July 20, 2007

The Honorable Bennie G. Thompson
Chairman, Committee on Homeland Security
United States House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

On behalf of the U.S. Nuclear Regulatory Commission (NRC), I am responding to your letter of May 15, 2007, regarding the cyber-security posture of the Nation's nuclear power plants. Your letter expressed concerns regarding several issues, including the adequacy of NRC regulations to impose adequate cyber-security protections.

The NRC is committed to ensuring the continued protection of the public health and safety, the environment, and the secure use and management of radioactive materials. Shortly after the events of September 11, 2001, the NRC issued a number of new security requirements that, in part, required power reactor operators to implement measures to enhance their cyber-security. Recently, the NRC completed a rulemaking to amend nuclear power plant security requirements to include a cyber attack as a threat attribute against which nuclear power plants must defend. In addition, the NRC is currently developing a final rule which will require all nuclear power plants to establish cyber-security programs to protect any system that could adversely impact safety, security, or emergency preparedness of a facility.

Your letter also raised several specific concerns, based on Information Notice 2007-15, regarding the effects of a malfunction of non-safety-related controls connected to an internal plant data network. On August 19, 2006, the Browns Ferry Nuclear Plant Unit 3 was manually shutdown from 40 percent power as a result of the unplanned loss of both recirculation pumps. The loss of the non-safety-related recirculation pumps was due to a control system failure. The plant is designed to ensure that reactor safety systems remain capable of addressing component failures regardless of the cause. For this event, despite the non-safety component failure, all safety-related systems performed as designed and the operator followed established procedures to safely shutdown the reactor.

The licensee determined that the cause of the event was a malfunction of the recirculation pump variable frequency drive (VFD) microprocessor-based controller. The controller failure was attributed to excessive traffic on the internal control network. Since the control network is physically and electrically independent of networks that interface outside the plant, the NRC is confident that the failure was not the result of a cyber attack. As stated in the Information Notice, the licensee subsequently installed firewalls to prevent similar control network traffic from affecting the VFD controller. The NRC determined that these actions are appropriate to ensure plant safety and consistent with the agency's policy and requirements for digital instrumentation and control (I&C) systems.

The NRC issued Information Notice 2007-15 to notify nuclear plant operators about the Browns Ferry incident. The NRC expects that licensees will examine the information for applicability at their facilities and consider actions, as appropriate, to avoid similar problems. Additionally, the NRC's Office of Nuclear Security and Incident Response has been coordinating with other Federal partners and several National Laboratories to examine existing cyber-security vulnerabilities, specifically in the digital I&C area. NRC also works in close collaboration with the Department of Homeland Security and other Federal agencies to identify any emerging cyber-security threats. Information on the nature of an emerging threat and appropriate mitigative measures is readily conveyed to any NRC licensees that may be vulnerable to such emerging threats. For additional information regarding digital I&C, refer to http://www.nrc.gov/about-nrc/regulatory/research/digital.html. Similar steps are being taken to incorporate the lessons learned from this event and rulemaking efforts into the licensing of the next generation of reactor designs.

More specific responses to your questions are provided in the enclosure. If you have further questions or would like to arrange a briefing, please contact me.

Sincerely,

/RA/

Dale E. Klein

Enclosure:
As stated

Identical letter sent to:

The Honorable Bennie G. Thompson
Chairman, Committee on Homeland Security
United States House of Representatives
Washington, D.C. 20515

The Honorable James R. Langevin
Chairman, Subcommittee on Emerging Threats,
Cybersecurity, and Science and Technology
Committee on Homeland Security
United States House of Representatives
Washington, D.C. 20515

NRC Response to May 15, 2007, Questions Regarding the Cyber-Security Posture of the Nation's Nuclear Power Plants

QUESTION 1: Has the NRC conclusively determined the source of the data storm described in Information Notice 2007-15?

RESPONSE: No. In this case, a review of plant data found that the safety systems functioned as designed, the cause identified was credible and was corrected, and no evidence of external influences was observed. The consideration of an external source for the failure was specifically reviewed. Based on the lack of remote access to the controllers, and the configuration and failure modes of the failed components, it was determined by the licensee and the NRC staff that the failure was not due to outside sources.

QUESTION 2: Does the NRC plan to exercise its authority under 10 C.F.R 50.65 to conduct an investigation of the incident at Browns Ferry?

RESPONSE: Yes. The NRC's "Maintenance Rule," 10 CFR 50.65, requires NRC nuclear power plant licensees to monitor the overall continuing effectiveness of their maintenance programs and take corrective action as necessary. The NRC routinely conducts inspections to verify that licensees comply with this rule. A detailed review of the August 2006 event at Browns Ferry was conducted by the NRC. After confirming that the reactor was shut down and that all safety systems performed as designed, the on-site NRC resident inspection staff provided details regarding plant status and performance of equipment and personnel to NRC management, event review staff, and risk analysts. These details were used to determine the level of agency response.

As part of the routine inspection program, the NRC will review and assess the adequacy of the licensee's corrective actions and provide a determination as to whether any additional NRC action for Browns Ferry is warranted.

