



Union of Concerned Scientists

Citizens and Scientists for Environmental Solutions

2008 SEP -5 PM 2:57

RECEIVED

September 5, 2008

Michael T. Lesar, Chief
Rulemaking, Directives and Editing Branch
Office of Administration (Mail Stop: T6-D59)
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

4/29/08
70 FR 43960
4

Re: COMMENTS ON NRC-2008-0413, POSSIBLE IMPROVEMENTS TO THE LEVEL OF OPENNESS AND TRANSPARENCY OF INFORMATION ASSOCIATED WITH NRC SECURITY INSPECTION AND SECURITY ASSESSMENT OF NRC LICENSEES

Dear Mr. Lesar:

On behalf of the Union of Concerned Scientists (UCS), we submit the attached comments in response to the July 22, 2008, *Federal Register* notice.

29

Sincerely,

David Lochbaum
Director, Nuclear Safety Project

Edwin S. Lyman, Ph.D.
Senior Staff Scientist

Attachments:

- 1) Performance Indicator Summary from 2nd Quarter of 2002
- 2) NRC Inspection Finding Summary from 3rd Quarter of 2002

SONSI Review Complete
Template = ADM-013

E-RIDS = ADM-03
Call = P. Harris (PWH)

**ATTACHMENT: UCS COMMENTS ON POSSIBLE IMPROVEMENTS TO THE
LEVEL OF OPENNESS AND TRANSPARENCY OF INFORMATION
ASSOCIATED WITH NRC SECURITY INSPECTION AND ASSESSMENT**

UCS prefaces our comments with the explicit statement that we fully realize that 9/11 changed things in America such that the NRC had to re-draw the line for publicly releasing information on nuclear plant security issues. UCS accepts that less security information is available today as a result. However, the public must have the same rights and opportunities to engage the NRC on security issues up to the re-drawn line as it had prior to 9/11.

After 9/11, the NRC not only re-drew the line but also re-crafted its rules of engagement with the American public on security policy making. Essentially, the NRC's post 9/11 rules of engagement preclude the public from meaningful input, and severely limit the public's access to output from the NRC's security policy decision-making.

It is not only possible but essential to responsibly discuss nuclear plant security policy in public. That fact has been demonstrated repeatedly since 9/11 by open Congressional hearings, many broadcast far and wide by C-SPAN. UCS's experts have testified at open, public Congressional hearings as have representatives of other public interest groups. Yet the NRC has resisted repeated attempts by UCS to engage the agency in responsible, productive dialogues like those conducted with the Congress. Like Congress has done, the NRC must engage public stakeholders about nuclear plant security policy issues in enough detail so that the public can make informed judgments on the adequacy of NRC's post-9/11 security measures. We are convinced that this can be achieved without disclosing information that would aid terrorists in carrying out attacks against nuclear facilities.

Topic: Annual Report to Congress

Number Comment

AR-1 Table 2 in the NRC's Annual Report for Calendar Year 2007 (NUREG-1885, Rev. 1) summarizes the force-on-force inspection program results for FYs 2005, 2006, and 2007. Because the NRC's oversight program for security currently spans a three-year period, this contextual format should be retained in future annual reports.

AR-2 In the NRC's Annual Report for Calendar Year 2007 (NUREG-1885, Rev. 1), the NRC provided information on force-on-force inspection program results, performance indicator results, and NRC inspection findings for the past three years. In addition to these cumulative totals, the NRC should provide yearly totals to communicate performance trends.

For example, the Table 2 reported 10 inspection findings from the 66 force-on-force inspections conducted during the prior three years. Two entirely different pictures form if 6 of those inspection findings occurred in year 1, 3 in year 2, and 1 in year 3 than if 1 inspection finding occurred in year 1, 3 in year 2, and 6 in year 3.

Public disclosure of a declining performance trend, even one more pronounced than in the hypothetical example above, would not provide useful information to potential enemies because (a) inspection findings reflect past weaknesses now identified and corrected, and (b) the industry-wide trend does not specifically reveal who is having what problems.

**ATTACHMENT: UCS COMMENTS ON POSSIBLE IMPROVEMENTS TO THE
LEVEL OF OPENNESS AND TRANSPARENCY OF INFORMATION
ASSOCIATED WITH NRC SECURITY INSPECTION AND ASSESSMENT**

Topic: Annual Report to Congress

Number Comment

AR-3 As of September 4, 2008, the NRC's website had the annual report for 2006 posted (NUREG-1885, <http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1885/>) but did not have the most recent annual report (NUREG-1885, Rev. 1, dated July 2008) posted. The annual reports should be posted to the NRC's website within a few days after being submitted to Congress.

