

EDWARD J. MARKEY
MASSACHUSETTS

COMMITTEES:
ENVIRONMENT AND PUBLIC WORKS

FOREIGN RELATIONS

RANKING MEMBER:

SUBCOMMITTEE ON EAST ASIA, THE PACIFIC,
AND INTERNATIONAL CYBERSECURITY POLICY

COMMERCE, SCIENCE, AND TRANSPORTATION

RANKING MEMBER:

SUBCOMMITTEE ON
SPACE, SCIENCE, AND COMPETITIVENESS

SMALL BUSINESS AND ENTREPRENEURSHIP

CHAIRMAN:

U.S. SENATE CLIMATE CHANGE TASK FORCE

United States Senate

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 01103
413-785-4610

August 13, 2018

The Honorable Kirstjen M. Nielsen
Secretary
U.S. Department of Homeland Security
Office of Legislative Affairs
Mail Stop 0020
Washington, D.C. 20528

Dear Secretary Nielsen,

According to recent press reports, state-sponsored groups in Russia were behind a cyberattack on U.S. electric utilities last year.¹ In light of these concerning reports, I write to better understand how the federal government is working to maximize the security of our electric grid and minimize its vulnerabilities to attack.

On July 23, the Wall Street Journal reported that, in 2016 and 2017, hackers backed by the Russian government successfully penetrated the U.S. electric grid through hundreds of power companies and third party vendors with whom they do business.² Utilizing techniques to access purportedly secure networks, these Russian hackers managed to invade the networks of key utility vendors — companies “who have special access to update software, run diagnostics on equipment and perform other services that are needed to keep millions of pieces of gear in working order.”³ Through these vendors, the Russian hackers gained access to the control rooms of U.S. electric utilities, putting them in position to severely disrupt the U.S. power flow. There is now also concern that Russia may be seeking to automate these types of attacks, which could lead to more pervasive and broader hacking and harm to the electric grid.⁴

This recent attack should come as no surprise. In 2013, the Department of Homeland Security (DHS) considered the threat of cyberattack so serious that it issued an alert warning industry and

¹ Rebecca Smith, Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say, Wall Street Journal (July 23, 2018), <https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110>

² *Id.*

³ *Id.*

⁴ *Id.*

government officials about it.⁵ That same year, I released a report entitled “Electric Grid Vulnerability: Industry Responses Reveal Security Gaps,” which found that the electric grid was the target of ongoing cyberattacks.⁶ In August 2016, the Idaho National Laboratory issued a report entitled “Cyber Threat and Vulnerability Analysis of the U.S. Electric Center,” which warned that, “[w]ith utilities in the U.S. and around the world increasingly moving toward smart grid technology and other upgrades with inherent cyber vulnerabilities, correlative threats from malicious cyberattacks on the North American electric grid continue to grow in frequency and sophistication.”⁷ And just last year, in the Department of Energy’s Quadrennial Energy Review, that agency found that the “cybersecurity landscape is characterized by rapidly evolving threats and vulnerability, juxtaposed against the slower-moving deployment of defense measures” and recommended that “system planning must evolve to meet the need for rapid response to system disturbances.”⁸

Following the release of my 2013 report, the Federal Energy Regulatory Commission (FERC) initiated a series of rulemakings to help address the security of our electric-system infrastructure. The most recent of these rules, issued in April 2018, institutes mandatory security controls for transient electronic devices, such as thumb drives, in an attempt to address classic cyber-infiltration methods through third party devices.⁹ However, as this most recent incident demonstrates, these security measures do not impede the sophisticated actions now being employed by foreign hackers.

To gain a better understanding of the federal government’s work in protecting our national grid and the coordination between key federal agencies and electric utilities, I respectfully ask for a staff briefing by September 7, 2018 to, at a minimum, discuss the following:

- The role your agency plays in identifying, analyzing, responding to, or creating new rules and standards to address cyber vulnerabilities of electric utilities.
- How your agency works with other federal agencies to coordinate efforts around cybersecurity of electric utilities.

