MARK E. GREEN, MD, TENNESSEE
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

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

February 17, 2023

The Honorable Kenneth L. Wainstein
Under Secretary for Intelligence and Analysis
U.S. Department of Homeland Security
Washington, DC 20528

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
Washington, DC 20528

Dear Under Secretary Wainstein and Director Easterly:

We write to request that the Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) and the Cybersecurity and Infrastructure Security Agency (CISA) brief us on threats posed by domestic violent extremists to our Nation's critical infrastructure, particularly the energy sector, and efforts by your respective agencies to defend against such attacks.

On February 8, 2023, DHS and the Federal Bureau of Investigation (FBI) issued a Joint Intelligence Bulletin (JIB) highlighting "the continued interest by some RMVEs [racially- or ethnically- motivated violent extremists] in conducting attacks against US critical infrastructure, particularly electrical infrastructure"[1] after law enforcement thwarted a plot hatched by two neo-Nazis to attack five electric facilities in Baltimore, Maryland.[2] One of the conspirators is a founding member of a paramilitary neo-Nazi group, the Atomwaffen Division, which has been implicated in violence across the country. The other told a law enforcement source that the plot would "completely destroy" the city, which is predominantly Black.[3] According to Assistant Attorney General for National Security Matthew G. Olsen, the two individuals were "[d]riven by their ideology of racially-motivated hatred" and "conspired to carry out attacks against critical

[1] Dep't of Homeland Sec. & FBI, *Disruption of Two Racially or Ethnically Motivated Violent Extremists Plotting To Attack the US Power Grid*, JOINT INTELLIGENCE BULLETIN, Feb. 8, 2023.
[2] Glenn Thrush & Michael Levenson, *Pair is Charged with Plotting to 'Destroy Baltimore' by Attacking Electrical Grid*, N.Y. TIMES (Feb. 6, 2023), https://www.nytimes.com/2023/02/06/us/politics/baltimore-electrical-grid-attack.html.
[3] *Id.*

infrastructure, specifically electrical substations, in furtherance of . . . racially or ethnically motivated violent extremist beliefs."[4]

The disrupted Baltimore plot is consistent with increased interest in attacks against the energy sector. Over the past five years, physical attacks at electrical facilities across the United States have been on the rise. In 2022 alone, the Department of Energy reported 163 direct physical attacks against electrical infrastructure across the country[5]— an all-time high that represents a 77 percent year-over-year increase in such attacks.[6] The physical attacks last year affected more than half of U.S. states and around 90,000 customers, putting hospitals, businesses, local governments, and American citizens at risk.[7] In just the past three months, our country has suffered from high-profile attacks against at least nine electrical substations,[8] including a firearm attack against two electrical substations in North Carolina that resulted in power outages affecting 45,000 homes and businesses,[9] and attacks against four power substations in Washington that cut power to thousands of residents over the Christmas holiday.[10]

While the motivation behind each attack is unknown, a 2022 study by the Project on Extremism at George Washington University found that RMVEs have been "laser-focused on conducting attacks on the energy sector."[11] Similarly, a DHS National Terrorism Advisory System (NTAS) Bulletin issued on November 30, 2022, advises that "[t]he United States remains in a heightened threat environment. Lone offenders and small groups motivated by a range of ideological beliefs and/or personal grievances continue to pose a persistent and lethal threat to the Homeland."[12]

Physical attacks on our grid infrastructure are not the only mechanism RMVEs could use to cause damage or disruption to energy reliability. The U.S. energy sector is also vulnerable to cyberattacks, as Russia and other foreign adversaries have demonstrated for many years. Multiple Federal agencies have warned about persistent cyber threats to the grid, including "multiple intrusion campaigns conducted by state-sponsored Russian cyber actors from 2011 to 2018" wherein hackers "gained remote access to U.S. and international Energy Sector networks,

