

Congress of the United States

House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371
www.science.house.gov

July 10, 2018

The Honorable Gene L. Dodaro
Comptroller General of the United States
U.S. Government Accountability Office (GAO)
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Dodaro:

Public utilities provide critical services for households, hospitals, businesses and local governments. All of these systems, without exception, are vulnerable to natural hazards as well as intentional physical and cyber-related attacks. The vulnerabilities in our digital networks that tie our critical infrastructure together were highlighted earlier this year when the Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) issued a joint “Technical Alert” regarding “Russian government actions targeting U.S. Government entities as well as organizations in the energy, nuclear, commercial facilities, water, aviation and critical manufacturing sectors.” The alert detailed a Russian effort beginning in 2016 that has targeted American-based computer networks of “small commercial facilities.”¹

Eric Chien, a security technology director at Symantec, which published a report in October 2017 on Russian efforts to infiltrate the U.S. energy infrastructure, told the *New York Times*: “We now have evidence they’re sitting on the machines, connected to industrial control infrastructure, that allow them to effectively turn the power off or effect sabotage,” said Chien. “From what we can see ... [t]hey have the ability to shut the power off. All that’s missing is some political motivation,” he warned.²

Russia, however, is not the only foreign nation targeting our critical infrastructure. In June 2018, a Houston, Texas based energy-consulting firm named Opportune LLP reported that during a cybersecurity review for a client they discovered that a power plant’s control system had been hacked by unknown perpetrators in China.³ In February 2018, the U.S. Department of Justice (DOJ) indicted nine Iranians for engaging in cyberattacks against the U.S. Federal Energy Regulatory Commission (FERC), 144 U.S.

¹ “Alert (TA18-074A) – Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors,” United States Computer Emergency Readiness Team (US CERT), March 16, 2018, accessed here: <https://www.us-cert.gov/ncas/alerts/TA18-074A>

² Nicole Perlroth and David E. Sanger, “Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says,” *New York Times*, March 15, 2018, accessed here: <https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html>

³ Glenn Hartfiel, “Power Plants: Cybersecurity Threats and Risks (Part I),” *Opportune LLP*, June 2018, accessed here: <https://opportune.com/Energy-Sector-Insights-Events/Insights/Power-Plants-Cybersecurity-Threats-and-Risks-Part-1/>

universities and 36 private companies, including one “industrial machinery company.”⁴ In April 2018, at least four U.S. natural gas pipeline companies were victims of cyberattacks that temporarily shut down their ability to electronically communicate with their customers.⁵

The ability of cyber-criminals or foreign state actors to damage or degrade public utilities and critical infrastructure networks through cybersecurity vulnerabilities and digital infiltrations is a rising and justified concern. The Department of Homeland Security has designated 16 core industries as part of U.S. critical infrastructure, including the chemical, energy, water, communications, healthcare, transportation and government facilities arenas, which includes the U.S. election infrastructure. Cyberattacks and the potential consequences of these attacks against critical infrastructure are escalating. This has made the need to thoroughly address the weaknesses and vulnerabilities of our critical infrastructure paramount.

In August 2017, a Saudi Arabian petrochemical company was the victim of a cyberattack that investigators believe was intended not to manipulate or obtain critical data, but to trigger an explosion. Fortunately, a simple coding error prevented that from occurring.⁶ Other cyber-attacks have successfully damaged critical infrastructure services. In 2000, an Australian man hacked into the computerized waste management system in Maroochy Shire, Queensland, causing millions of liters of raw sewage to spill out into local parks, rivers and even the grounds of the Hyatt Regency hotel. “Marine life died, the creek water turned black and the stench was unbearable for residents,” Jeanelle Bryant of the Australian Environmental Protection Agency told *The Register* newspaper at the time.⁷ More than one decade ago researchers at the U.S. Department of Energy’s Idaho National Laboratory (INL) also successfully caused a generator to self-destruct and explode through a cyberattack they carried out in an experiment called “Aurora.”⁸ Other cyber-attacks have been less nefarious but have caused serious damage.

Just before Christmas in 2015, a cyberattack that experts believe was perpetrated by Russia resulted in massive power outages in Ukraine. The attacks did not stop there. The Central Intelligence Agency (CIA) also attributed to Russian military hackers a June 2017 cyberattack against Ukraine that crippled the country’s financial systems and wiped data from the computers at banks, energy firms, and an airport.⁹ The British government has attributed the WannaCry ransomware cyberattack that severely disrupted its National Health Service in May 2017 to North Korea.¹⁰ In March 2016, the U.S. Department of Justice indicted seven Iranian hackers for engaging in a coordinated cyberattack against dozens of U.S.