⁵ Ellen Nakashima, U.S. warns industry of heightened risk of cyberattack, Washington Post (May 9, 2013), https://www.washingtonpost.com/world/national-security/us-warns-industry-of-heightened-risk-of-cyberattack/2013/05/09/39a04852-b8df-11e2-aa9e-a02b765ff0ea_story.html

⁶ Electric Grid Vulnerability: Industry Responses Reveal Security Gaps, prepared by the staff of Congressmen Edward J. Markey (D-MA) and Henry Waxman (D-CA) (May 21, 2013), https://www.markey.senate.gov/imo/media/doc/Markey%20Grid%20Report_05.21.131.pdf

⁷ Mission Support Center Analysis Report, Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, Idaho National Laboratory (August 2016), <https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf>

⁸ Quadrennial Energy Review, Transforming the Nation’s Electricity System: The Second Installment of the QER, U.S. Department of Energy (January 2017), <https://www.energy.gov/sites/prod/files/2017/02/f34/Quadrennial%20Energy%20Review--Second%20Installment%20%28Full%20Report%29.pdf>

⁹ 83 FR 17913

The Honorable Kirstjen M. Nielsen

August 13, 2018

Page 3

- Efforts to engage both electric utilities and critical third party vendors to protect electric utility assets against vulnerability.
- Efforts to proactively identify vulnerabilities in the U.S. electric grid.
- What more can be done to improve the electric grid's resiliency against sophisticated and relentless cybersecurity attacks.

Thank you in advance for your attention to these requests. If you have any questions about them, please contact Lindsey Griffith of my staff at 202-224-2742.

Sincerely,

A handwritten signature in blue ink that reads "Edward J. Markey". The signature is written in a cursive style and is positioned above a horizontal line.

Edward J. Markey

United States Senator

EDWARD J. MARKEY
MASSACHUSETTS

COMMITTEES:
ENVIRONMENT AND PUBLIC WORKS

FOREIGN RELATIONS

RANKING MEMBER:

SUBCOMMITTEE ON EAST ASIA, THE PACIFIC,
AND INTERNATIONAL CYBERSECURITY POLICY

COMMERCE, SCIENCE, AND TRANSPORTATION

RANKING MEMBER:

SUBCOMMITTEE ON
SPACE, SCIENCE, AND COMPETITIVENESS

SMALL BUSINESS AND ENTREPRENEURSHIP

CHAIRMAN:

U.S. SENATE CLIMATE CHANGE TASK FORCE

United States Senate

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 01103
413-785-4610

August 13, 2018

The Honorable Rick Perry
Secretary
U.S. Department of Energy
The Office of Congressional & Intergovernmental Affairs
1000 Independence Ave., SW
Washington, DC 20585

Dear Secretary Perry,

According to recent press reports, state-sponsored groups in Russia were behind a cyberattack on U.S. electric utilities last year.¹ In light of these concerning reports, I write to better understand how the federal government is working to maximize the security of our electric grid and minimize its vulnerabilities to attack.

On July 23, the Wall Street Journal reported that, in 2016 and 2017, hackers backed by the Russian government successfully penetrated the U.S. electric grid through hundreds of power companies and third party vendors with whom they do business.² Utilizing techniques to access purportedly secure networks, these Russian hackers managed to invade the networks of key utility vendors — companies “who have special access to update software, run diagnostics on equipment and perform other services that are needed to keep millions of pieces of gear in working order.”³ Through these vendors, the Russian hackers gained access to the control rooms of U.S. electric utilities, putting them in position to severely disrupt the U.S. power flow. There is now also concern that Russia may be seeking to automate these types of attacks, which could lead to more pervasive and broader hacking and harm to the electric grid.⁴

This recent attack should come as no surprise. In 2013, the Department of Homeland Security (DHS) considered the threat of cyberattack so serious that it issued an alert warning industry and

¹ Rebecca Smith, Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say, Wall Street Journal (July 23, 2018), <https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110>

² *Id.*

³ *Id.*

⁴ *Id.*

government officials about it.⁵ That same year, I released a report entitled “Electric Grid Vulnerability: Industry Responses Reveal Security Gaps,” which found that the electric grid was the target of ongoing cyberattacks.⁶ In August 2016, the Idaho National Laboratory issued a report entitled “Cyber Threat and Vulnerability Analysis of the U.S. Electric Center,” which warned that, “[w]ith utilities in the U.S. and around the world increasingly moving toward smart grid technology and other upgrades with inherent cyber vulnerabilities, correlative threats from malicious cyberattacks on the North American electric grid continue to grow in frequency and sophistication.”⁷ And just last year, in the Department of Energy’s Quadrennial Energy Review, that agency found that the “cybersecurity landscape is characterized by rapidly evolving threats and vulnerability, juxtaposed against the slower-moving deployment of defense measures” and recommended that “system planning must evolve to meet the need for rapid response to system disturbances.”⁸

Following the release of my 2013 report, the Federal Energy Regulatory Commission (FERC) initiated a series of rulemakings to help address the security of our electric-system infrastructure. The most recent of these rules, issued in April 2018, institutes mandatory security controls for transient electronic devices, such as thumb drives, in an attempt to address classic cyber-infiltration methods through third party devices.⁹ However, as this most recent incident demonstrates, these security measures do not impede the sophisticated actions now being employed by foreign hackers.

