POLICY ISSUE
(Notation Vote)

November 24, 2008 SECY-08-0185

FOR: The Commissioners

FROM: R. W. Borchardt
Executive Director for Operations

SUBJECT: OPTIONS FOR SECURITY OPENNESS, TRANSPARENCY, AND REACTOR OVERSIGHT PROCESS IMPROVEMENTS

PURPOSE:

To obtain Commission approval of recommended options related to (1) the amount of U.S. Nuclear Regulatory Commission (NRC) security-related inspection and licensee performance information available to the general public without jeopardizing security or revealing actual or potential vulnerabilities, and (2) improving staff efficiency by recombining various aspects of the security cornerstone with the other six cornerstones of the Reactor Oversight Process (ROP) for commercial nuclear power licensees. This paper also summarizes the staff's evaluation of comments received from its outreach efforts to solicit external stakeholder comment on options to enhance openness and transparency of NRC security inspection programs and licensee performance information.

SUMMARY:

The staff describes three options. The first option is to maintain the *status quo* with regard to the current level of openness and transparency associated with NRC security inspection and licensee performance information. Option 2 enhances the level of openness and transparency

CONTACTS: Paul W. Harris, NSIR/DSO
(301) 415-1169

Terrence G. Barry, NSIR/DSO
(301) 415-7044

and improves staff efficiency by: providing additional information in the NRC's Annual Security Report to Congress[1] and NRC's cover letters to security inspection reports; making the security performance indicator (PI) and significance determination processes (SDPs) available for public review; and re-combining the safety and security ROP self assessments (SAs), the NRC's annual assessment letters communicating commercial power reactor licensee performance, and the annual ROP public meetings. This option maintains the separate security and safety action matrices. This option also recommends that the inspection report cover letter actions be applied to other NRC inspection programs (i.e. fuel cycle facilities) where applicable. Option 3 is the full integration of the security cornerstone back with the other six cornerstones of the ROP, including integration of the security and safety action matrices in one combined program.

Options 2 and 3 can be accomplished without releasing security-related information that could challenge facility security, safeguarding of NRC-licensed materials, or effective control of sensitive information, such as that designated as Classified or Safeguards Information (SGI), or Official Use Only (OUO) Security-Related Information (SRI). No information would be released until any site-specific or generic issue has been adequately compensated or corrected. The information being recommended for release will not identify site-specific or generic vulnerabilities, nor would it aid in the planning or conduct of hostile action against critical infrastructure or NRC-regulated facilities or activities.

BACKGROUND:

On October 25, 2007, the staff provided the Commission SECY-07-0189, "Staff Considerations Regarding Increased Openness and Transparency in the Security Inspection Programs." The staff informed the Commission that it was considering various actions to enhance the level of openness and transparency associated with security-related NRC inspection and licensee performance information. The Commission was informed that the staff was considering making inspection findings more transparent, reinstating public reporting of security PI results, making NRC inspection procedures and mid-cycle and end-of-cycle security cornerstone licensee performance assessment letters publicly available, and possibly recombining the security cornerstone with the other six ROP cornerstones. The staff also informed the Commission that public meetings would be held to discuss these considerations and to gain public insights to inform staff's recommended options and that any resulting Commission direction would be applied to other NRC security oversight programs as well.

The staff issued a *Federal Register* Notice to solicit comments on options to increase security openness and transparency and conducted four public meetings. The staff also directly informed public interest groups, such as the Union of Concerned Scientists (UCS), Project on Government Oversight (POGO), Greenpeace, Mothers for Peace, and industry groups such as the Nuclear Energy Institute (NEI). Details of the staff's outreach effort and a summary of the public comments will be placed on the NRC website.

The staff communicated with Federal security counterparts to enhance their awareness and understanding of the openness initiative and to present them with an effective opportunity to

[1] NUREG-1885, "Report to Congress on the Security Inspection Program, for Commercial Nuclear Power Reactors and Category I Fuel Cycle Facilities: Results and Status Update."

comment. The staff also informed the U.S. Department of Homeland Security, Federal Bureau of Investigation, U.S. Coast Guard, and U.S. Department of Energy, including Naval Reactors.

The comments received from the public followed three major themes. First, the general public desired more timely and useful information in order to make an informed decision about current (or recent) security performance of NRC licensees. The public was concerned that they could not make informed decisions regarding security because the only information they are provided about security performance at the site is received via the news media or rumor mill. The public was most interested in knowing of a licensee's overall security performance and, in particular, that of Force-on-Force (FOF) exercises.

