CESER Blueprint

January 2021

U.S. DEPARTMENT OF ENERGY

OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Introduction

In 2018, the U.S. Department of Energy (DOE) established the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to elevate the Department's energy security responsibilities and safeguard against growing and evolving cyber and physical threats to U.S. critical energy infrastructure. CESER focuses on addressing these threats and engaging across industry, government, and academia to secure energy infrastructure against all hazards; reduce the risk of disruptive events; and respond to energy disruptions that could have devastating effects on national security, public health and safety, or the U.S. economy. Consistent with these priorities, the CESER team is pleased to introduce this Blueprint to guide its support in addressing the most compelling energy and cybersecurity challenges facing the sector.

Threats and Trends in the Energy Sector

Cybersecurity for critical infrastructure, particularly the energy sector, is one of the Nation's most important and complex national security challenges. Cybersecurity can only be effectively addressed through partnerships among a broad set of stakeholders, including all levels of government, private industry, and academia. CESER leads the building, maintaining, and operationalizing of these trusted partnerships to increase the cybersecurity of this critical infrastructure for the energy sector.

- The Nation's energy infrastructure and digital supply chain present a key target for cyber compromise, and the frequency and sophistication of cyber threats is increasing, including from nation-state actors.
- Energy systems are geographically dispersed, increasingly interconnected, and interdependent across multiple States, companies, and sectors, creating a multi-threat environment with the potential for cascading impacts during a disruption.
- Technological innovation and increasing connectivity are rapidly changing the risk posture for the energy sector. These trends have been accelerated by the global pandemic and resulting push for remote operation of geographically dispersed infrastructure.
- Energy sector companies are highly heterogenous; entities vary greatly in size, resourcing, and maturity level in capability to detect, deter, and mitigate cyber threats.

All segments of the energy sector face evolving physical threats that if combined with a cyber-attack could further degrade system reliability. Communities nationwide are experiencing the impacts of a changing climate and increasing natural hazards, such as wildfires and hurricanes, which have affected millions of energy customers in the United States. Compelled to action, State policymakers are actively exploring and adopting energy policies to encourage innovation, fairness and equity, energy economic development, and energy efficiency, all of which have energy security and cybersecurity implications.

CESER's Distinct Roles

CESER provides capabilities and support to energy sector partners to advance critical energy infrastructure security and resilience from all-hazards and manages key DOE authorities and responsibilities. These include serving as the Sector-Specific Agency (SSA) for the energy sector, as the coordinating agency for Emergency Support Function (ESF) #12-Energy under the National Response Framework, and fulfilling DOE responsibilities under the Fixing America's Surface Transportation (FAST) Act. True public-private partnership is integral to CESER's objectives. CESER's partnerships—with energy owners and operators, manufacturers, and trade associations; with other Federal agencies; across States, local governments, tribes, territories; with academia, National Labs, and the research community; and with the energy information sharing and analysis centers (ISACs)—help to advance collective preparedness and response to the growing landscape of threats, technology development, and energy system trends.

CESER's Progress

Since its inception, CESER has made notable progress that is rooted in the strategic partnerships it has fostered across the energy sector in executing its mission. In 2020, CESER:

- Ensured the reliability of critical energy infrastructure during the COVID-19 pandemic, in close coordination with the States and energy system owners and operators.
- Supported the energy sector's emergency response to a record number of hurricanes.
- Initiated a Department-wide cyber vulnerability testing program, leveraging unparalleled technical expertise from the National Labs, to assess digital components in energy systems. The program has participation agreements with five manufacturers and asset owners and is testing components of priority policy and security importance.
- Initiated the Energy Sector Pathfinder, in partnership with industry and the Department of Defense (DOD), Department of Homeland Security (DHS), and Federal Bureau of Investigation (FBI), to pilot and exercise increased operational coordination in cybersecurity between government and industry.
- Updated the energy sector's list of entities at greatest risk of attacks that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security (Section 9 entities) for the first time in seven years to include a representative segment of all energy subsectors and align to DOD defense-critical facilities.
- Completed 20 research and development (R&D) projects and launched seven new projects along with transitioning seven technologies into practice at energy companies.
- Launched the Operational Technology (OT) Defender Fellowship. This program offers middle- and senior-level OT security managers in the U.S. energy sector an opportunity to more fully understand the cyber strategies and tactics that adversarial state and non-state actors use in targeting U.S. energy infrastructure, in concert with our partners at Idaho National Laboratory and the Foundation for Defense of Democracies.

- Launched the Securing Energy Infrastructure Executive Task Force to convene key stakeholders from all levels of government, industry, academia, and the National Labs to jointly address priority technical vulnerabilities in energy systems.
- Identified use cases and developed tools to enhance detection of malicious cyber activity in OT networks and expanded tools to include application in the wind industry.

CESER also built capacity across the energy sector to mature preparedness and response efforts and develop the energy and cyber workforce:

- 450 energy sector officials engaged in CESER natural disaster and cyber exercises.
- 1,500 State energy officials, governors, energy advisors, public utility commissioners, State legislators, and emergency managers participated in CESER-supported events and training for energy and cyber-security planning.
- 145 cybersecurity experts from 75 electricity, oil, and gas sector companies participated in updating and validating the Cybersecurity Capability Maturity Model (C2M2).
- More than 200 university students from 36 States participated in the CyberForce Competition™.

Looking Ahead

CESER is continuously working to deliver value to its partners in managing the most compelling energy and cyber-security challenges facing the sector. This Blueprint is based on inputs and insights from CESER's partners and will help guide CESER's efforts. The five strategic goals and core objectives outline a foundation to align strategic investment, present areas of partnership, and measure collective progress into the future.