On a related note, the annual report on security was posted on the NRC's webpage of "Publications Prepared by NRC Staff" (<http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/>) but not on the "Security Spotlight" webpage (<http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/security-spotlight/index.html>), the "Nuclear Reactor Quick Links" webpage (<http://www.nrc.gov/reactors/ql-reactors.html>), the "Reactor Oversight Process" webpage (<http://www.nrc.gov/NRR/OVERSIGHT/ASSESS/index.html>) or any other webpage. The NRC should add links to the annual report from several of its webpage.

Topic: Reactor Oversight Process

Number Comment

ROP-1 During development of the reactor oversight process (ROP) circa 1999, considerable discussion probed whether the inclusion of security-related performance indicators and inspection findings could provide too much information to those seeking to cause radiological sabotage at nuclear power plants. While such potential existed, it was determined that the specific performance indicators and the limited inspection finding narratives posed no undue risk.

After the NRC's website, including the ROP webpages, were removed from the internet in October 2002, the NRC staff revisited this ground and re-confirmed that the security-related performance indicator and inspection finding information did not provide potential enemies with undue insights of weaknesses and vulnerabilities. The security components of the ROP were restored to the internet after this post 9/11 screening.

In August 2004, the Commission directed its staff to remove the security-related information from the NRC's website. It was not clear then and remains unclear today why the Commission overturned earlier decisions and mandated the security "blackout" for ROP. The Commission did it as a *fait accompli*, with no publicly disseminated explanation of what new factors or reconsidered old factors caused this radical change.

The Commission never publicly articulated its reasons for removing security information from the public arena in August 2004. The most likely reason is the pending resumption of force-on-force security testing. The NRC suspended force-on-force testing of nuclear plant security after 9/11 and resumed full-scale force-on-force testing in November 2004 (see <http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/force-on-force.html> for details). It was well-known prior to 9/11 that a high percentage of force-on-force tests resulted in the mock intruders completely destroying the target set of equipment needed

**ATTACHMENT: UCS COMMENTS ON POSSIBLE IMPROVEMENTS TO THE
LEVEL OF OPENNESS AND TRANSPARENCY OF INFORMATION
ASSOCIATED WITH NRC SECURITY INSPECTION AND ASSESSMENT**

Topic: Reactor Oversight Process

Number Comment

to prevent reactor core meltdown. It seems likely that the Commissioners did not want to risk the “bad press” associated with continuation of this poor performance after 9/11, so they mandated a security information “blackout” to hedge their bets.

Now that a full cycle of force-on-force tests using the post 9/11 methods have been completed, the Commission’s “bad press” concerns have been put to bed. Even this illegitimate reason for with-holding security information from the public is gone, so the NRC must restore security information to its ROP.

ROP-2 UCS was heavily engaged with the NRC staff and other stakeholders during the development and pilot testing of the ROP. One of most commendable attributes of the ROP, which we have often pointed out publicly, is that the ROP was intentionally designed to be a constant “work-in-progress.” Features such as the formal annual self-assessments and monthly ROP public meetings seek to ensure that the ROP’s structure and implementation are meeting expectations, and if not, to permit mid-course corrections.

A byproduct of the Commission’s August 2004 mandate to its staff removing security-related ROP information from the website has been to bar public participation in discussions about the efficacy of security-related performance indicators and inspection procedures. Prior to 9/11, UCS’s David Lochbaum and Ed Lyman (then working for the Nuclear Control Institute) regularly participated in public meetings on security issues conducted by the NRC on a nearly monthly basis. Those meetings produced SECY-01-0100 and SECY-01-0101, both dated June 4, 2001.

Due to the Commission’s decision, the public has been unable to participate in ROP discussions of security matters. Since 9/11, the public’s participation in ROP discussions such as those on safety culture have, in our opinion, resulted in tangible, positive improvements. It is also our opinion that the public’s participation in ROP discussions would have yielded similar positive outcomes on security issues.

ROP-3 The removal of security-related information from the publicly available ROP webpages impaired NRC’s ability to enforce security regulations. The ROP is essentially a publicly available report card on licensee performance prowess. Licensees with all green performance indicators and no/no greater-than-green inspection findings are perceived as being better performers. Wall Street, for example, takes note and has been known to lower company projections based on worsening ROP indications. This public spotlight on the safety side is an invaluable albeit intangible aid to licensees avoiding greater-than-green outcomes and to recover from greater-than-green outcomes as rapidly as possible when they occur.

The ROP blackout on security-related performance indicator and inspection findings aids and abets poor performing licensees by shielding their performance problems from Wall Street and others. The NRC must restore security-related information to the ROP to undue this self-inflicted impairment.

**ATTACHMENT: UCS COMMENTS ON POSSIBLE IMPROVEMENTS TO THE
LEVEL OF OPENNESS AND TRANSPARENCY OF INFORMATION
ASSOCIATED WITH NRC SECURITY INSPECTION AND ASSESSMENT**

Topic: Reactor Oversight Process

Number Comment

ROP-4 The NRC's procedure for determining the significance (i.e., color) of NRC inspection findings involving security should be made publicly available to provide the needed context for greater-than-green findings. This information does not provide potential bad guys with site-specific information they would need to increase the chances of a successful attack.