The second theme, voiced by public interest organizations (e.g., UCS and POGO) was that the NRC should be entirely consistent and release all security-related information that is not designated Classified, SGI, or OUO-SRI. The staff notes that because the security environment has changed, sensitive information control requirements have tightened since September 11, 2001. This position requests that security openness and transparency be restored closer to a pre-9/11 level of control.

The third theme communicated by the industry and NEI was that the NRC is already a very open and transparent agency through, in part, its licensee performance public meetings, publicly-available security inspection report cover letters, its inspection information posted on its ROP website (http://www.nrc.gov/NRR/OVERSIGHT/ASSESS/index.html), and by its communications with Congress, licensees, and State governments. NEI also asserted that NRC's openness and transparency is already based on a reasonable balance of the public's right to know and the need to protect sensitive information.

DISCUSSION:

The NRC has traditionally provided the public with a significant amount of health and safety information about the facilities and materials for which the NRC has regulatory responsibilities. This level of openness and transparency, as part of the NRC's Organizational Excellence Objective, has been and remains an important part of the NRC's regulatory agenda to achieve its safety and security goals, as described in its *Strategic Plan, Fiscal Years 2008-2013*, NUREG-1614, Vol. 4, February 2008. Effective implementation of this objective helps enhance public awareness of the NRC's independent role in protecting public health and safety, the environment, and the common defense and security. Furthermore, it helps enable accurate and timely communication to the public about the how the NRC views individual licensee safety/security performance. Lastly, it facilitates early communication with stakeholders on issues of substantial interest and it contributes to fair, timely, and meaningful stakeholder involvement in NRC decisionmaking. These outcomes help build public confidence in NRC's ability to effectively license and regulate the Nation's civilian use of byproduct, source, and special nuclear materials. However, there is a balance between providing SRI to the public and withholding information that may be useful to an adversary.

In proposing the following options, the staff remains consistent with the existing requirements for Classified, SGI, and OUO-SRI information. The staff also utilized Commission directives to assist in the classification of information that is clearly not Classified, or SGI. In particular, the staff implemented the guidance described in COMSECY-02-0015, "Withholding Sensitive

Homeland Security Information," that provided withholding criteria and a standard that information should be withheld when its release would provide a clear and significant benefit to a terrorist in a potential attack. In addition, SECY-04-0191 found that staff's use of reasonable judgment was sometimes necessary in reaching conclusions or professional consensus on the relative usefulness of non-classified, non-safeguards, or non-SUNSI information to a potential adversary planning or conducting a hostile act against a regulated activity. Additionally, in its Staff Requirements Memorandum (May 7, 2004), the Commission directed that the staff revise its basic standard for withholding information from the public to cover information that "could reasonably be expected to be useful" to persons planning or executing hostile actions against NRC-licensed facilities or licensed materials. Lastly, the staff reviewed SECY-05-0091, "Task Force Report on Public Disclosure of Security-Related Information," in its development of the following options.

Evaluation Criteria

1. Disclosure of licensee security performance information needs to be consistent with and accomplished in accordance with statutory and regulatory requirements.

2. Disclosure of licensee security performance information (findings, assessments, etc.) will be released only if: (a) the information does not disclose site-specific or generic vulnerabilities; (b) the information is not exploitable (i.e., it can not aid in the planning or conduct of a hostile act); and (c) the specific issue, no matter if it is site-specific or generic, has been adequately compensated or corrected.

3. Disclosure of more information would enhance the knowledge of an average member of the public reading publicly-available information (e.g., electronic or printed) in order to be involved in and/or to understand NRC's disposition of security inspection findings and/or assessment of historical site-specific security performance inspection report cover letters.

Option 1

Maintain the *status quo*. Currently, the staff provides limited information (e.g., that security inspections have been conducted, and whether there were Green or greater-than-Green findings.) The staff also provides information related to numbers of violations in the Annual Security Report to Congress. The staff notes that this is a viable, conservative, and reasonable option that balances the need for the public to know that a security inspection activity occurred, while overall licensee performance information and any details associated with NRC security oversight activities that could be useful to an adversary is withheld.

Option 2

First, this option has several aspects. The staff proposes to provide additional detail in the Annual Security Report to Congress. Most notably, the staff proposes to provide additional

information such as the sites that had security findings, the attribute[2] the finding was associated with, and the significance level.[3] Furthermore, the staff proposes to list licensees' greater-than-Green findings in the columns of the security action matrix and describe any findings that have resulted in previous NRC public discussion. For the case of previous NRC public discussion or public involvement, the staff uses inattentive security officers as an example that may warrant further annual report discussion.