To gain a better understanding of the federal government’s work in protecting our national grid and the coordination between key federal agencies and electric utilities, I respectfully ask for a staff briefing by September 7, 2018 to, at a minimum, discuss the following:

- The role your agency plays in identifying, analyzing, responding to, or creating new rules and standards to address cyber vulnerabilities of electric utilities.
- How your agency works with other federal agencies to coordinate efforts around cybersecurity of electric utilities.

⁵ Ellen Nakashima, U.S. warns industry of heightened risk of cyberattack, Washington Post (May 9, 2013), https://www.washingtonpost.com/world/national-security/us-warns-industry-of-heightened-risk-of-cyberattack/2013/05/09/39a04852-b8df-11e2-aa9e-a02b765ff0ea_story.html

⁶ Electric Grid Vulnerability: Industry Responses Reveal Security Gaps, prepared by the staff of Congressmen Edward J. Markey (D-MA) and Henry Waxman (D-CA) (May 21, 2013), https://www.markey.senate.gov/imo/media/doc/Markey%20Grid%20Report_05.21.131.pdf

⁷ Mission Support Center Analysis Report, Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, Idaho National Laboratory (August 2016), <https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf>

⁸ Quadrennial Energy Review, Transforming the Nation’s Electricity System: The Second Installment of the QER, U.S. Department of Energy (January 2017), <https://www.energy.gov/sites/prod/files/2017/02/f34/Quadrennial%20Energy%20Review--Second%20Installment%20%28Full%20Report%29.pdf>

⁹ 83 FR 17913

The Honorable Rick Perry

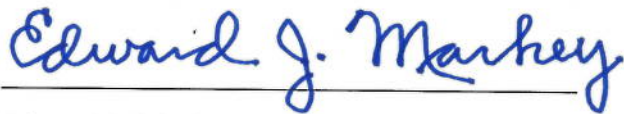
August 13, 2018

Page 3

- Efforts to engage both electric utilities and critical third party vendors to protect electric utility assets against vulnerability.
- Efforts to proactively identify vulnerabilities in the U.S. electric grid.
- What more can be done to improve the electric grid's resiliency against sophisticated and relentless cybersecurity attacks.

Thank you in advance for your attention to these requests. If you have any questions about them, please contact Lindsey Griffith of my staff at 202-224-2742.

Sincerely,

A handwritten signature in blue ink that reads "Edward J. Markey". The signature is written in a cursive style and is positioned above a horizontal line.

Edward J. Markey

United States Senator

EDWARD J. MARKEY
MASSACHUSETTS

COMMITTEES:
ENVIRONMENT AND PUBLIC WORKS
FOREIGN RELATIONS
RANKING MEMBER:

SUBCOMMITTEE ON EAST ASIA, THE PACIFIC,
AND INTERNATIONAL CYBERSECURITY POLICY

COMMERCE, SCIENCE, AND TRANSPORTATION

RANKING MEMBER:

SUBCOMMITTEE ON

SPACE, SCIENCE, AND COMPETITIVENESS

SMALL BUSINESS AND ENTREPRENEURSHIP

CHAIRMAN:

U.S. SENATE CLIMATE CHANGE TASK FORCE

United States Senate

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 01103
413-785-4610

August 13, 2018

The Honorable Kevin McIntyre
Chairman
Federal Energy Regulatory Commission
888 First Street, NE, Room 11H
Washington, DC 20426

Dear Chairman McIntyre,

According to recent press reports, state-sponsored groups in Russia were behind a cyberattack on U.S. electric utilities last year.¹ In light of these concerning reports, I write to better understand how the federal government is working to maximize the security of our electric grid and minimize its vulnerabilities to attack.