Providing this information to the public allows external stakeholders to better understand the proper context of security problems. This increased awareness facilitates acceptance by external stakeholders that the majority of NRC's inspection findings (green) did not represent serious vulnerabilities because of the defense-in-depth features that overlap with or backup the specific problem areas.

Topic: Security-related Docketed Correspondence

Number Comment

DC-1 In December 2007, the NRC issued Bulletin 2007-01 to licensees requesting responses to five questions about security officer attentiveness. The licensees' docketed responses varied from complete public availability of all information (Exelon – ML080430467 and Fermi 2 – ML080460551) to partial availability of some information (Callaway – ML080510628 and South Texas Project – ML080460553) to availability of only the transmittal letter (Vermont Yankee – ML080500263 and Indian Point – ML080510585) to not even the transmittal letter being publicly available (TVA).

It's virtually impossible for any reasonable person to believe that Exelon's completely public response and TVA's completely hidden response to the same five publicly available NRC questions about security officer attentiveness can be right. Either Exelon divulged sensitive information with their response or TVA withheld non-sensitive information with their response. Of course, another option has TVA placing something like "N" (where N is the not-so-secret number of attackers in the updated DBT) on top of every page so every page could be considered sensitive.

DC-2 Using the lessons learned from the Bulletin 2007-01 responses, in the future when the NRC issues publicly available docketed correspondence to licensees (Bulletin 2007-01 is available online at http://adamswebsearch2.nrc.gov/idmws/doccontent.dll?library=PU_ADAMS^PBNTAD01&ID=073470209) that requires docketed responses from those licensees, the NRC should:

- 1) Provide clear guidance on the agency's expectations for public availability of the responses.
- 2) Require, as a minimum, that the licensees' transmittal letters be publicly available.

When the NRC sends non-public communications to licenses, like security advisories, it

**ATTACHMENT: UCS COMMENTS ON POSSIBLE IMPROVEMENTS TO THE
LEVEL OF OPENNESS AND TRANSPARENCY OF INFORMATION
ASSOCIATED WITH NRC SECURITY INSPECTION AND ASSESSMENT**

Topic: Security-related Docketed Correspondence

Number Comment

is appropriate for any licensee responses to also be non-public.

But when the NRC publicly releases questions/concerns about security, it seems entirely appropriate that, to the maximum extent possible, NRC-requested responses also be publicly available.

Topic: Security Rulemaking and Policy Decision-Making

Number Comment

RM-1 Just as the US Congress has conducted numerous open, public hearings on post 9/11 nuclear plant security issues, the NRC could and should do so, too. There's no legitimate reason for Commission briefings not to be open, public meetings including public interest group representatives at the table. Likewise, there's no legitimate reason for NRC staff meetings with industry on security policy issues not to be open, public meetings.

This does not suggest or mean that every minute of every NRC briefing/meeting on security needs to be conducted in an open, public manner. Some of the hearings conducted by the US Congress had closed portions. NRC could close a portion of a briefing/meeting or pair a closed briefing/meeting with an open one.

The point is that the public has an interest in security policies and the NRC must provide a suitable way for the public to provide input into NRC's decision-making processes.

RM-2 The NRC should charter a panel under the Federal Advisory Committee Act (FACA) with at least one public interest group representative on it to monitor the agency's openness and transparency efforts related to security issues. This FACA panel should be tasked with reviewing publicly and non-publicly available documents and issuing periodic reports on how well the NRC is achieving its openness and transparency goals.

For example, the FACA panel could review the force-on-force inspection reports that are described, in rollup fashion, in the annual report to Congress. Similar to how the Advisory Committee on Reactor Safeguards issues letters to the Commission regarding its reviews, the FACA panel could issue a letter on its review that could then be included with the annual report.

The goal of this FACA panel would be twofold: (1) to help the NRC meet its openness and transparency goals, and (2) to help convince external stakeholders that the goals have been met.