For security inspection report cover letters, the staff proposes to provide information related to the fact that a security finding(s) was identified, the key attribute the finding(s) was related to, whether the inspection was an FOF exercise, and the "color" (significance) of the finding(s).

The staff also proposes that this option be applied where applicable and appropriate to other NRC security inspection/oversight programs, including, but not limited to fuel cycle facilities, research and test reactors, independent spent fuel storage facilities, and reactors under construction. However, there still remains the need to withhold certain information from public review, such as that for certain Category I fuel facilities and material licensees. For the materials oversight program, there remains the need to withhold certain information from public review, such as information that would identify both NRC and Agreement State licensees that possess radioactive materials in quantities of concern.[4] For commercial power reactors, since Option 2 informs the public of any significant inspection findings, this information will be included in a publicly-available security action matrix table on the NRC's external ROP website, similar to that done for the other six cornerstones.

Option 2 also enhances the level of transparency associated with the security PI and the security SDP. The staff notes that specific information regarding how the security PI is measured and calculated is publicly available. Furthermore, site-specific PI information is historical and licensees are required to implement timely corrective actions if pre-established metrics are exceeded. Therefore, making site-specific PI performance trend information publicly available on the NRC's external website (as currently done for the safety PIs) is equivalent to the staff's proposal to enhance public information regarding security inspection findings and meets the Evaluation Criteria. This transparency will improve public understanding and confidence in NRC's ability to consistently, predictably, and effectively regulate the safe and secure commercial use of radioactive materials.

Option 2 also improves staff efficiency in implementing the ROP while improving security openness and transparency. The staff proposes to re-combine the safety and security SAs and to recombine the safety and security ROP mid-cycle and end-of-cycle NRC assessment letters and public meetings of licensee performance. The security SA, assessment letters, and licensee performance meetings are currently independent of the assessments, letters and meetings conducted for the other six ROP cornerstones. These security activities were

---

[2] The five "key attributes" described in NRC Inspection Manual Chapter 0320, "Operating Reactor Assessment Program," are Physical Protection System, Access Authorization, Access Control, Response to Contingency Events, and Material Control and Accounting.

[3] The significance level of a finding is illustrated by its color: Green – very low security significance; White – low to moderate security significance; Yellow – moderate to high (i.e., substantial) security significance; and, Red – high security significance.

[4] Staff initiatives are ongoing to develop a Commission paper addressing the public release of information regarding high risk sources of Category 1 and 2 radioactive source materials licensees.

separated to help ensure effective information control of sensitive security information. The staff has found, however, that little benefit has resulted from this independence when compared to the staff effort needed to conduct these three oversight activities separately. In addition, withholding this particular information from the public precluded effective public involvement in the security oversight process. Should there be the need to communicate sensitive security information, a controlled non-public attachment can be issued with the licensee performance letters and a breakout session or separate non-public meeting can be held.

Option 3

For Option 3, the staff proposes to fully integrate the security cornerstone with that of the other six ROP cornerstones and to make the security portion of the ROP publicly available. This would include, in part, implementation of Option 2 activities and the full integration of IMC 0320, "Operating Reactor Security Oversight Process," into IMC 0305, "Operating Reactor Assessment Process." This comprehensive program change would restore the ROP to a pre-9/11 status and would make the security oversight process, redacted non-SGI portion of inspection reports, security inspection procedures and reports publicly available. The primary benefits would be to (1) combine safety and security action matrices into a single action matrix of commercial power reactor performance, and (2) increase openness through the public availability of redacted security inspection reports and procedures. The staff notes that Option 3 would result in only a marginal improvement in openness and transparency over Option 2 because IMC 0320 is already publicly available and security sensitive details associated with the security SDP assessment, inspection procedures, and inspection reports would still be withheld from public disclosure and issued separately. Significant staff effort would be necessary to redact the security inspection procedures and reports. Furthermore, significant coordination and communication with public and industry stakeholders, as well as NRC's Federal and State security partners, will be necessary prior to initiating these changes.

