements the release of security information in a controlled and graded manner.
- Provides additional incentive for licensees to improve performance.
- Enables appropriate control of significant licensee performance deficiencies requiring longer-term compensatory measures.
- Maintains the integrity of the revised security assessment process within the ROP.
- Minimal impact on budgeted resources.

Disadvantage:

- Increases the amount of security and licensee performance information available to a potential terrorist.

***Option 3*: Provide redacted security information, such as security inspection reports, to the public after the completion of long-term corrective actions.**

The public would have access to a redacted version of the security inspection report after NRC

verification of licensee's permanent corrective actions (i.e., several months later). This redacted inspection report may provide more site-specific licensee information. However, the staff notes that the information would be limited and of marginal value in light of sensitive unclassified information controls. The redacted version of the inspection report could identify the particular area or areas of the Security Cornerstone that was inspected (e.g., access authorization, access control, physical protection, and/or contingency response) and any associated non-sensitive inspection-related information such as inspection sub-topics (e.g., fitness for duty, vital area controls, protective strategy assessment, and insider threat mitigation).

Depending upon the effectiveness of redaction, the public report could link a physical protection or security attribute to an identified, but corrected deficiency or vulnerability, since a violation would be cited. However, the resulting paragraph within the inspection report would likely need to be redacted. Through process of elimination, there is a possibility that a member of the public could trend and track licensee performance within specific areas of the Security Cornerstone and be potentially more informed of licensee programmatic or cross-cutting issues or potential generic vulnerabilities.

The staff notes that Option 3 is consistent with the permissive requirement of 10 CFR 73.21(b)(3)(i) which states that "[i]nformation regarding defects, weaknesses or vulnerabilities may be released after corrections have been made." However, DG-SGI-1, "NRC's Designation Guide for Safeguards Information," dated September 30, 2005, provides the following guidance:

> Generally, information on defects, weaknesses or consequences will not be released even after corrections have been made. The rationale is that a weakness corrected at one facility may not yet be discovered at another facility. Corrected weaknesses or consequences may be designated as 2.390 information by licensees.

As a result, Option 3 could provide public access to information from which one could ascertain physical protection and licensee performance information that was previously removed from disclosure by Staff Requirements to SECY-04-0020.

Advantage:

- Provides greater public access to information about NRC security oversight and licensee performance.

Disadvantages:

- Redacted inspection report information would be limited and of marginal value.

- As a result of long-term compilation, there exists a possibility for trending of licensee performance within specific areas and increased awareness of licensee programmatic or cross-cutting issues or potential generic vulnerabilities.

- Larger expenditure of resources for a small enhancement to the balance of openness and security.

RESOURCES:

The efforts described in Option 1 have already been budgeted for FY2006 and beyond.

For Option 2A, the staff does not anticipate the need for additional resources. For Option 2B, the staff estimates 160 reactor security inspection reports (baseline, special, and force-on-force reports) will be issued per year on a nationwide basis. Based on this issuance rate, resource implications consider an increased level of public and media interaction as well as program doctrine revisions. The level of effort is estimated annually to be 1.0 FTE more than Option 1 (0.8 FTE in the regions and 0.2 FTE headquarters).

Option 3 would have resource implications consisting mainly of a redacted inspection report (additional staff reviews, training, and administrative services are required), revision of staff guidance associated with the ROP Security Cornerstone, and an increased level of public and media interaction. Option 3 would require approximately 6 FTE annually more than Option 1, specifically 4.8 FTE in the regions and 1.2 FTE headquarters.

Any resource adjustments will be provided to the Commission with the FY2007 and FY2008 budgets which the staff is currently developing. For Options 2 and 3, FY2006 work will be accomplished utilizing existing resources.

COORDINATION:

The Office of the General Counsel has reviewed this Commission paper and has no legal objections to its contents.

The Office of the Chief Financial Officer has reviewed this Commission paper for resource implications and has no objections.

RECOMMENDATION:

The staff recommends that the Commission approve Option 2, Sub-option B. After sufficient

time to implement and assess this option, the staff will evaluate the need for additional enhancements in its efforts to strike the appropriate balance between openness and security.

/RA/

Luis A. Reyes
Executive Director
for Operations