Because the NRC has many external stakeholders, the FACA panel membership should include as a minimum a public interest group representative, a representative of State government, a reporter, a staff member of the US Congress, a representative of the nuclear industry. Appointment to the FACA panel should be conditional on having or being able to obtain a clearance for safeguards / sensitive information. The members of

**ATTACHMENT: UCS COMMENTS ON POSSIBLE IMPROVEMENTS TO THE
LEVEL OF OPENNESS AND TRANSPARENCY OF INFORMATION
ASSOCIATED WITH NRC SECURITY INSPECTION AND ASSESSMENT**

Topic: Security Rulemaking and Policy Decision-Making

- | Number | Comment |
|--------|--|
| | <p>the FACA panel would then review selected information – such as the non-public annual report submitted to Congress and its publicly available counterpart – to verify that the information being with-held is done so for appropriate reasons and the information being publicly released fairly characterizes the situation.</p> <p>This FACA panel need not and should not be a permanent one. A fairly short duration of around three years should be sufficient to demonstrate the NRC’s security information openness and transparency efforts have met their stated objectives.</p> |
| RM-3 | <p>Despite the NRC’s blackout on security-related information and its erection of many unnecessary barriers to meaningful public participation, the public still managed to provide substantive constructive input to the NRC security rulemaking and policy decision-making processes. For example, the September 2002 report <i>Nuclear Power Plant Security: Voices from Inside the Fences</i> was a major factor in the fitness-for-duty and training enhancements orders issued by the NRC in April 2003 to its power reactor licensees. And the April 2003 petition for rulemaking submitted by the Union of Concerned Scientists and the Mothers For Peace of San Luis Obispo was a major factor in the security/safety interface section of the 2007 final security rule adopted by the NRC.</p> <p>It’s both scary and disheartening to think about how many other security gains were lost because the NRC’s post 9/11 antics prohibited meaningful public participation from its processes.</p> |

Topic: NRC’s Specific Questions

- | Number | Comment |
|--------|---|
| NRC-1 | <p><i>Q - In addition to the information currently in publicly-available cover letters for the majority of NRC security inspections, what additional information would be effective in informing the public about licensee security performance? For example, what specific details would increase the public’s level of satisfaction in NRC regulatory oversight of licensed facilities?</i></p> <p>Security-related performance indicator and inspection finding information must be fully restored to the ROP.</p> <p>The NRC does not primarily rely on publicly-available reports of NRC safety inspections to communicate to the public about licensee safety performance. The ROP’s Action Matrix conveys the NRC’s overall assessment of individual licensee performance. The NRC’s quarterly performance summaries (such as http://www.nrc.gov/NRR/OVERSIGHT/ASSESS/BRAI1/brai1_chart.html for Braidwood Unit 1) communicate plant-specific assessments of licensee performance in the cornerstone areas based on results from performance indicators and inspection findings. Probing details about a specific inspection finding will direct the public to an NRC inspection report about safety, but the inspection reports are not the prime means of communicating to the public</p> |

**ATTACHMENT: UCS COMMENTS ON POSSIBLE IMPROVEMENTS TO THE
LEVEL OF OPENNESS AND TRANSPARENCY OF INFORMATION
ASSOCIATED WITH NRC SECURITY INSPECTION AND ASSESSMENT**

Topic: NRC's Specific Questions

Number Comment
 about safety performance.

Neither should publicly-available cover sheets of NRC security inspections be agency's primary method of communicating to the public about security performance. The ROP was intentionally and deliberately developed to be the agency's means of assessing performance and communicating its assessments to external stakeholders. The NRC must restore security-related performance indicators and inspection findings to the ROP so the public can learn about safety and security performance.

The ROP was designed to integrate safety and security performance. After 9/11, the Commission opted to segregate security performance information from the ROP's safety performance reporting. It is unproductive and wrong to now attempt to design a separate but equal way of communicating security performance information to the American public. The NRC must instead re-integrate security performance information into the ROP.

Attachment 1 provides the ROP's summary of safety and security performance indicators for the 2nd quarter of 2002. The three security (or physical protection, PP) performance indicators are in the three rightmost columns. The 15 safety performance indicators are to the left. This post 9/11 performance snapshot showed most reactors doing well (green) in both safety and security areas. The Kewaunee and Quad Cities Unit 1 reactors were shown to have had safety issues rising to the yellow category and the LaSalle Units 1 and 2 reactors having a security issue rising to the white level. As intended when it was designed, this ROP communication tool provided licensees and other external stakeholders with performance assessment information in context, without providing security vulnerability information to those wishing us harm.

Likewise, attachment 2 provides the ROP's summary of safety and security NRC inspection findings for the 3rd quarter of 2002. The single security (i.e., physical protection) cornerstone is the rightmost column while the six safety cornerstones are to the left. As with the performance indicator results, these NRC inspection findings showed most reactors having no identified problems or identified problems of low safety significance (green). The Point Beach Units 1 and 2 reactors had NRC inspection findings in the mitigating systems cornerstone of the most serious level (red) while the Indian Point Unit 2 reactor had an NRC inspection finding in the same cornerstone of the second most serious level (yellow). The Vermont Yankee reactor was shown to have a serious (yellow) NRC inspection finding in security. The details on this yellow finding that existed in the ROP in 2002 (and remains today in the ROP's online archives) stated:

**ATTACHMENT: UCS COMMENTS ON POSSIBLE IMPROVEMENTS TO THE
LEVEL OF OPENNESS AND TRANSPARENCY OF INFORMATION
ASSOCIATED WITH NRC SECURITY INSPECTION AND ASSESSMENT**

Topic: NRC's Specific Questions

Number Comment

Physical Protection

Significance: Y Nov 28, 2001

Identified By: NRC

Item Type: FIN Finding

Operational Safeguards Response Evaluation (OSRE) Force-On-Force Exercise Results

On August 23, 2001, the NRC completed an Operational Safeguards Response Evaluation (OSRE) at the Vermont Yankee power reactor facility. The evaluation consisted of a selective examination of physical security plans, procedures and representative records; review and walkdown of selective portions of the Vermont Yankee facility; conduct of table-top exercises; examination and review of target sets; observations of force-on-force response exercises and exercise critiques; observation of firearms proficiency by security officers; and interviews with selected personnel. During the conduct of the force-on-force exercises, response strategy weaknesses were identified. This finding was determined to be a Yellow finding based on the Interim Physical Protection Significance Determination Process. Upon identification of the finding, VY established immediate compensatory measures. These were taken to assure the security program was adequate while necessary longer term corrective actions are implemented. Before leaving the site, the inspectors determined that the security program at Vermont Yankee was sound, an important step given the current threat environment. The maintenance of the completed compensatory measures were confirmed by a NRC Security Specialist on September 27, 2001 and October 16, 2001. In a letter dated November 21, 2001, Vermont Yankee confirmed its commitment to continue these actions, and the compensatory measures addressing the weaknesses revealed from the OSRE, pending the implementation of long-term corrective actions. The finding will continue to be considered in our assessment process until the appropriate supplemental inspection (95002), has been completed and we have determined that corrective actions relative to root cause and extent of condition are appropriate. As a result, the event date has been changed from September 26, 2001 (exit date) to November 28, 2001 (issued report date) to keep the finding active in our assessment process.

Inspection Report# : [2001010\(pdf\)](#)

Inspection Report# : [2003001\(pdf\)](#)

No reasonable person, and few unreasonable ones, would argue that this level of detailed security information was inappropriate in a post 9/11 environment. While the area of concern was identified (i.e., "response strategy weaknesses"), the precise nature was not revealed. And even if someone were able to guess the precise nature, that guess would be moot because, as the report stated, the "maintenance of the completed compensatory measures were confirmed by a NRC Security Specialist." Thus, while past performance problems were reported, no current security vulnerabilities were ever revealed.

The ROP was intentionally designed to provide the optimal communication of safety and security performance assessment results to the public. Restoration of security-related performance indicator and inspection finding information to the ROP would remove the current impairment to optimal communication.

NRC-2a *Q - At what stage in the inspection process is interaction with the public most effective and beneficial? For example, immediately upon closure of an inspection when a finding is identified, but may be withheld from public disclosure or some time after licensee correction of the finding, when it may be possible to release additional security-related inspection information?*

Security-related performance indicator and inspection finding information must be fully restored to the ROP.

The ROP defines when and how safety performance results are communicated to the public. The ROP can and should also define when and how security performance results are communicated.

**ATTACHMENT: UCS COMMENTS ON POSSIBLE IMPROVEMENTS TO THE
LEVEL OF OPENNESS AND TRANSPARENCY OF INFORMATION
ASSOCIATED WITH NRC SECURITY INSPECTION AND ASSESSMENT**

Topic: NRC's Specific Questions

Number	Comment
	<p>UCS does not understand why security findings could not be publicly disclosed as safety findings are disclosed. If an NRC inspection finds that a security widget is broken or that a security response procedure is defective, the licensee must immediately correct or compensate for that finding. Thus, there should be no identified, uncorrected, uncompensated security findings at any nuclear plant site. Any reluctance to publicly disseminate information about security findings compensated for but not yet corrected suggests that the NRC concedes that compensatory measures have little or no value and the only thing protecting the public from the serious security vulnerability is that potential bad guys are not aware of it.</p>
NRC-2b	<p><i>Q - At what stage in the NRC's licensee performance assessment process is interaction with the public most effective and beneficial? For example, upon NRC determination that licensee performance changed from one Action Matrix column to another or during NRC's mid-cycle or end-of-cycle licensee performance reviews.</i></p> <p>Security-related performance indicator and inspection finding information must be fully restored to the ROP.</p> <p>The ROP defines when and how safety performance results are communicated to the public. The ROP can and should also define when and how security performance results are communicated. Security-related performance indicators and inspection findings should reflect security problems in the next quarterly ROP update cycle after they have been corrected or adequately compensated for.</p> <p>If poor safety performance drives a reactor from one Action Matrix column to another, the ROP defines how that change is communicated to external stakeholders. This same process should be applied when poor security performance forces an Action Matrix column move.</p>
NRC-3	<p><i>Q - What method of public interaction is most preferred? For example, is the conduct of a public meeting, a redacted inspection report, additional information in NRC's annual report to Congress regarding security inspections, or additional information posted on the NRC Website the most beneficial (efficient, effective, or informative) method of informing the public?</i></p> <p>Security-related performance indicator and inspection finding information must be fully restored to the ROP.</p> <p>The ROP defines when and how safety performance results are communicated to the public. The ROP can and should also define when and how security performance results are communicated. The ROP is the proper tool for NRC to use in interacting with the public on safety and security issues.</p>