On July 23, the Wall Street Journal reported that, in 2016 and 2017, hackers backed by the Russian government successfully penetrated the U.S. electric grid through hundreds of power companies and third party vendors with whom they do business.² Utilizing techniques to access purportedly secure networks, these Russian hackers managed to invade the networks of key utility vendors — companies “who have special access to update software, run diagnostics on equipment and perform other services that are needed to keep millions of pieces of gear in working order.”³ Through these vendors, the Russian hackers gained access to the control rooms of U.S. electric utilities, putting them in position to severely disrupt the U.S. power flow. There is now also concern that Russia may be seeking to automate these types of attacks, which could lead to more pervasive and broader hacking and harm to the electric grid.⁴

This recent attack should come as no surprise. In 2013, the Department of Homeland Security (DHS) considered the threat of cyberattack so serious that it issued an alert warning industry and government officials about it.⁵ That same year, I released a report entitled “Electric Grid

¹ Rebecca Smith, Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say, Wall Street Journal (July 23, 2018), <https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110>

² *Id.*

³ *Id.*

⁴ *Id.*

⁵ Ellen Nakashima, U.S. warns industry of heightened risk of cyberattack, Washington Post (May 9, 2013), https://www.washingtonpost.com/world/national-security/us-warns-industry-of-heightened-risk-of-cyberattack/2013/05/09/39a04852-b8df-11e2-aa9e-a02b765ff0ea_story.html

Vulnerability: Industry Responses Reveal Security Gaps,” which found that the electric grid was the target of ongoing cyberattacks.⁶ In August 2016, the Idaho National Laboratory issued a report entitled “Cyber Threat and Vulnerability Analysis of the U.S. Electric Center,” which warned that, “[w]ith utilities in the U.S. and around the world increasingly moving toward smart grid technology and other upgrades with inherent cyber vulnerabilities, correlative threats from malicious cyberattacks on the North American electric grid continue to grow in frequency and sophistication.”⁷ And just last year, in the Department of Energy’s Quadrennial Energy Review, that agency found that the “cybersecurity landscape is characterized by rapidly evolving threats and vulnerability, juxtaposed against the slower-moving deployment of defense measures” and recommended that “system planning must evolve to meet the need for rapid response to system disturbances.”⁸

Following the release of my 2013 report, the Federal Energy Regulatory Commission (FERC) initiated a series of rulemakings to help address the security of our electric-system infrastructure. The most recent of these rules, issued in April 2018, institutes mandatory security controls for transient electronic devices, such as thumb drives, in an attempt to address classic cyber-infiltration methods through third party devices.⁹ However, as this most recent incident demonstrates, these security measures do not impede the sophisticated actions now being employed by foreign hackers.

To gain a better understanding of the federal government’s work in protecting our national grid and the coordination between key federal agencies and electric utilities, I respectfully ask for a staff briefing by September 7, 2018 to, at a minimum, discuss the following:

- The role your agency plays in identifying, analyzing, responding to, or creating new rules and standards to address cyber vulnerabilities of electric utilities.
- How your agency works with other federal agencies to coordinate efforts around cybersecurity of electric utilities.
- Efforts to engage both electric utilities and critical third party vendors to protect electric utility assets against vulnerability.
- Efforts to proactively identify vulnerabilities in the U.S. electric grid.

⁶ Electric Grid Vulnerability: Industry Responses Reveal Security Gaps, prepared by the staff of Congressmen Edward J. Markey (D-MA) and Henry Waxman (D-CA) (May 21, 2013), https://www.markey.senate.gov/imo/media/doc/Markey%20Grid%20Report_05.21.131.pdf

⁷ Mission Support Center Analysis Report, Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, Idaho National Laboratory (August 2016), <https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf>

⁸ Quadrennial Energy Review, Transforming the Nation’s Electricity System: The Second Installment of the QER, U.S. Department of Energy (January 2017), <https://www.energy.gov/sites/prod/files/2017/02/f34/Quadrennial%20Energy%20Review--Second%20Installment%20%28Full%20Report%29.pdf>


⁹ 83 FR 17913

Chairman Kevin McIntyre
August 13, 2018
Page 3

- What more can be done to improve the electric grid's resiliency against sophisticated and relentless cybersecurity attacks.

Thank you in advance for your attention to these requests. If you have any questions about them, please contact Lindsey Griffith of my staff at 202-224-2742.

Sincerely,

A handwritten signature in blue ink that reads "Edward J. Markey". The signature is written in a cursive style and is positioned above a horizontal line.

Edward J. Markey

United States Senator