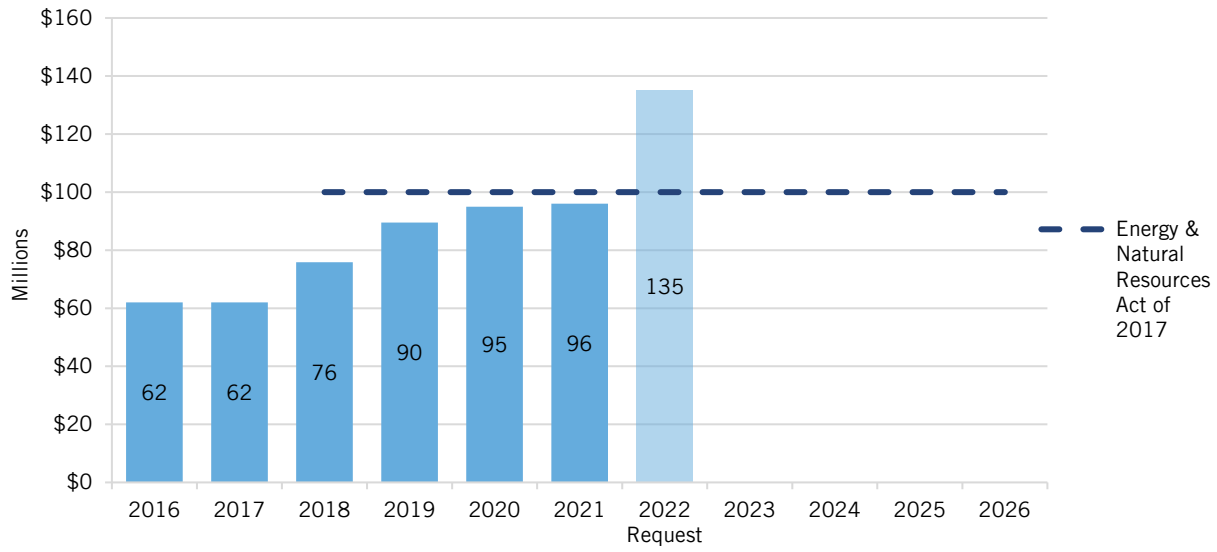
Federal Energy RD&D: Cybersecurity for Energy Systems

BY COLIN CUNLIFF AND LINH NGUYEN | JUNE 2021

The goal of the Cybersecurity for Energy Delivery Systems (CEDS) program is to reduce the risk of energy disruptions from cyber events. Through CEDS, the Department of Energy (DOE) directly collaborates with energy-sector utility owners, operators, and vendors to both strengthen the cybersecurity of critical energy infrastructure against current and future threats and mitigate vulnerabilities.[1]

Figure 1: Historical funding for CEDS research, development, and demonstration (RD&D)[2]



WHAT'S AT STAKE

The energy sector has in recent years been subjected to a dramatic increase in focused cyber probes, data exfiltration, and malware attacks. Previous rounds of threats have been aimed at information technology (IT) systems (e.g., email and business applications) at energy companies, but a new wave of cyberattacks is targeting operational technologies (OT), including software and hardware that directly control equipment on the grid. The cyberattack on the Ukrainian electricity distribution system in December 2015 caused the first-ever cyber-linked blackout—and demonstrated the vulnerability of power grids to cyber events.[3]

In March 2018, the Department of Homeland Security (DHS) accused Russian government cyber actors of targeting critical U.S. infrastructure, including the electrical grid and nuclear power plants, to steal data on several generation facilities.[4] And in March 2019, DOE reported that several counties in California, Utah, and Wyoming experienced a cyber event that caused interruptions of electrical system operations, marking the first successful cyberattack to disrupt U.S. grid operations.[5] The COVID-19 pandemic, which forced employees across the energy industry to work remotely, has created a unique opportunity for cybercriminals and led to an

unprecedented rise in cyberthreats to critical energy infrastructure. The major cyber hack on IT management software company SolarWinds in December 2020, which compromised major federal agencies like the Federal Energy Regulatory Commission and power utilities such as the New York Power Authority, underscores the dangers of cyberthreats to the grid and the need for action.[6]