**ATTACHMENT: UCS COMMENTS ON POSSIBLE IMPROVEMENTS TO THE
LEVEL OF OPENNESS AND TRANSPARENCY OF INFORMATION
ASSOCIATED WITH NRC SECURITY INSPECTION AND ASSESSMENT**

Topic: NRC's Specific Questions

Number Comment

NRC-4 *Q - How useful are the above methods for communicating NRC security-related inspection and licensee performance information to all stakeholders?*

None are nearly as useful as fully restoring security-related performance indicator and inspection finding information to the ROP.

NRC-5 *Q - What are the reasons why various stakeholders desire security-related information? For example, is this information necessary to build confidence in NRC regulatory oversight or understand current licensee performance?*

The reasons various stakeholders desire security-related information are almost certainly identical to the various reasons stakeholders desire safety-related information.

People living near nuclear power reactors are as interested in knowing that a safely run reactor is properly secure as they are in knowing that a properly secure reactor is safely run.

Members of the financial community are as interested in knowing that management can successfully meet or exceed NRC's security requirements as they are in knowing that management meets or exceeds NRC's safety requirements.

Public oversight of security, to the extent possible, also serves the same function as public oversight of safety – to ensure that the NRC and the industry are fully accountable to the public.

NRC-6 *Q - What level of public participation in any substantial and future revision of the security oversight process (e.g., changes made to performance indicators, significance determination process, etc.) would be beneficial? What constraints and considerations on such participation would be necessary to protect the details of sensitive security information?*

After security-related performance indicator and inspection finding information are fully restored to the ROP, changes to performance indicators, significance determination process, etc. should include meaningful public participation just as changes to safety-focused performance indicators, significance determination processes, etc. are made. Specifically, meaningful public participation includes re-inclusion of security-related discussions in the open portions of public meetings such as those held on a monthly basis by the NRC staff with industry representatives on the ROP. Proposed changes to ROP procedures, questions about implementation of ROP procedures, and potentially unintended consequences from the ROP for safety issues are routinely and properly discussed in these meetings. Reintroduction of security-related information into the ROP should allow meaningful public participation in changes to the security portions of the ROP.

**ATTACHMENT: UCS COMMENTS ON POSSIBLE IMPROVEMENTS TO THE
LEVEL OF OPENNESS AND TRANSPARENCY OF INFORMATION
ASSOCIATED WITH NRC SECURITY INSPECTION AND ASSESSMENT**

Topic: NRC's Specific Questions

Number Comment

The exception involves an undue and unwarranted imposition on licensees. Licensees can cite actual plant events as the bases for requesting changes to the ROP. For example, the monthly public meetings between NRC and licensees include discussions of frequently asked questions (FAQs). The typical FAQ recounts an actual event at a site and proposes to the NRC staff how it should be handled for the applicable performance indicator. The industry should retain the FAQ process for security-related performance indicators, but those discussions cannot effectively be conducted in public. The ROP meetings should be configured to discuss safety-related FAQs and policy-level questions about security-related performance indicators during open, public portions and then to close the meeting so only those participants with the need-to-know discuss security-related FAQs.

Attachment 1

Three Mile Island 1	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G
Turkey Point 3	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G
Turkey Point 4	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G
Vermont Yankee	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G
Vogtle 1	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G
Vogtle 2	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G
Waterford 3	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G
Watts Bar 1	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G
Wolf Creek 1	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G

Legend: R=Red W=White T=Thresholds under development N=Not Applicable
 Y=Yellow G=Green I=Insufficient data to calculate PI U=Unique Design

- | | |
|---|--|
| IE01 = Unplanned Scrams per 7000 Critical Hours | IE02 = Scrams with Loss of Normal Heat Removal |
| IE03 = Unplanned Power Changes | MS01 = Emergency RC Power System |
| MS02 = High Pressure Injection System | MS03 = Heat Removal System |
| MS04 = Residual Heat Removal System | MS05 = Safety System Functional Failures |
| BI01 = Reactor Coolant System Specific Activity | BI02 = Reactor Coolant System Leakage |
| EP01 = Drill/Exercise Performance | EP02 = ERO Drill Participation |
| EP03 = Alert and Notification System | OR01 = Occupational Exposure Control Effectiveness |
| PR01 = RETS/ODCM Radiological Effluent | PP01 = Protected Area Equipment |
| PP02 = Personnel Screening Program | PP03 = FFD/Personnel Reliability Program |

