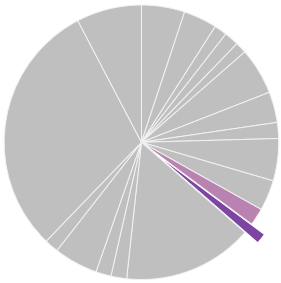
Federal Energy R&D:
Cybersecurity for Energy Systems

BY COLIN CUNLIFF | APRIL 2019

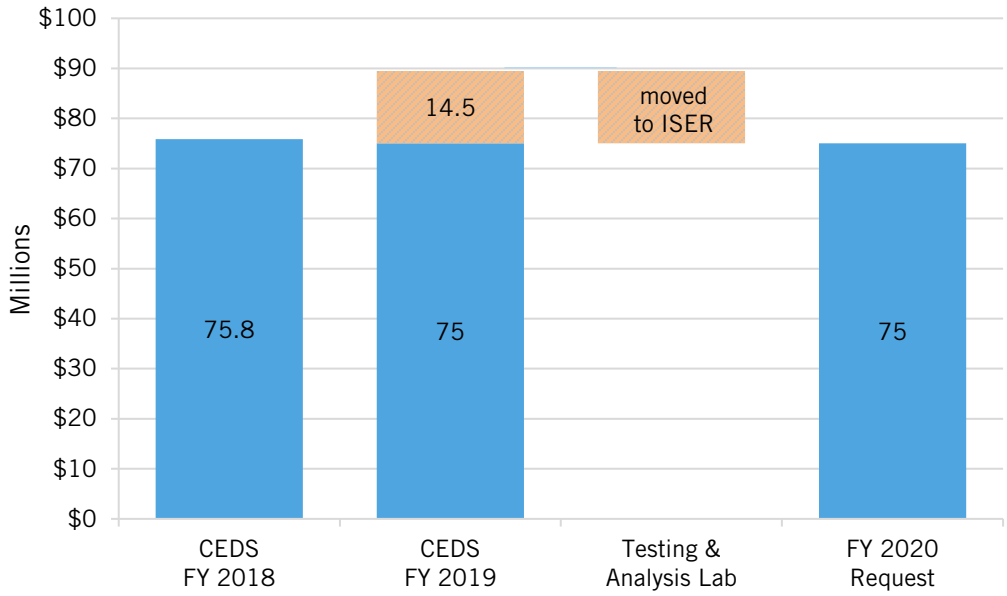
This briefing is part of a series on the U.S. energy budget. See: itif.org/energy-budget.



Cyber (purple)
Electricity TS&D
Energy R&D (light 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.[1]

Figure 1: The FY 2020 Budget Request Would Maintain Flat Funding for Cybersecurity for Energy Delivery Systems R&D.[2]



What's At Stake

The energy sector has been subjected to a dramatic increase in focused cyber probes, data exfiltration, and malware attacks in recent years. 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 operating 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, highlighting the need for greater cybersecurity.[4] In September 2018, the White House released the *National Cyber Strategy of the United States* to help federal agencies coordinate efforts, define roles and responsibilities, and prioritize cybersecurity efforts.[5] 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.[6]

Cybersecurity R&D Activities

In FY 2019, CEDS focused on these key research activities:[7]

- **Cybersecurity Risk Information Sharing Program (CRISP)** develops situational-awareness tools and facilitates the near-real-time sharing of cyber-threat information with energy owners and operators—such that they can promptly analyze the data and receive machine-to-machine mitigation measures.
- **Cyber Analytics Tools and Techniques (CATT)** supports utility data migration into the Intelligence Community Information Technology Environment (IC ITE), which provides a common platform for the intelligence community to easily and securely share analytic tools and technologies, information, and resources.
- **Cybersecurity for the Operational Technology Environment (CYOTE) Pilot** monitors utility data in the complex OT environment to identify malicious actions and aims to design an approach for collecting and sharing OT data.
- **Advanced Industrial Control System Analysis Center** develops capabilities to assess energy components and energy sector supply chain for vulnerabilities and to mitigate and respond to system threats.

Additionally, CEDS previously funded an energy delivery system testing and analysis laboratory (orange in figure 1) that is being moved to ISER.

Key Elements of the FY 2020 Budget Proposal

The new Cybersecurity, Energy Security, and Emergency Response (CESER) office houses the Cybersecurity for Energy Delivery Systems (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:[8]

- Transferring the $14.5 million energy delivery system testing and analysis laboratory from CEDS to ISER for operationalizing the results of CEDS R&D activities;
- Discontinuing the DarkNet project to secure communications based on optical fibers;

- Discontinuing the Automated System R&D project to isolate automated systems and remove vulnerabilities;

- New funding for the Advanced Threat Mitigation initiative that aims to detect and mitigate high-risk threats faster by improving the speed and effectiveness of public-private information sharing;

- New funding that supports demonstrating and refining cybersecurity solutions for energy sector entities that provide power to military and government installations.

ENDNOTES

1. DOE, "FY 2020 Congressional Budget Request," Volume 3 Part 1, DOE/CF-0152 (Washington, D.C.: DOE Chief Financial Officer, March 2019), 65-77, https://www.energy.gov/sites/prod/files/2019/03/f61/doe-fy2020-budget-volume-3-part-1_2.pdf.
2. DOE, FY 2020 Congressional Budget Justification Volume 3 Part 1, 75.
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. 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. 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.
6. Jeremy Dillon, "Perry Told to Do More on Grid Cybersecurity After Russian Hacks," *Roll Call* (Washington, D.C.: March 20, 2018), https://www.rollcall.com/news/policy/perry-told-grid-cybersecurity-russian-hacks.
7. DOE, "FY 2019 Congressional Budget Justification," Volume 3 Part 1, 63-69, (DOE Chief Financial Officer DOE/CF-0140, March 2018), https://www.energy.gov/sites/prod/files/2018/03/f49/DOE-FY2019-Budget-Volume-3-Part-1_0.pdf; DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER), "From Innovation to Practice: Re-Designing Energy Delivery Systems to Survive Cyber Attacks," (DOE CESER, July 2018), https://www.energy.gov/sites/prod/files/2018/09/f55/CEDS%20From%20Innovation%20to%20Practice%20FINAL_0.pdf.
8 . DOE, FY 2020 Congressional Budget Justification Volume 3, Part 1, 75. See also DOE Office of Electricity Delivery and Energy Reliability, "Multiyear Plan for Energy Sector Cybersecurity," (DOE OE, March 2018), https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf.

ACKNOWLEDGMENTS

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

ABOUT THE AUTHOR

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.

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 one of the world's leading science and technology think tanks, 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.