The White House released the *National Cyber Strategy of the United States* in September 2018 to help federal agencies coordinate efforts, define roles and responsibilities, and prioritize cybersecurity efforts.[7] In June 2019, the Senate Energy and Natural Resources committee approved the Securing Energy Infrastructure Act to remove vulnerabilities in digital software systems hackers could exploit to access the energy grid.[8] Recent events indicate the need for strong federal support to coordinate efforts between the intelligence community and energy utilities to improve cybersecurity of critical energy systems infrastructure.[9] The cybersecurity landscape is characterized by rapidly evolving threats and vulnerabilities juxtaposed against grid modernization and the convergence of utility OT and IT systems. Additional RD&D is needed to work with industry partners to create cyberthreat detection, prevention, and mitigation tools for energy delivery systems.

The Fixing America's Surface Transportation Act of 2015 provides DOE the authority to protect and restore the power grid during a grid security emergency, including grid cyberattacks. The act directs DOE to work with DHS, in collaboration with infrastructure owners and operators, to identify vulnerabilities, improve emergency preparedness, and manage cyber incidents.[10] The Senate Energy and Natural Resources Act of 2017 (S. 1460) establishes a program for energy sector cybersecurity RD&D and authorizes $65 million annually for FY 2018 through FY 2026 for the program to be carried out by DOE. The bill also authorizes $15 million annually for an energy sector component testing for cyber resilience program, $10 million annually for an energy sector operational support for cyber resilience program, and $10 million annually for an advanced energy security program for FY 2018 through FY 2026.[11]

Figure 1 shows historical DOE investment in CEDS RD&D for FY 2016 through FY 2021 and the FY 2022 budget request. The dashed blue line shows authorized funding levels from the Senate Energy and Natural Resources Act (S. 1460), which was introduced in 2017 but was unable to pass the Senate and ultimately did not become law.

Cybersecurity RD&D Activities

In FY 2021, CEDS focused on these key RD&D activities:[12]

- **Cyber Analytic Tools and Techniques™ 2.0 (CATT™ 2.0)** provide situational awareness and actionable information to support discovery and mitigation of cyberthreats to the United States' energy infrastructure and operational technology environment, with classified threat information owned by the U.S. government.

- **Cybersecurity for Operational Technology Environments (CyOTE™)** support demonstration of data sharing and analysis in the OT environment to help utilities address the challenges of collecting data on OT networks.

- **Cybersecurity Risk Information Sharing Program (CRISP)** is a public-private partnership between DOE and energy-sector partners both to facilitate the timely bidirectional sharing of unclassified and classified threat information, and to develop situational awareness tools that enhance the sector's ability to identify, prioritize, and coordinate the protection of critical infrastructure.

- **Cybersecurity Capability Maturity Model (C2M2)** helps private-sector owners and operators better evaluate their cybersecurity capabilities, and prioritize and improve their cybersecurity activities.

Key Elements of the FY 2022 Budget Proposal[13]

The Cybersecurity, Energy Security, and Emergency Response (CESER) office houses the Risk Management Technology and Tools (RMT) program, formerly the Cybersecurity for Energy Delivery Systems (CEDS) R&D program. CESER also houses the Infrastructure Security and Energy Restoration (ISER), an energy-sector emergency-support function that does not include R&D activities. Elements of RMT's proposed budget include:

- Continued funding for existing cybersecurity projects, including CyOTE™ and C2M2.
- Increase in funding for the Cybersecurity Testing for Industrial Control Systems (CyTRICS), which focuses on cyber supply chain vulnerability testing and component design and manufacturing improvements. Funding will support two additional testing labs (NREL and ORNL) and scale up cyber supply chain vulnerability testing for the digital components of renewables and distributed energy resources.
- Funding for RD&D of next-generation cyber information sharing tools and technologies to enhance the ability to detect cyberthreats.

Acknowledgments

The authors wish to thank David M. Hart for providing input to this report. Any errors or omissions are the authors' alone.

About the Authors

Colin Cunliff is a senior policy analyst for clean energy innovation with ITIF. He previously worked at the U.S. Department of Energy on energy sector resilience and emissions mitigation. He holds a Ph.D. in physics from the University of California, Davis.