Attachment 2

3Q/2002 ROP Inspection Findings Summary

Note: This summary provides the color designation of the most significant inspection findings over the previous 4 quarters

Plants	Initiating Events	Mitigating Systems	Barrier Integrity	Emergency Preparedness	Occupational Radiation Safety	Public Radiation Safety	Physical Protection
Arkansas Nuclear 1	No Findings	Green	No Findings	No Findings	No Findings	Green	No Findings
Arkansas Nuclear 2	Green	Green	No Findings	No Findings	Green	Green	No Findings
Beaver Valley 1	Green	Green	No Findings	White (1)	No Findings	No Findings	No Findings
Beaver Valley 2	Green	Green	No Findings	White (1)	No Findings	No Findings	No Findings
Braidwood 1	Green	White (1)	Green	No Findings	Green	No Findings	No Findings
Braidwood 2	Green	Green	Green	No Findings	Green	No Findings	No Findings
Browns Ferry 2	Green	No Findings	Green	No Findings	Green	Green	No Findings
Browns Ferry 3	Green	Green	Green	No Findings	Green	No Findings	Green
Brunswick 1	No Findings	Green	No Findings	No Findings	Green	No Findings	No Findings
Brunswick 2	No Findings	Green	No Findings	No Findings	No Findings	No Findings	No Findings
Byron 1	No Findings	Green	Green	No Findings	No Findings	No Findings	No Findings
Byron 2	No Findings	Green	Green	No Findings	No Findings	No Findings	No Findings
Callaway	No Findings	White (1)	No Findings	No Findings	No Findings	Green	No Findings
Calvert Cliffs 1	No Findings	Green	Green	White (1)	Green	White (1)	No Findings
Calvert Cliffs 2	No Findings	Green	Green	White (1)	Green	White (1)	No Findings
Catawba 1	Green	Green	Green	No Findings	No Findings	No Findings	No Findings
Catawba 2	No Findings	Green	Green	No Findings	No Findings	No Findings	No Findings
Clinton	Green	Green	Green	No Findings	Green	No Findings	No Findings
Columbia Generating Station	No Findings	White (1)	No Findings	No Findings	Green	No Findings	Green
Comanche Peak 1	No Findings	Green	No Findings	No Findings	Green	White (1)	No Findings
Comanche Peak 2	No Findings	Green	No Findings	No Findings	Green	White (1)	Green
Cooper	Green	White (1)	Green	White (3)	Green	Green	Green
Crystal River 3	Green	Green	No Findings	No Findings	No Findings	No Findings	No Findings
D.C. Cook 1	Green	White (1)	Green	No Findings	Green	Green	No Findings
D.C. Cook 2	Green	White (2)	Green	No Findings	No Findings	Green	No Findings
Davis-Besse	No Findings	Green	No Findings	No Findings	Green	Green	No Findings
Diablo Canyon 1	Green	Green	No Findings	No Findings	Green	No Findings	No Findings
Diablo Canyon 2	Green	Green	No Findings	No Findings	Green	No Findings	No Findings
Dresden 2	Green	Green	No Findings	Green	Green	Green	Green
Dresden 3	Green	Green	No Findings	Green	Green	Green	Green
Duane Arnold	No Findings	Green	No Findings	No Findings	No Findings	No Findings	No Findings
Farley 1	Green	Green	No Findings	No Findings	No Findings	No Findings	Green
Farley 2							

