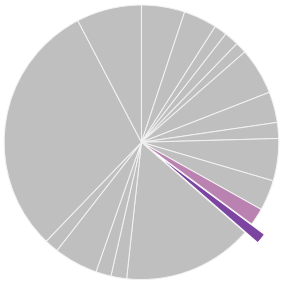
Federal Energy R&D:
Cybersecurity for Energy Systems

BY COLIN CUNLIFF AND BATT ODGEREL | MARCH 2020

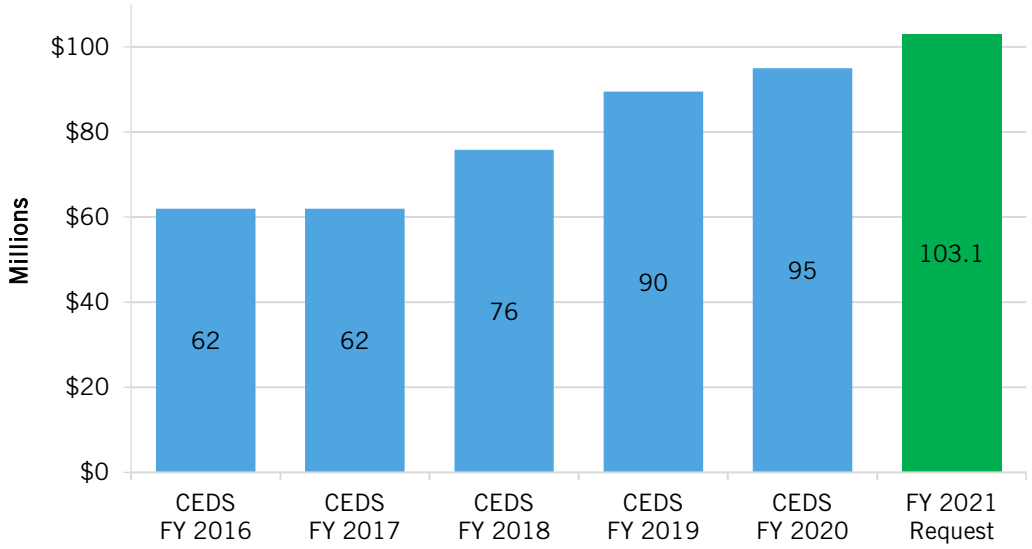
This briefing is part of a series on the U.S. energy budget. See: itif.org/energy-budget.



Cyber (purple)
Electricity TS&D (light purple)
Energy R&D (gray)

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 strengthen the cybersecurity of critical energy infrastructure against current and future threats and mitigate vulnerabilities.[1]

Figure 1: The FY 2021 budget request would increase funding for CEDS R&D by 9 percent[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 disrupting U.S. grid operations.[5]

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.[6] 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.[7] 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.[8] 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 research, development, and demonstration (RD&D) is needed to work with industry partners to create cyberthreat detection, prevention, and mitigation tools for energy delivery systems.

Cybersecurity R&D Activities

In FY 2020, CEDS focused on these key research activities:[9]

- **Cyber Analytic Tools and Techniques™ 2.0 (CATT™ 2.0)** provides situational awareness and actionable information to support discovery and mitigation of cyber threats 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™)** supports 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 to facilitate the timely bidirectional sharing of unclassified and classified threat information, and 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 2021 Budget Proposal

The Cybersecurity, Energy Security, and Emergency Response (CESER) office houses the CEDS R&D program, as well as the Infrastructure Security and Energy Restoration (ISER), an energy-sector emergency-support function that does not include R&D activities. Elements of CEDS's proposed budget include:[10]

- Continued funding for the Advanced Threat Mitigation initiatives supporting existing cybersecurity projects, including CATT™, CyOTE™, and C2M2.
- New funding of $22 million to develop cybersecurity solutions for the next generation of advanced tools and technologies.
- New funding of $12.1 million for demonstration of cybersecurity solutions for energy systems that support military and government installations.
- No additional funding for two FY 2020 congressionally directed programs: DarkNet project, which is focused on optical fibers and communication technologies, and Consequence-driven Cyber-informed Engineering project, which supports consequence prioritization processes to simplify and isolate automated systems; and no additional funding for advanced cyber and cyber-physical solutions for distribution and municipal utilities.

ENDNOTES

1. Department of Energy, "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.
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. 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.
7. Securing Energy Infrastructure Act, S.174, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/senate-bill/174/.
8. 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.
9. 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.

10 . DOE, FY 2021 Congressional Budget Justification Volume 3, Part 1, 23–29.

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 the Information Technology and Innovation Foundation. He previously worked at the U.S. Department of Energy (DOE) Office of Energy Policy and Systems Analysis (EPSA), with a portfolio focused on energy sector resilience and emissions mitigation. He holds a Ph.D. in physics from the University of California, Davis.

Batt Odgerel is a policy fellow for clean energy innovation at the Information Technology and Innovation Foundation. He previously worked for the Energy Policy Research Foundation (EPRINC) and Smart Electric Power Alliance (SEPA). Batt holds a master's degree in energy policy from Johns Hopkins University's School of Advanced International Studies, Washington, D.C.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as the world's leading science and technology think tank, 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.