



One Hundred Tenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

May 15, 2007

Dale E. Klein
Chairman
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Dear Chairman Klein,

We write to you with great concern about the cybersecurity posture of our nation's nuclear power plants, and ask that you move with all deliberate speed in ensuring that nuclear plant licensees institute comprehensive cybersecurity policies and procedures on safety and non-safety systems alike.

On April 17, 2007, the U.S. Nuclear Regulatory Commission (NRC) issued NRC Information Notice 2007-15, "Effects of Ethernet-Based, Non-Safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations." The Notice describes an incident that occurred on August 19, 2006, at the Brown's Ferry Unit 3 facility, which was manually scrambled following a loss of both of the recirculation pumps. After conducting a review of the event, the licensee determined that the root cause of failure was the malfunction of the variable frequency drive (VFD) controller due to "excessive traffic" on the plant's computer network. The licensee notified the NRC of the incident and the corrective actions implemented, which included placing a firewall that limits connections and traffic to any devices on the plant's integrated computer system (ICS) network. In accord with current regulations, NRC staff decided against investigating the failure as a "cybersecurity incident" because 1) the failing system was a "non-safety" system rather than a "safety" system, and 2) it was determined by the licensee that the incident did not involve an external cyber attack on the system.

We have deep reservations about the NRC's hesitation to conduct a special investigation into this incident. First, although NRC regulations only specify cyber requirements for safety systems, it is clear from the Notice that the disruption of a non-safety system can impact a plant's safety systems. The manual scram by the operators was the only reason that the excessive network traffic in this incident did not trigger a scram by the plant's safety systems. It is clear, therefore, that a nuclear plant's safety systems are directly impacted by the security of its non-safety systems; a weakness or vulnerability in the non-safety network can disrupt operations and trigger a safety system shutdown. According to 10 C.F.R. 50.65(b)(2)(iii), the NRC may take corrective action against a license holder whose non-safety systems could cause a reactor scram. The connection between the systems in this incident, coupled with the authority retained by the

May 15, 2007

Page 2

NRC under §50 of its regulations, should be enough to trigger a thorough and rigorous review of the licensee's cybersecurity posture.

Furthermore, according to the Notice, "the licensees could not conclusively establish" whether the network malfunction was caused by a network disruption within the plant or the malicious activity of an external source. Conversations between the Homeland Security Committee staff and NRC representatives suggest that it is possible that this incident could have come from outside the plant. Unless and until the cause of the excessive network load can be explained, there is no way for either the licensee or the NRC to know that this was not an external distributed denial of service attack. Without a thorough, independent review of the logs and associated data, the assumption that this incident is not an outside attack is unjustifiable.

We are concerned that current NRC regulations fail to comprehensively proscribe adequate cybersecurity protections of both safety and non-safety systems. Though safety systems are regulated by specific cyber requirements in the design system, licensees are not required to adhere to a specific set of regulations in securing their non-safety systems. Instead, the NRC issues general recommendations to guide licensees in developing their cybersecurity plans. This might be considered acceptable if a non-safety system could never affect a safety system. But given the apparent nexus between the two, it is hard to understand how the differential regulation of the systems remains compelling.

We understand that the NRC is engaged in a comprehensive rulemaking that will cover new physical security requirements for plant licensees. Among the additional requirements include regulations for cybersecurity. Given the regulatory shortfalls exposed by this recent incident, we hope that the new regulations will reach beyond safety systems and underscore the impact that disruptions of non-safety systems can have on the operation of a plant. We also hope that the NRC will review "important to safety systems," as cyber disruptions to those systems may also have an impact on a plant's functions.

We ask that you please provide the Committee with the following information:

1. Has the NRC conclusively determined the source of the data storm described in Information Notice 2007-15?
2. Does the NRC plan to exercise its authority under 10 C.F.R. 50.65 to conduct an investigation of the incident at Brown's Ferry?
3. In reviewing the incident, will the NRC determine what cybersecurity policies and procedures the site followed, and what cybersecurity assessments were performed?
4. How will future NRC regulations address the cybersecurity interdependencies of non-safety systems and safety systems? What specific security features will these systems contain?

May 15, 2007

Page 3

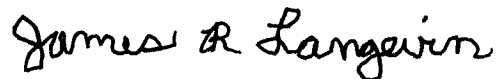
5. Non-safety systems are not the only networked operations within a nuclear plant. As time passes, more and more safety systems will be networked and accessible online. How will future NRC regulations address the rise of networked safety systems?
6. How has the NRC reached out to the non-nuclear control 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?
7. The NRC concluded that the remote access capability of the VFD controllers at the Brown's 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?

Pursuant to Rule X (3) (g) and Rule XI of the Rules of the House of Representatives, we request a response in writing by not later than June 14, 2007. If you have any questions, please contact Cherri L. Branson, Chief Oversight Counsel, Committee on Homeland Security at (202) 226-2616.

Sincerely,



Bennie G. Thompson
Chairman



James R. Langevin
Chairman
Subcommittee on Emerging Threats,
Cybersecurity, and Science and
Technology

BGT/jso