

COMMITTEES:

ENVIRONMENT AND PUBLIC WORKS

RANKING MEMBER:

SUPERFUND, WASTE MANAGEMENT, AND  
REGULATORY OVERSIGHT

FOREIGN RELATIONS

RANKING MEMBER:

SUBCOMMITTEE ON AFRICA  
AND GLOBAL HEALTH POLICY

COMMERCE, SCIENCE, AND TRANSPORTATION

SMALL BUSINESS AND ENTREPRENEURSHIP

CHAIRMAN:

U.S. SENATE CLIMATE CHANGE CLEARINGHOUSE

## United States Senate

July 10, 2017

SUITE SD-255  
DIRKSEN BUILDING  
WASHINGTON, DC 20510-2107  
202-224-2742

975 JFK FEDERAL BUILDING  
15 NEW SUDBURY STREET  
BOSTON, MA 02203  
617-565-8519

222 MILLIKEN BOULEVARD, SUITE 312  
FALL RIVER, MA 02721  
508-677-0523

1550 MAIN STREET, 4TH FLOOR  
SPRINGFIELD, MA 01101  
413-785-4610

The Honorable James N. Mattis  
Secretary of Defense  
Department of Defense  
1000 Defense Pentagon  
Washington, DC 20301

The Honorable John F. Kelly  
Secretary of Homeland Security  
Department of Homeland Security  
3801 Nebraska Ave NW  
Washington, DC 20528

The Honorable Rick Perry  
Secretary of Energy  
Department of Energy  
1000 Independence Ave SW  
Washington, DC 20585

The Honorable Kristine L. Svinicki  
Chairman  
Nuclear Regulatory Commission  
11555 Rockville Pike  
Rockville, MD 20555

The Honorable Andrew G. McCabe  
Acting Director  
Federal Bureau of Investigation  
935 Pennsylvania Ave NW  
Washington, DC 20535

Dear Secretary Mattis, Secretary Kelly, Secretary Perry, Chairman Svinicki, and Director McCabe:

I write to request information about reports that foreign hackers compromised the cybersecurity of U.S. nuclear power plant operators. A cyber-attack on a nuclear power station could result in the theft of information related to the plant's safety and security systems, and it could cause physical damage to the power station, increasing the risk of a catastrophic radioactive release. These profound risks to public safety and U.S. national security require a robust and coordinated response across federal agencies.

According to the New York Times, the Department of Homeland Security and the Federal Bureau of Investigation recently completed a report indicating that an "advanced persistent threat" actor targeted personnel working for nuclear plant operators and companies that manufacture power plant control systems. The targeted personnel included industrial control engineers with "direct access to systems that, if damaged, could lead to an explosion, fire or a

spill of dangerous material.”<sup>1</sup> Bloomberg reported that the chief suspect in these attacks was Russia, which is also suspected of disrupting energy infrastructure in Ukraine.<sup>2</sup>

The Department of Homeland Security has stated that the impact of these attacks “appears to be limited to administrative and business networks.” However, there is no guarantee that malicious code could not migrate to physical control systems through the errant or unauthorized use of removable storage devices. Furthermore, administrative and business networks could contain information relevant to the safety and security of nuclear plants, as well as personal information about the plant’s personnel. Malicious actors could use this sensitive data to undermine plant security.

Given the consequences of a breach of safety at a nuclear power station – including the deliberate sabotage of the reactor core or the spent-fuel storage pool – evidence that foreign governments have targeted U.S. nuclear power stations must be treated with the utmost gravity. In light of that, please provide answers to the following questions:

1. How many nuclear plants in the United States have been affected by cyber-attacks?
2. Were the attacks described in this report discovered by plant operators themselves, or by federal agencies?
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?
4. Within the federal government, which agency or agencies are responsible for coordinating cybersecurity at U.S. nuclear power stations?
5. What coordination exists between the Department of Defense, the Department of Homeland Security, the Department of Energy, the Federal Bureau of Investigation, 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?
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?

---

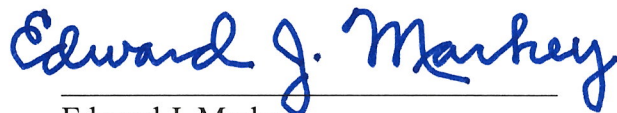
<sup>1</sup> Nicole Perlroth, “Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say,” *New York Times*, July 6, 2017, <https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html>

<sup>2</sup> Michael Riley, Jennifer A. Dlouhy, and Bryan Gruley, “Russians Are Suspects in Nuclear Site Hackings, Sources Say,” Bloomberg, July 6, 2017, <https://www.bloomberg.com/news/articles/2017-07-07/russians-are-said-to-be-suspects-in-hacks-involving-nuclear-site>

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

Please provide these answers to my office by August 10. I also request that officials from your agencies provide me with a classified briefing that addresses the cyber-vulnerabilities of U.S. nuclear power stations and other critical infrastructure. Thank you for your attention to this serious issue for our national security.

Sincerely,



---

Edward J. Markey  
United States Senator  
Ranking Member, Subcommittee on  
East Asia, the Pacific, and  
International Cybersecurity Policy  
Senate Foreign Relations Committee