Linh Nguyen is a research assistant for clean energy innovation with ITIF. She previously worked for Climate Advisers and Resource Energy. Linh holds a master's degree in energy policy from Johns Hopkins University.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent, nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized by its peers in the think tank community as the global center of excellence for science and technology policy, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

For more information, visit us at www.itif.org.

ENDNOTES

1. DOE, "FY 2021 Congressional Budget Request," Volume 3 Part 1, DOE/CF-0163 (Washington, D.C.: DOE Chief Financial Officer, February 2020), 315–346, https://www.energy.gov/sites/prod/files/2020/02/f72/doe-fy2021-budget-volume-3-part-1_1.pdf.
2. DOE, FY 2021 Congressional Budget Justification Volume 3 Part 1, 321; Energy and Natural Resources Act of 2017, S.1460, 115th Cong. (2017); Energy and Natural Resources Act of 2017, S.1460, 115th Cong. (2017).
3. For a description of the Ukraine hacking and its implications for the U.S. electric sector, see the *E&E* News Special Report by Peter Behr and Blake Sobczak, "The Hack" (*E&E News* Special Report, Washington, D.C.: July 2016), https://www.eenews.net/special_reports/the_hack.
4. Blake Sobczak, "U.S. ties Russia to energy-sector hacks," *E&E News* (March 16, 2018), https://www.eenews.net/stories/1060076555/; Department of Homeland Security, "Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure" (Washington, D.C.: March 15, 2018), https://www.us-cert.gov/ncas/alerts/TA18-074A.
5. Blake Sobczak, "Experts assess damage after first cyberattack on U.S. grid," *E&E News* (May 2019), https://www.eenews.net/stories/1060281821; DOE, "OE-417 Electric Emergency and Disturbance Report - Calendar Year 2019" (DOE, April), https://www.oe.netl.doe.gov/download.aspx?type=OE417PDF&ID=79.
6. Maggie Miller, "Experts see 'unprecedented' increase in hackers targeting electric grid," *The Hill* (April 2021), https://thehill.com/policy/cybersecurity/548051-experts-see-unprecedented-increase-in-hackers-targeting-electric-grid?rl=1; Christian Vasquez, "Huge federal hack ripples across energy industry," *E&E News* (December 2020), https://www.eenews.net/stories/1063720933; Maggie

Miller, "Officials warn of increasing cyber threats to critical infrastructure during pandemic," *The Hill* (August 2020), https://thehill.com/policy/cybersecurity/510755-officials-warn-of-increasing-foreign-cyber-threats-to-electric-grid?rl=1.

7. The White House, "National Cyber Strategy of the United States of America" (White House, September 2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
8. Securing Energy Infrastructure Act, S.174, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/senate-bill/174/.
9. Jeremy Dillon, "Perry Told to Do More on Grid Cybersecurity After Russian Hacks," *Roll Call* (March 20, 2018), https://www.rollcall.com/news/policy/perry-told-grid-cybersecurity-russian-hacks.
10. Fixing America's Surface Transportation Act of 2015, H.R. 22, 114th Cong. (2015).
11. Energy and Natural Resources Act of 2017, S.1460, 115th Cong. (2017).
12. DOE, "FY 2021 Congressional Budget Justification," Volume 3 Part 1, 318–320 (DOE Chief Financial Officer DOE/CF-0163, February 2020), https://www.energy.gov/sites/prod/files/2018/03/f49/DOE-FY2019-Budget-Volume-3-Part-1_0.pdf; DOE, "Energy Sector Cybersecurity Preparedness," accessed March 6, 2020, https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity; DOE, "Cybersecurity Risk Information Sharing Program (CRISP)," accessed March 6, 2020, https://www.energy.gov/sites/prod/files/2018/09/f55/CRISP%20Fact%20Sheet.pdf.
13. DOE, "FY 2022 Congressional Budget Justification" Volume 3 Part 1, 303, (DOE Chief Financial Officer DOE/CF-0173, June 2021), 75-80, https://www.energy.gov/sites/default/files/2021-06/doe-fy2022-budget-volume-3.1-v2.pdf.