Responses to Requests for Information
Senator Edward J. Markey
Letter Dated July 10, 2017

1. How many nuclear plants in the United States have been affected by cyber attacks?

The Nuclear Regulatory Commission (NRC) maintains continuous awareness of actual and potential cyber attacks by working with its licensees, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and other Federal partners. As early as this spring, the NRC was notified that advanced persistent threat actors have targeted the business networks of multiple power reactor licensees. NRC staff and the NRC's Federal partners can provide additional detail regarding the number and nature of these attacks during the classified briefing that you have requested. The impact of these attacks to NRC licensees was limited to the business network and did not impact any safety, security, or emergency preparedness function. As a general matter, NRC-required security controls implemented between licensee business networks and separate plant control system networks are designed to protect against the cyber threat. Accordingly, no nuclear power plants were affected; rather, the business networks of companies that operate the plants were affected.

2. Were the attacks described in this report discovered by plant operators themselves, or by Federal agencies?

Cyber attacks are generally identified by either an entity self-reporting, reporting by a trusted third-party, by tools deployed on computer networks that detect malicious activity, or some combination of these methods. The recent attacks referred to in your letter were identified through the businesses that were targeted and other sources, including both U.S. and international partners.

3. Do corporate and administrative systems at nuclear plant operators contain any information that malicious actors could use to compromise the safety and security of physical systems or personnel with access to those systems?

Current NRC regulations area designed to prevent malicious cyber actors from compromising safety and security systems by accessing corporate and administrative systems at nuclear power plants or other methods. The NRC is aware that some nuclear power plants may have select emergency preparedness and security-related digital equipment connected to the corporate and administrative systems. However, licensees are required to restrict access to that information and protect the digital equipment in accordance with NRC regulations. However, malicious cyber actors could gain access to information about the companies and their personnel that is maintained on the corporate and administrative systems. The NRC is part of Federal Government efforts working with the private sector to share information and technical assistance to strengthen the protection of these computer networks.

4. Within the Federal Government, which agency or agencies are responsible for coordinating cybersecurity at U.S. nuclear power stations?

For cyber incidents affecting critical infrastructure, such as nuclear reactors, the Federal

Government's roles and responsibilities are guided by Presidential Policy Directive (PPD) 41, the National Cyber Security Response Plan as well as other statutory authorities. The DHS coordinates cyber security communications and initiatives for all critical infrastructure, including the nuclear sector. The NRC regulates cyber security of computers, communication systems, and networks associated with safety, security, and emergency preparedness functions at U.S. nuclear power plants, in accordance with NRC's cyber security rule and other portions of its regulations.

5. What coordination exists between the Department of Defense, the Department of Homeland Security, the Department of Energy, the Federal Bureau of Investigations, and the Nuclear Regulatory Commission? Is there a single official responsible for coordinating the work of these agencies to safeguard cyber-security at U.S. nuclear power stations? If not, are there plans to appoint a single official to do so?

For cyber security at nuclear power plants, the DHS, FBI, the Department of Energy, and the NRC coordinate to bring their individual expertise and authorities to bear to prevent and respond to cybersecurity issues, guided by PPD 21. Additionally, DHS leads the National Cybersecurity and Communications Integration Center (NCCIC), which serves as the central node for government agencies, the private sector, and international entities involved in cybersecurity. NRC's cyber security specialists routinely coordinate with the NCCIC.

6. Given your agencies' assessments of the cyber-threat to nuclear power stations, are U.S. nuclear reactor licensees devoting sufficient resources to cyber-security?

From the NRC's perspective, adequate actions are being taken, based on our understanding of the threat assessment. That perspective is informed by the NRC's oversight of licensees' efforts to comply with cyber security regulations under 10 CFR Part 73. The current cyber security rule, issued in 2009, provides a cyber framework for adequate protection of digital computer and communication systems and networks associated with safety, security, and emergency preparedness functions against cyber attacks. By 2012, NRC licensees implemented the interim requirements, and the NRC inspected implementation from 2013 to 2015. During those inspections, the staff found that the licensees were in compliance with the interim cyber security requirements. With a few limited exceptions, such as plants that are decommissioning prior to 2019, all licensees are scheduled to fully implement the remaining regulatory requirements for cyber security by December 2017. Some licensees are already fully compliant. The NRC began inspecting the full cyber security implementation in July 2017. Since the NRC issued its cyber notification rule in 2015, the staff has not been notified that any of the NRC-regulated safety, security, or emergency preparedness functions at the operating nuclear plants have been penetrated by a cyber attack.

7. In your view, do the Design Basis Threat (DBT) and associated implementation guidance for U.S. nuclear reactors need to be updated to reflect changes in the severity of cyber-attacks on U.S. nuclear plants?

No. The NRC maintains communications with our Federal partners, including the intelligence community, to assess the threat environment, including the cyber threat. Based on this communication and ongoing threat analysis, the NRC has determined that

our current cyber framework provides adequate protection of U.S. nuclear reactors and the public. The NRC will implement improvements to our cyber framework if new information and analysis indicates that changes are needed.

8. The U.S. nuclear energy industry has asked the Nuclear Regulatory Commission to narrow the regulations governing cybersecurity at licensed reactors, such that the regulations would only apply to systems involved in the protection of the reactor and spent fuel pools. Given that the attacks cited in this report targeted systems outside that scope, wouldn't it be more appropriate to increase the scope of the cyber security rule, rather than decrease it?

The Petition for Rulemaking that you reference is currently under review, and a determination relative to the request has not been made. Separately, the NRC staff plans to do an assessment during the next round of cyber security inspections to determine, in part, the proper scope of the existing cyber security rule.

9. Do your agencies have sufficient funding to address cyber-security vulnerabilities at U.S. nuclear power stations?

Yes, the NRC has adequate funding to implement its cyber security responsibilities.