⁴ Garrett M. Graff, “DOJ Indicts 9 Iranians for Brazen Cyberattacks Against 144 U.S. Universities,” *WIRED*, March 23, 2018, accessed here: <https://www.wired.com/story/iran-cyberattacks-us-universities-indictment/>

⁵ Naureen S. Malik, Ryan Collins and Meenal Vamburkar, “Cyberattack Pings Data Systems of At Least Four Gas Networks,” *Bloomberg Technology*, April 3, 2018, accessed here: <https://www.bloomberg.com/news/articles/2018-04-03/day-after-cyber-attack-a-third-gas-pipeline-data-system-shuts>

⁶ Nicole Perlroth and Clifford Krauss, “A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.” *New York Times*, March 15, 2018, accessed here: <https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html>

⁷ See: Bob Gourley, “The March and April 2000 Hack on Maroochy Shire: Cyber History Made,” *CTO Vision*, July 13, 2012, accessed here: <https://ctovision.com/the-march-and-april-2000-hack-on-maroochy-shire-cyber-history-made/> and Tony Smith, “Hacker jailed for revenge sewage attacks,” *The Register*, October 31, 2001, accessed here: http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

⁸ Jeanne Meserve, “Sources: staged cyber attack reveals vulnerability in power grid,” *CNN*, September 26, 2007, accessed here: <http://www.cnn.com/2007/US/09/26/power.at.risk/>

⁹ Ellen Nakashima, “Russian military was behind ‘NotPetya’ cyberattack in Ukraine, CIA concludes,” *Washington Post*, January 12, 2018, accessed here: https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html?utm_term=.f87cd3d7215f

¹⁰ “Cyber-attack: U.S. and U.K. blame North Korea for WannaCry,” *BBC*, December 19, 2017, accessed here: <http://www.bbc.com/news/world-us-canada-42407488>

banks and an unsuccessful attempt to shut down a dam in New York.¹¹ In 2016, Russia-linked hackers were also probing and in some cases penetrating the U.S. election infrastructure.¹²

The Need for Cybersecurity Experts

The threats against our critical infrastructure are widespread, growing and deeply concerning. The ability to respond to these cyber dangers and emerging risks within our critical infrastructure varies greatly among small and large companies, and public and private entities. A 2018 survey of U.S. electric, gas and water utility officials found that they believed cybersecurity threats posed the largest anticipated threat to their operations, followed by critical employee retirements. On average, the survey found that utilities had nine full-time-equivalent employees dealing with compliance-related issues, including cybersecurity. However, it also found that 13% of utilities had less than one full-time employee addressing compliance issues and that three of the top four skill gaps within the utility industry related to security.¹³ Those findings are troubling given the growing cyber-related threats that are confronting our nation's critical infrastructure networks and the lack of qualified cybersecurity experts available to respond to them.

Last July, several media stories reported that the U.S. intelligence community had detected Russian hackers who had infiltrated U.S. nuclear power plants and other energy companies. According to these reports, U.S. officials said the hackers appeared to have accessed business and personnel files but had not attempted to seize control of the power plants. One of the nuclear plants targeted was reportedly the Wolf Creek Nuclear Operating Corporation, which runs a nuclear generating station in Burlington, Kansas.¹⁴ The DHS/FBI alert issued in March 2018, however, said that in "multiple instances" the cyber intruders "accessed workstations and servers on a corporate network that contained data output from control systems within energy generation facilities" and that they accessed files pertaining to Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems.¹⁵ Both systems are critical to the control, management and operation of our critical infrastructure utilities.

Kaspersky Lab & U.S. Critical Infrastructure

These are the most recent public warnings about Russian cybersecurity threats and specific Russian efforts to infiltrate U.S. critical infrastructure networks. However, in September 2017, DHS issued a Binding Operational Directive (BOD) banning the use of Moscow-based Kaspersky Lab computer security products by U.S. government entities. All federal agencies were required to remove Kaspersky

¹¹ David E. Sanger, "U.S. Indicts 7 Iranians in Cyberattacks on Banks and a Dam," *New York Times*, March 24, 2016, accessed here: <https://www.nytimes.com/2016/03/25/world/middleeast/us-indicts-iranians-in-cyberattacks-on-banks-and-a-dam.html>

¹² "2016 Presidential Hacking Fast Facts," *CNN*, February 21, 2018, accessed here: <https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html>

¹³ "2018 BRIDGE Index Utility Industry Survey," *Bridge Energy Group*, March 13, 2018, accessed here: <https://www.bridgeenergygroup.com/news/press/bridge-survey-reveals-cip-compliance-security-tools-and-compliance-automation-among-top-skills-gaps/>