---

[4] Dep't of Justice, *Maryland Woman and Florida Man Charged Federally for Conspiring to Destroy Energy Facilities*, Press Release, Feb. 6, 2023, https://www.justice.gov/usao-md/pr/maryland-woman-and-florida-man-face-federal-charges-conspiring-destroy-energy-facilities.
[5] Naureen S. Malik, *Attacks on US Power Grids Rose to All-Time High in 2022*, BLOOMBERG (Feb. 2, 2023), https://www.bloomberg.com/news/articles/2023-02-01/attacks-on-us-power-grids-rise-to-all-time-high-in-2022.
[6] *Id.*
[7] Michael Levenson, *Attacks on Electrical Substations Raise Alarm*, N.Y. TIMES (Feb. 4, 2023), https://www.nytimes.com/2023/02/04/us/electrical-substation-attacks-nc-wa.html.
[8] *Id.*
[9] Aaron Cooper & John Miller, *A Vulnerable Power Grid Is In the Crosshairs of Domestic Extremist Groups*, CNN (Feb. 4, 2023), https://www.cnn.com/2023/02/04/us/us-power-grid-attacks/index.html.
[10] Livia Albeck-Ripka, *Attacks on 4 Washington Substations Cut Power to Thousands, Officials Say*, N.Y. TIMES (Dec. 27, 2022), https://www.nytimes.com/2022/12/27/us/power-substation-attack-washington-state.html.
[11] ILANA KIRILL & BENNET CLIFFORD, MAYHEM, MURDER, AND MISDIRECTION: VIOLENT EXTREMIST ATTACK PLOTS AGAINST CRITICAL INFRASTRUCTURE IN THE UNITED STATES, 2016-2022 25 (2022).
[12] Dep't of Homeland Sec., *Summary of Terrorism Threat to the United States*, NATIONAL TERRORISM ADVISORY SYSTEM, Nov. 22, 2022, https://www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-november-30-2022.

deployed [industrial control system (ICS)]-focused malware, and collected and exfiltrated enterprise and ICS-related data."[13]

This threat activity has not waned. Just last week, cybersecurity firm Dragos said that a new, likely-Russian malware called PIPEDREAM came "the closest we've ever been" to having to take down "around a dozen" U.S. electric and liquid natural gas sites.[14] As RMVEs embrace the use of grid disruptions for ideological means, we cannot assume they will not seek to exploit cyber vulnerabilities—particularly where the malware and tactics used to carry such an exploit are known.

The February JIB issued after the Baltimore attack stressed the "importance of law enforcement and the public having awareness of the most common indicators of radicalization and mobilization to violence, which can be used to detect and thwart violent attacks."[15] According to the JIB, the FBI's Joint Terrorism Task Force "leverage[ed] state and local law enforcement partnerships" to disrupt the plot, highlighting the important role of coordinating efforts to combat threats of violence against critical infrastructure.[16]

DHS I&A is responsible for serving as a conduit for information sharing between the Intelligence Community and State, Local, Tribal, and Territorial (SLTT) governments, leveraging a network of fusion centers. Through these relationships, I&A can share threat information critical to situational awareness for Federal and SLTT governments.

Similarly, CISA is tasked with coordinating Federal efforts to secure all 16 sectors of critical infrastructure, including the energy sector, in preparing for, responding to, and building resilience against elevated threats. To carry out this mission, CISA relies on I&A to provide actionable, timely threat intelligence that it can use to drive effective, informed communication and coordination with sector owners and operators through designated Sector Risk Management Agencies—in this case, the Department of Energy.

Together, I&A and CISA have the tools, resources, intelligence, and expertise that can be brought to bear in protecting targeted energy infrastructure against domestic extremists. Given the alarming rise of domestic violent extremism and in attacks against critical infrastructure generally, and the energy sector in particular, I&A and CISA have essential roles in ensuring SLTTs are informed and prepared to prevent attacks against electrical facilities.

We appreciate your efforts to protect the Homeland and respectfully request a briefing on how I&A and CISA are working together and with partners to keep our critical infrastructure safe, your

---

[13] *Cybersecurity Advisory: Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector (Alert (AA22-083A)),* CISA, FBI, and Department of Energy Mar. 24, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-083a.

[14] Maggie Miller, "Russian-linked malware was close to putting U.S. electric facilities 'offline' last year," Politico, Feb. 14, 2023, https://www.politico.com/news/2023/02/14/russia-malware-electric-gas-facilities-00082675/.

[15] Dep't of Homeland Sec. & FBI, *Disruption of Two Racially or Ethnically Motivated Violent Extremists Plotting To Attack the US Power Grid*, JOINT INTELLIGENCE BULLETIN, Feb. 8, 2023.

[16] *Id.*

assessments on potential threats to the energy sector, and the role of racially- or ethnically-motivated violent extremism in perpetuating the threat. Additionally, we would like to understand evolving cybersecurity threats to the energy sector, such as the PIPEDREAM malware, and how domestic extremists might seek to exploit cyber vulnerabilities for ideological purposes.

Thank you for your attention to this matter.

Sincerely,

BENNIE G. THOMPSON
Ranking Member

ERIC SWALWELL
Ranking Member
Subcommittee on Cybersecurity and Infrastructure Protection

SETH MAGAZINER
Ranking Member
Subcommittee on Counterterrorism, Law Enforcement, and Intelligence