	No Findings	Green	No Findings	No Findings	No Findings	No Findings	Green
Fermi 2	No Findings	Green	Green	No Findings	No Findings	No Findings	No Findings
FitzPatrick	Green	Green	Green	No Findings	No Findings	Green	No Findings
Fort Calhoun	No Findings	Green	No Findings	No Findings	Green	White (1)	No Findings
Ginna	No Findings	Green	Green	White (1)	No Colors	No Colors	No Findings
Grand Gulf 1	Green	Green	Green	No Findings	No Findings	No Findings	No Findings
Harris 1	No Findings	White (3)	No Findings	No Findings	No Findings	Green	No Findings
Hatch 1	Green	Green	No Findings	No Findings	Green	Green	No Findings
Hatch 2	Green	Green	No Findings	No Findings	Green	Green	No Findings
Hope Creek 1	Green	Green	Green	No Findings	Green	No Findings	No Findings
Indian Point 2	Green	Yellow (1)	Green	Green	No Findings	No Findings	Green
Indian Point 3	No Findings	Green	No Findings	Green	No Findings	No Findings	No Findings
Kewaunee	No Findings	Green	No Findings	Green	Green	No Findings	No Findings
La Salle 1	No Colors	Green	Green	No Findings	Green	Green	No Findings
La Salle 2	No Colors	Green	Green	No Findings	Green	Green	No Findings
Limerick 1	Green	Green	No Findings	No Findings	No Findings	Green	No Findings
Limerick 2	Green	Green	White (1)	No Findings	No Findings	Green	No Findings
McGuire 1	Green	Green	No Findings	No Findings	Green	No Findings	No Findings
McGuire 2	Green	Green	No Findings	No Findings	Green	No Findings	No Findings
Millstone 2	No Findings	Green	No Findings	No Findings	No Findings	No Colors	No Findings
Millstone 3	No Findings	Green	Green	No Findings	No Findings	No Findings	No Findings
Monticello	No Findings	Green	Green	No Findings	Green	No Findings	No Findings
Nine Mile Point 1	Green	Green	No Findings				
Nine Mile Point 2	Green	Green	No Findings	No Findings	No Colors	No Findings	No Findings
North Anna 1	No Findings						
North Anna 2	No Findings						
Oyster Creek	No Findings	Green	No Findings				
Oconee 1	No Findings	White (1)	White (1)	No Findings	Green	No Findings	No Findings
Oconee 2	No Findings	Green	Green	No Findings	Green	No Findings	No Findings
Oconee 3	Green	Green	Green	No Findings	Green	No Findings	No Findings
Palisades	Green	Green	Green	No Findings	No Findings	No Findings	No Findings
Palo Verde 1	No Findings	No Findings	No Findings	Green	No Findings	No Findings	Green
Palo Verde 2	No Findings	No Findings	No Findings	Green	No Findings	No Findings	Green
Palo Verde 3	No Findings	Green	No Findings	Green	Green	No Findings	Green
Peach Bottom 2	Green	Green	Green	Green	Green	No Findings	No Findings
Peach Bottom 3	No Findings	Green	Green	Green	Green	No Findings	No Findings
Perry 1	Green	Green	Green	Green	No Findings	No Findings	No Findings

Pilgrim 1	No Findings	Green	No Findings	No Findings	No Colors	No Findings	No Findings
Point Beach 1	No Findings	Red (1)	No Findings	White (1)	No Findings	No Findings	No Findings
Point Beach 2	No Colors	Red (1)	No Findings	White (1)	No Findings	No Findings	No Findings
Prairie Island 1	Green	Green	No Findings				
Prairie Island 2	Green	Green	No Findings				
Quad Cities 1	Green	Green	No Findings				
Quad Cities 2	Green	Green	No Findings				
River Bend 1	No Findings	Green	No Findings	White (1)	Green	No Findings	No Findings
Robinson 2	No Findings						
Saint Lucie 1	No Findings	Green	No Findings	No Findings	No Findings	No Findings	Green
Saint Lucie 2	No Findings	Green					
Salem 1	Green	Green	No Findings	No Findings	No Findings	Green	No Findings
Salem 2	Green	Green	Green	No Findings	No Findings	Green	No Findings
San Onofre 2	Green	Green	No Findings	No Findings	Green	No Findings	Green
San Onofre 3	Green	Green	No Findings	No Findings	Green	No Findings	Green
Seabrook 1	Green	Green	No Findings	No Findings	No Findings	No Findings	Green
Sequoyah 1	Green	Green	Green	No Findings	Green	No Findings	No Findings
Sequoyah 2	Green	Green	Green	No Findings	Green	No Findings	No Findings
South Texas 1	Green	Green	Green	No Findings	Green	No Findings	No Findings
South Texas 2	Green	Green	Green	No Findings	Green	No Findings	No Findings
Summer	No Findings	Green	No Findings				
Surry 1	No Findings	Green	No Colors	No Findings	No Findings	No Findings	No Findings
Surry 2	No Findings	Green	No Findings				
Susquehanna 1	Green	Green	Green	Green	No Findings	No Findings	No Findings
Susquehanna 2	No Findings	Green	Green	Green	No Findings	No Findings	No Findings
Three Mile Island 1	Green	Green	No Findings				
Turkey Point 3	No Findings	Green	No Findings	No Findings	No Findings	No Findings	No Colors
Turkey Point 4	No Findings	Green	No Findings	No Findings	No Findings	No Findings	No Colors
Vermont Yankee	Green	Green	Green	No Findings	No Findings	No Findings	Yellow (1)
Vogtle 1	Green	Green	Green	No Findings	No Findings	No Findings	No Findings
Vogtle 2	Green	Green	No Findings				
Waterford 3	No Findings	Green	Green	No Findings	Green	No Findings	No Findings
Watts Bar 1	Green	Green	No Findings	No Findings	Green	No Findings	No Findings
Wolf Creek 1	No Findings	Green	Green	No Findings	No Findings	No Findings	No Findings