¹⁴ Nicole Perlroth, "Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say," *New York Times*, July 6, 2017, accessed here: https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html?_r=1&utm_source=Early+Bird+subscribers&utm_campaign=2596883ed6-Early_Bird_07_07_17&utm_medium=email&utm_term=0_f26e77fe91-2596883ed6-87206581 ;

Lisa Rodriguez, "Cyberattack Targeting Kansas Nuclear Facility Highlights Bigger Cybersecurity Threats," *KCUR*, July 7, 2017, accessed here: <http://kcur.org/post/cyberattack-targeting-kansas-nuclear-facility-highlights-bigger-cybersecurity-threats#stream/0>

¹⁵ "Alert (TA18-074A) – Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," United States Computer Emergency Readiness Team (U.S. CERT), March 16, 2018, accessed here: <https://www.us-cert.gov/ncas/alerts/TA18-074A>

products from their networks by mid-December 2017. The U.S. intelligence community was concerned that the Russian government could capitalize on access to Kaspersky's computer software that is used to monitor computer networks for potential security flaws and hacker penetrations, in order to compromise U.S. government computer networks that utilized Kaspersky software.¹⁶ In June 2018, the Department of Defense (DOD), General Services Administration (GSA) and National Aeronautics and Space Administration (NASA) also issued an interim rule published in the *Federal Register* that would prohibit federal government contractors and subcontractors "from providing any hardware, software, or services developed or provided by Kaspersky Lab."¹⁷

However, those requirements would not apply to public utilities, such as water treatment facilities, power plants, natural gas pipelines, or other entities in the private sector, such as hospitals, airports or telecommunications companies. Kaspersky Lab provides security products to more than 270,000 organizations worldwide. Some of those organizations include critical infrastructure related businesses, particularly in Europe. A recent review of some of Kaspersky's current clients also found that a Houston, Texas based oil company with 7,000 employees, 38 offshore platforms and over 77 mobile land rigs around the world, including in North and South America, Europe, the Middle East, Asia and Africa, purchased 1,000 endpoint licenses and 40 virtual server licenses for Kaspersky Lab security software. Another Illinois-based healthcare facility with more than 300 physicians and 2,400 employees purchased Kaspersky security licenses for 400 virtual desktops and 2,900 workstations. If the U.S. intelligence community's concerns about the potential security threats posed by Kaspersky products are accurate, then the use of Kaspersky products on U.S. critical infrastructure by the private sector also poses a legitimate threat to the public.¹⁸ However, the extent to which Kaspersky products are being used on critical nodes and computer servers across the U.S. critical infrastructure network, including natural gas facilities, dams, electrical plants, water distribution systems, and healthcare networks, or the U.S. election infrastructure is unclear. The presence of Kaspersky products at these facilities could pose a threat to our critical infrastructure.

NIST Cybersecurity Standards

The National Institute of Standards and Technology (NIST) cybersecurity framework, which is geared towards improving the cybersecurity practices of private-sector owners and operators of critical infrastructure in the United States, is used by 16 distinct infrastructure sectors.¹⁹ As stated on the agency's website, "this voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk."²⁰ Although it is extremely useful and was established with extensive input from the private sector, it is not mandatory.

Gartner Research found that only 30% of U.S. private organizations were using the NIST framework in 2015 and that the number was expected to increase to 50% by 2020. However, that still leaves half of

¹⁶ "DHS Statement on the Issuance of Binding Operational Directive 17-01," Department of Homeland Security, September 13, 2017, accessed here: <https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01>

¹⁷ See: Derek B. Johnson, "New federal contracting rule cuts off Kaspersky," *Federal Computer Week*, June 15, 2018, accessed here: <https://fcw.com/articles/2018/06/15/kaspersky-rule-contractors.aspx> and "Federal Acquisition Regulation; Use of Products and Services of Kaspersky Lab," Interim Rule, Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA), accessed here: <https://www.gpo.gov/fdsys/pkg/FR-2018-06-15/pdf/2018-12847.pdf>

¹⁸ See a list of Kaspersky's "Case Studies" here: <https://usa.kaspersky.com/enterprise-security/resources/case-studies>

¹⁹ "Critical Infrastructure Perspectives," National Institute of Standards and Technology, last updated March 1, 2018, accessed here: <https://www.nist.gov/cyberframework/perspectives/critical-infrastructure>

²⁰ "Cybersecurity Framework," National Institute of Standards and Technology, accessed here: <https://www.nist.gov/cyberframework>

U.S. industry not applying best practices or appropriate cybersecurity standards to their business operations, some of which provide critical services to the American public. This includes providing water, electricity, natural gas and other critical infrastructure services. In addition, Gartner Research found that less than 20 States had implemented NIST's Critical Infrastructure Framework.²¹