RECOMMENDATION:

The staff recommends Option 2 because it meets the staff's Evaluation Criteria and represents a cautious and comprehensive enhancement to the current level of openness and transparency applied to security-related NRC inspection results and assessment of licensee security performance that can be timely and effectively implemented. Application of Option 2 to other NRC security oversight programs, where applicable and appropriate, will help improve agency-wide consistency and public confidence in NRC's ability to consistently, predictably, and effectively regulate the secure commercial use of radioactive materials. This option better communicates a timely and integrated NRC assessment of commercial power reactor and other licensee performance and will also help improve staff efficiency by reducing redundant staff activities. This option also allows a measured, incremental step to increase openness that the staff can assess to understand the effectiveness. A longer range goal of moving toward Option 3, to reintegrate security completely back into the safety ROP will be implemented in a phased approach. Sufficient resources will be identified through the Planning, Budgeting, and Performance Management process to accomplish this objective.

Overall, the staff continues to look at the entire suite of activities in the security area to identify areas where the Agency can be more open and transparent, and will continue to keep the Commission apprised of any other planned changes in this area.

RESOURCES:

Option 1, *status quo*, can be accomplished within existing budgeted resources for Fiscal Year (FY) 2009.

For Option 2, the staff estimates that the recommendations can be accomplished within existing budgeted resources for FY 2009 and beyond.

For Option 3, the staff estimates a total of 3.1 FTE (1.0 Office of Nuclear Security and Incident Response, 1.0 Office of Nuclear Reactor Regulation, 0.2 Office of Nuclear Material Safety and Safeguards, 0.1 Office of Federal and State Materials and Environmental, and 0.2 for each Region) will be necessary to implement this option's activities for FY 2011. In addition, the staff estimates 3.2 FTE (0.8 FTE per Region per year) to redact future security inspection reports. If Option 3 is selected, these resources will be addressed through the Planning, Budgeting, and Performance Management process of FY 2012 and beyond.

COORDINATION:

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

/RA Martin Virgilio for/

R. W. Borchardt
Executive Director
for Operations

RESOURCES:

Option 1, *status quo*, can be accomplished within existing budgeted resources for Fiscal Year (FY) 2009.

For Option 2, the staff estimates that the recommendations can be accomplished within existing budgeted resources for FY 2009 and beyond.

For Option 3, the staff estimates a total of 3.1 FTE (1.0 Office of Nuclear Security and Incident Response, 1.0 Office of Nuclear Reactor Regulation, 0.2 Office of Nuclear Material Safety and Safeguards, 0.1 Office of Federal and State Materials and Environmental, and 0.2 for each Region) will be necessary to implement this option's activities for FY 2011. In addition, the staff estimates 3.2 FTE (0.8 FTE per Region per year) to redact future security inspection reports. If Option 3 is selected, these resources will be addressed through the Planning, Budgeting, and Performance Management process of FY 2012 and beyond.

COORDINATION:

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

/RA Martin Virgilio for/

R. W. Borchardt
Executive Director
for Operations

DISTRIBUTION:

NSIR/DSO	Regions	NRR/ADRO	NRO/DCIP	NMSS/FCSS
NMSS/SFST	NMSS/SFST	FSME/DMSSA	OE	OPA
RidsNsirMailCenter	RidsEdoMailCenter (W200700407, W200800209, W200800210)			

ADAMS ACCESSION NO.: ML082810156

OFC	NSIR:SPM	QTE	NSIR:BC	NSIR:DSO/DD	NSIR/DSO:D	OGC
NAME	PHarris	KAzariak-Kribbs	GWest	BWestreich	THolahan	JGoldberg
DATE	10/24/08	10/22/08	10/17/08	10/18/08	10/24/08	10/21/08

OFC	NSIR/DSP	NRR/ADRO/DIRS:D	FSME:OD	NMSS:OD	OE:OD
NAME	RCorreia	FBrown for ELeeds	RLewis for CMiller	MWeber	CCarpenter
DATE	10/24/08	10/23/08	10/23/08	10/27/08	10/24/08

OFC	Rgn I/DIRS:D	Rgn II/DRS:D	RGN III/DRS:D	RGN IV/DRS/D	OPA
NAME	MGamberoni	ABoland	RCroteau for SWest	RCaniano	BHayden for EBrenner
DATE	10/23/08	10/23/08	10/23/08	10/23/08	10/23/08

OFC	NSIR/PMDA	OCFO:OD	NSIR:OD	EDO
NAME	SAbraham for VHuth	RMitchell for JDyer	RZimmerman	RBorchardt (MVirgilio for)
DATE	10/24/08	10/29/08	10/31/08	11/24/08

OFFICIAL RECORD COPY