QUESTION 3: In reviewing the incident, will the NRC determine what cyber-security policies and procedures the site followed, and what cyber-security assessments were performed?

RESPONSE: Yes. As part of the event follow-up, the NRC inspectors reviewed event assessments and corrective actions completed by the Browns Ferry staff to ensure that appropriate actions were taken consistent with NRC requirements and site procedures. The NRC's review of the August 2006 event found that the actions taken by Browns Ferry ensured that the safety and security of the facility were maintained.

Enclosure

QUESTION 4: How will future NRC regulations address the cyber-security interdependencies of non-safety and safety systems? What specific features will these systems contain?

RESPONSE: The NRC has already established a design requirement in 10 CFR Part 50 for safety systems to function in the event of a non-safety system failure. Section 50.55a(h) of 10 CFR requires that the safety system design shall be such that credible failures in, and consequential actions by, other systems shall not prevent the safety systems from performing their safety functions.

As stated previously, new security regulations in 10 CFR Part 73 will specifically identify cyber attack as a threat that must be protected against.

Lastly, plans are in place for NRC reviews of new reactor designs and safety systems to include security features against cyber threats, as well as physical threats.

QUESTION 5: Non-safety systems are not the only networked operations within a nuclear plant. As time passes, more and more safety systems will be networked and accessible online. How will future NRC regulations address the rise of networked safety systems?

RESPONSE: Regulations for new reactors and safety systems already exist and require that the safety system designs, which include safety-related networks, shall be such that credible failures in, and consequential actions by, other systems will not prevent them from performing their safety functions.

Our response to the previous question (Question 4) addresses the safety and security of networked safety systems. For deployment of digital systems in nuclear facilities (e.g., new reactors), upgrades to operating reactors and fuel cycle facilities, the NRC will evaluate these networked safety systems to determine whether they comply with the relevant regulations. This will include NRC requirements for the separation of safety and non-safety systems as well as the requirement that failure of other systems will not impair the ability of safety systems to perform their safety functions, as mentioned above.

Once the proposed rule for cyber-security requirements is published in final form and regulatory guidance has been issued, the NRC will incorporate the requirements into the baseline inspection program to help ensure that all nuclear power plants maintain adequate protection against external sources.

The current regulatory review plan for existing and future nuclear safety-related systems is to ensure that no modem or other means of connectivity provides access to safety systems via external networks.

QUESTION 6: How has the NRC reached out to the non-nuclear control system community to solicit feedback to the proposed rulemaking? What role have these experts played in assisting the NRC in developing regulations for nuclear plants?

RESPONSE: The NRC's Design Basis Threat rule (10 CFR 73.1), which requires power reactor licensees to be able to defend against a cyber attack with high assurance, was published for public comment in the *Federal Register* from November 7, 2005 through February 22, 2006. The NRC received over 900 comments from the public regarding that rulemaking, including a comment on cyber-security. In addition, the NRC also published a proposed rule that would revise the physical security requirements for all nuclear power plants and includes provisions related to cyber-security. That proposed rule was published in the *Federal Register* for public comment from October 26, 2006 through March 26, 2007, and three public meetings to solicit comments and resolve questions were held between November 2006 and February 2007. The NRC has received, and is reviewing, numerous comments on the proposed cyber-security requirements.

Our efforts also include outreach to our Federal partners, including the Department of Homeland Security, to gain additional insights on cyber-security best practices as related to control and safety systems. As a result, the NRC intends to integrate these insights into the current rulemaking on cyber-security requirements and to develop associated regulatory guidance to support rule implementation.

Recently, the NRC has established a Digital Information & Control Steering Committee. One of the functions of the Digital Information & Control Steering Committee has been to facilitate consistent resolution of issues across multiple NRC organizations and to ensure timely resolution of strategic and policy issues by forming task working groups assigned to individual key issues. These task working group meetings, as well as the Steering Committee meetings, are public meetings which solicit and involve participation by nuclear as well as commercial control system designers and users.

QUESTION 7: The NRC concluded that the remote access capability of the VFD controllers at the Browns Ferry plant was removed prior to the incident. However, it would seem that there exists a strong possibility that other plants are utilizing remotely accessible controllers, making them vulnerable to remote exploitation. Has the NRC conducted a review of plants to determine which ones are using remotely accessible controllers?

RESPONSE: Yes. Following the events of September 11, 2001, the NRC issued two orders, EA-02-026 *Interim Compensatory Measures*, and EA-03-086

Revised Design Basis Threat, which included requirements for power reactor licensees to implement measures to enhance cyber-security. In addition, the NRC has published NRC NUREG/CR-6847, *Cyber-security Self-Assessment Method for U.S. Nuclear Power Plants*. The NUREG forms the basis for an industry-generated guidance document that is being voluntarily implemented by plant owners to assess comprehensively their facilities for cyber-security vulnerabilities and to establish mitigation strategies. In May 2007, all plants completed site-specific self-assessments. The staff will review the self-assessments to identify if and how remotely accessible controllers are being utilized.

In 2004, the NRC completed a cyber-security assessment at four nuclear plants. The results of this assessment are summarized in NUREG/CR-6852, *An Examination of Cyber-security at Several U.S. Nuclear Power Plants*.