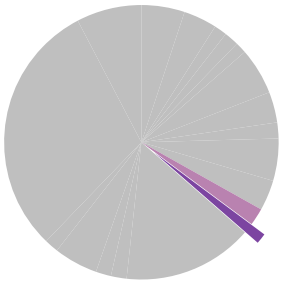
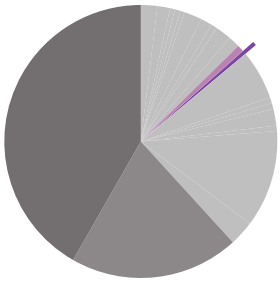
Federal Energy R&D:
Cybersecurity for Energy Systems

BY DAVID M. HART AND COLIN CUNLIFF | APRIL 2018

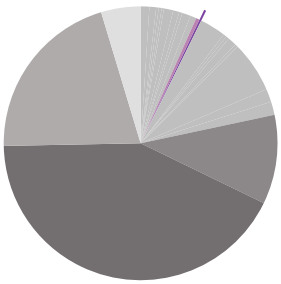
This briefing is part of a series on the U.S. energy budget. See: itif.org/energy-budget.



Cyber (purple)
Office of Electricity
Energy R&D (light gray)



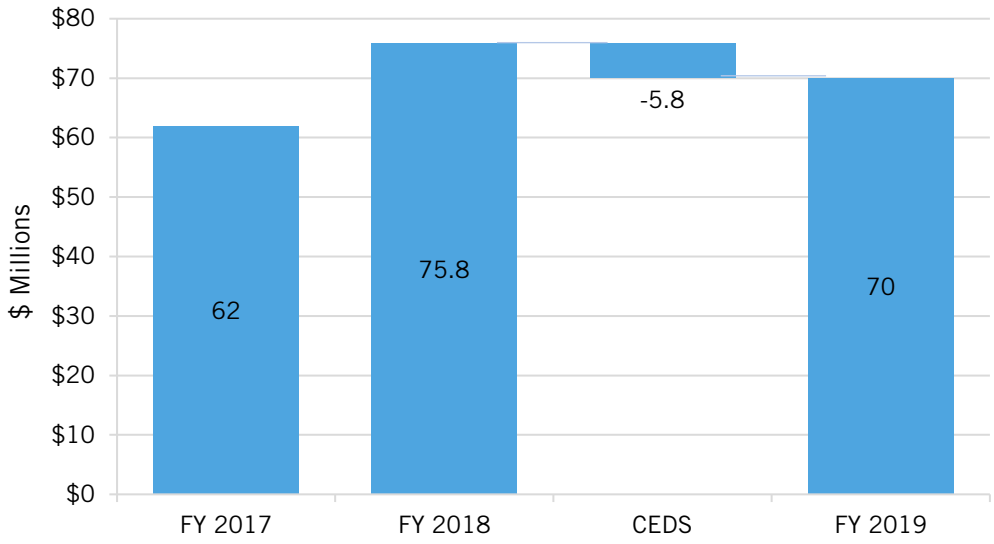
Cyber & Energy R&D
Basic Science R&D
Defense R&D



Cyber & Energy
Basic Science
Defense
Environ Mngmt
Other

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.

Figure 1: The FY 2019 Budget Request Would Cut Cybersecurity for Energy-delivery Systems R&D by 8 Percent



What's At Risk

The energy sector has been subjected to a dramatic increase in focused cyber probes, data exfiltration, and malware attacks in recent years.[1] 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.[2]

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.[3] Although the Trump

Administration is proposing an increase in grid cybersecurity R&D over FY 2017 levels, in light of the FY 2018 budget agreement, the administration's proposal would now actually yield a net reduction in this line item. Many legislators believe recent events indicate the need for an even greater effort than that which they supported in FY 2018.[4]

Cybersecurity R&D Activities

CEDS focuses on these key research activities:

- **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)** improves the speed, value, and cost of CRISP analyses, reports, and mitigation, while working to add new threat-detection capabilities to the CRISP platform.

- **Cybersecurity for the Operational Technology Environment (CYOTE)** monitors utility data in the complex OT environment to identify malicious actions. CYOTE is currently piloting two-way OT data sharing and analysis with four electric utilities, while also working to identify pathways hackers could use to compromise utility OT systems.

- **Cybersecurity Capability Maturity Model (C2M2)** works in partnership with utilities to help asset owners and operators assess their capabilities and improve their cybersecurity postures.

Key Elements of the FY 2019 Budget Proposal

The FY 2019 budget request proposes a new program, the Cybersecurity, Energy Security, and Emergency Response (CESER) office, and moves the CEDS research program from the Office of Electricity Delivery and Energy Reliability (OE) into CESER. The budget also moves the Infrastructure Security and Energy Restoration (ISER) program—an energy-sector emergency-support function that does not include R&D activities—into CESER. Elements of CESER's proposed budget include:

- New funding for Advanced Industrial Control Systems Analysis Center to model and assess energy-sector cyber-supply-chain components for vulnerabilities, through a public-private partnership between the National Laboratories and private-sector partners.[5]

- Increased funding for the development of cybersecurity tools, including cyber sensors, for information data sharing and data analytics, including continued support for C2M2.

- Reduced funding for the Virtual Energy Sector Advanced Digital Forensics Analysis Platform, which provides a virtual sandbox for executing untested code and programs. The platform is being developed for transition to the private sector, with the ultimate goal of becoming self-sustaining.

ENDNOTES

1. DOE, "FY 2017 Congressional Budget Justification," Volume 3, p 353 (Washington, D.C.: DOE/CFO, 2016).
2. 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.
3. 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.
4. 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.
5. DOE, "FY 2019 Congressional Budget Justification," volume 3 part 1, DOE/CF-0140 (Washington, D.C.: DOE/CFO, March 2018) 64 https://www.energy.gov/sites/prod/files/2018/03/f49/DOE-FY2019-Budget-Volume-3-Part-1_0.pdf.

ABOUT THE AUTHORS

David M. Hart is a senior fellow at ITIF and professor of public policy and director of the Center for Science, Technology, and Innovation Policy at George Mason University's Schar School of Policy and Government.

Colin Cunliff is a policy analyst for clean energy innovation at ITIF.

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.