Local and State Cybersecurity Standards on the non-Bulk Electric System (BES)

The electric grid is comprised of three primary components, including generation, transmission and distribution. The Bulk Electric System (BES) is composed of the generation and transmission components. The North American Electric Reliability Corporation (NERC) develops reliability standards for the BES that are enforced by the Federal Energy Regulatory Commission (FERC). The distribution section of the grid, comprised of local utility companies and referred to as the non-BES portion of the grid, is regulated by local and state governments. Most often, however, security vulnerabilities on the electric grid have focused solely on the Bulk Electric System. Although it is the least regulated, the non-BES portion comprises 80% of the electric grid and distributes electricity directly to critical infrastructure components, including telecommunications networks, water systems and oil and gas pipelines. According to a recent National Academy of Sciences study on grid resilience, "To date, NERC has mandated nine cybersecurity standards as part of the overall mandatory standards it has established for the electric industry. These critical infrastructure protection (CIP) standards address the security of cyber assets essential to grid reliability. In addition to the cybersecurity standards from the Nuclear Regulatory Commission (NRC), these are the only mandatory cybersecurity standards for any of the critical infrastructure sectors across the United States (NERC, 2017)."²²

Those cybersecurity standards only apply to the Bulk Electric System portion of the power grid under federal regulations, not the non-BES portions regulated by State and local authorities. However, operational issues affecting the non-BES sector of the grid can have a cascading effect influencing the BES components of the electric grid as well. One case in which that impact was made clear was the September 2011 blackout in the Southwestern United States that left 2.7 million customers without power, including all of San Diego, and affected parts of Arizona, southern California, and Mexico. The power outage resulted in a loss of power to water and sewage pumping stations and disrupted airport operations and public transportation. This incident highlighted the security vulnerabilities of the non-BES that can affect the Bulk Electric System. In addition, as the smart grid expands into the non-BES sectors, potential cybersecurity vulnerabilities may proliferate into the non-BES portions of the electric grid.²³

The issues above outline some of the key cybersecurity-related areas we request GAO evaluate in a review of potential cybersecurity issues that may impact the critical infrastructure in the United States. We understand that GAO already has several cybersecurity reviews underway. However, the specific questions we are asking GAO to evaluate are distinct from those other requests and highly important.

In reviewing the cybersecurity of the electricity grid, please assess the following core issues:

- 1) Do electric grid utilities have appropriate numbers of qualified staff to provide cybersecurity services to help protect their critical networks?

²¹ "NIST Impacts: Cybersecurity," National Institute of Standards and Technology, accessed here: <https://www.nist.gov/industry-impacts/cybersecurity>

²² "Enhancing the Resilience of the Nation's Electricity System," National Academies Press, 2017, accessed here: <https://www.nap.edu/download/24836#>

²³ Andreas Mueller, Peter Liebert, and Austin Heyworth, "Keeping the Lights On: The Critical Role of U.S. States in Electrical Sector Cybersecurity," Truman Center, April 2017, accessed here: <http://trumancenter.org/wp-content/uploads/2017/05/cyber-paper-v10-and-final.pdf>

- 2) Identify whether BES and non-BES components of the electric grid are employing Kaspersky Lab products on their networks, have taken any actions to ascertain if Kaspersky products are being utilized on their networks, and whether they have implemented any plans to remove them.
- 3) Review whether the non-Bulk Electric System and BES-related components of the electric grid are employing appropriate NIST cybersecurity standards.
- 4) Evaluate the cybersecurity risks to the non-BES portions of the electricity grid and the cybersecurity practices implemented by the non-BES portion of the grid. This should include an appraisal of the level of cybersecurity awareness and training provided to all employees working in the public utility sector, not just cybersecurity professionals.
- 5) Provide recommendations based on your findings to help enhance the cybersecurity preparedness of America's critical infrastructures.

If you or your staff have any questions or to discuss this request in more detail please have your staff contact Douglas Pasternak of the Committee's Minority staff at (202) 225-6375.

Your assistance in this matter is greatly appreciated.

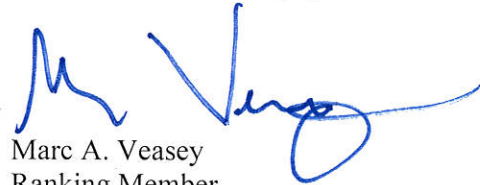
Sincerely,



Eddie Bernice Johnson
Ranking Member
Committee on Science, Space & Technology



Donald S. Beyer, Jr.
Ranking Member
Subcommittee on Oversight



Marc A. Veasey
Ranking Member
Subcommittee on Energy



Daniel W. Lipinski
Ranking Member
Subcommittee on Research and Technology