The security and resiliency of the U.S. energy sector is one of today's most important and complex national security issues. A widespread disruption to the energy sector could impact our energy supplies, economy, and daily lives. At the U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), ensuring cyber resilience for the nation's critical energy infrastructure is our top priority. As we build the modern, clean energy grid of the future, CESER is advancing collective preparedness and response to a growing landscape of new threats, technologies, and trends. Through public-private collaboration, CESER remains committed to protecting the energy supply that millions of Americans rely on every day.

CESER's Cybersecurity Priorities

Priority 1

Increase Cyber Visibility of Critical Energy Systems and Networks

We are continuing to advance technologies and systems that increase the visibility of cyber threats targeting energy companies' industrial controls systems across the nation. With enhanced cyber visibility, detection, monitoring capabilities, we can respond and curtail confront malicious cyberattacks before they compromise critical systems.

Priority 2

Build Security Into Future, Clean Energy Grid

As we transition to a 100% clean energy economy, it is critical to build effective cybersecurity measures into the evolving grid to ensure a reliable flow of energy across the nation. CESER and its stakeholders are ensuring renewable technologies – from wind to solar – will be able to deliver a high volume of energy while addressing grid vulnerabilities.

Priority 3

Manage Supply Chain Risks in Digital Components of Nation's Critical Energy Infrastructure

Digital components in our national critical infrastructure are increasingly becoming the strategic target for adversary nations. We're partnering across the energy sector to identify high priority digital components prevalent in the nation's critical energy systems, perform expert testing, and share information about vulnerabilities in the digital supply chain.

Priority 4

Strengthen the Current and Future Energy Cyber Workforce

A highly skilled cybersecurity workforce across the energy sector is critical to protecting the nation's energy systems. CESER is developing exercises, trainings, and resources that improve preparedness and coordination across governments and industry, while promoting a robust cybersecurity education for the next generation of cyber professionals. We are also utilizing Cyber-Informed Engineering – a methodology to ensure that cybersecurity is a core component in technologies from ideation to deployment.

Priority 5

Establish Policies, Procedures, and Capabilities to Enable Cyber Preparedness and Incident Response

Through risk-based energy security planning and strategic partnerships across a broad range of stakeholders, CESER is establishing policies, procedures, and capabilities needed to improve energy sector cyber resilience, address new threats, conduct more efficient and effective response, and mitigate disruptions to energy infrastructure in case of a cyberattack.

Our Priorities in Practice

- In April 2021, the Biden Administration kicked off a 100-Day Action Plan to improve the cybersecurity of the U.S. electricity subsector led by CESER, the Cybersecurity and Infrastructure Security Agency (CISA), and the electricity industry. With more than 150 electric utilities – serving almost 90 million Americans – already on board, this is a major step forward to enhancing the visibility, detection, and monitoring of critical networks across the country. Read a progress report here.
- In July 2021, DOE announced the release of C2M2 2.0, a tool designed to help energy sector organizations understand cyber risks to their IT and OT systems and measure the maturity of their cybersecurity capabilities. The updated model reflects today's threat landscape, addressing new technologies like cloud and AI, as well as evolving threats like ransomware and supply chain security. Learn more on the C2M2 page here.
- In 2020 and 2021, DOE's Cyber Testing for Resilient Industrial Control Systems (CyTRICS) program announced partnerships with several large manufacturers including, Hitachi ABB Power Grids, Schweitzer Engineering Laboratories, and Schneider Electric, to advance the cybersecurity of their grid components. Learn more about the CyTRICS program here.
- In 2021, DOE's cyber workforce development program, CyberForce, grew to include two virtual competitions, a webinar series, a virtual career fair, and an online workforce portal – in addition to the primary CyberForce Competition. The expanded program provides opportunities for students of all backgrounds to hone their cyber skills.

U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response