CESER Mission

To enhance the security of U.S. critical energy infrastructure to all hazards, mitigate the impacts of disruptive events and risk to the sector overall through preparedness and innovation, and respond to and facilitate recovery from energy disruptions in collaboration with other Federal agencies, the private sector, and State, local, tribal, and territory governments.

Strategic Goals and Objectives

The CESER Blueprint builds on existing programs and encompasses what CESER deems most timely and relevant, while also providing flexibility for the incorporation of new and emerging priorities. Most importantly, the five goals and objectives in this Blueprint endeavor to reflect the mission imperatives of industry and government partners from across the energy sector in working with CESER.

CESER's Blueprint comprises the following goals:

1. Advance cyber discovery, vulnerability assessment, and rapid risk mitigation.
2. Pursue game-changing R&D and technology transition.
3. Build capacity in the energy sector to understand risks, assess priorities, and identify cost-effective security and resilience improvements.
4. Enhance sector-wide situational awareness to inform decision-making in the energy sector.
5. Coordinate effective and efficient emergency response and recovery efforts.

GOAL 1: Advance cyber discovery, vulnerability assessment, and rapid risk mitigation

Partnering with the energy sector, CESER spearheads the development of tools and capabilities to understand and proactively address cyber threats and vulnerabilities that could disrupt or degrade critical U.S. energy infrastructure. Maturing the ability for early detection of malicious activity, compromised devices, and attack campaign indicators is a critical priority. CESER is positioned to collect sector-wide industry requirements, bring actionable cyber threat intelligence to sector partners to increase sector-wide awareness of emerging cyber threats, enhance federal-wide operational coordination in cyber among government and industry, and provide technical expertise to develop and test cyber mitigation approaches.

Core Objectives

- Discover cyber vulnerabilities in energy infrastructure through digital component testing and collaborate with industry to address high priority vulnerabilities.
- Build capacity and operationalize cyber technologies and capabilities to detect and isolate advanced threats and provide related mitigation and recovery strategies.
- Evaluate, validate, and verify mitigative solutions and assess the potential consequences of an adversary successfully exploiting vulnerabilities in energy sector networks.
- Proactively identify malicious cyber activity (i.e., adversaries' tactics, techniques, and procedures to infiltrate, conduct espionage on, and deliver effects) in order to disrupt and prevent cyber-attacks on critical energy sector infrastructure and operations.
- Provide intelligence-informed cyber threat analysis to the energy sector that includes context around the significance of the tactics, techniques, and procedures being shared; how that analysis aligns to energy systems; and what energy sector entities can do to mitigate.
- Coordinate across key energy sector industry and government stakeholders to increase and enhance operational coordination in cybersecurity.

GOAL 2: Pursue game-changing R&D and technology transition

CESER identifies technology areas ripe for energy and cyber security innovation and pursues R&D that meets urgent gaps identified by infrastructure owners and operators while evolving critical energy systems to be inherently resilient to novel threats. CESER supports a robust portfolio of highly collaborative R&D by teaming with the Nation's best minds and resources from the National Laboratories, equipment vendors and manufacturers, owners and operators, academia, and other government agencies. CESER's focus will be on early-stage R&D and emerging technologies, where the private sector has a limited business case, and provide support to transition novel tools and capabilities for adoption by the energy sector.

Core Objectives

- Competitively fund strategic R&D that meets specific industry needs and targets novel technology development beyond today's challenges, focusing investment both on near-term goals that allow for demonstration of products and services needed by owners and operators, vendors, and manufacturers today; and long-term goals that leverage National Lab capabilities and industry innovations to revolutionize cyber systems and capabilities.
- Coordinate with the DOE applied technology program offices to enhance energy and cyber security of clean, electric vehicle, and renewable energy research, development, and innovation efforts.

- Invest in research infrastructure—such as testing platforms, robust datasets, and test infrastructure—to enable testing and demonstration of new energy security technologies, lower per-project costs, and enable the sector to efficiently transition novel technology into practice.
- Establish a network of university-based, regional electric power cybersecurity R&D centers to develop self-healing and autonomous systems, support workforce development, and address the distinctive characteristics of regional energy systems.
- Collaborate with other DOE offices, Federal agencies, National Laboratories, States, and industry to transition innovative technologies, guidance, and practices to enhance energy company operations.

GOAL 3: Build capacity in the energy sector to understand risks, assess priorities, and identify cost-effective security and resilience improvements

CESER will bolster the energy sector's risk assessment and mitigation capabilities by streamlining threat information sharing and developing expert guidance, resources, training, and exercises. CESER helps to equip the Nation's energy workforce with the information, resources, and expertise needed to improve security and resilience in organizations of all sizes—thereby elevating the energy sector's overall security posture and reducing the need for Federal support. Capacity building within energy companies, States, and municipal governments promotes timely risk and threat information sharing, effective implementation of mitigation measures, and coordinated preparedness and response efforts.

Core Objectives

- Characterize and prioritize risks in the energy sector, improve the understanding of interdependencies with other critical infrastructure, and develop actionable mitigation measures, guidance, and cost-sharing pilots with the aim of managing risk, reducing the impact of disruption, and informing policy and investment decision-making.
- Host timely and relevant energy sector exercises and examine new platforms for expanded and virtual engagement that improve preparedness and coordination across governments and industry.
- Cultivate the 21st century energy sector cybersecurity workforce through tactical competitions and training at a State and local, collegiate, and industry level.
- Continue to explore pathways to expedite and eliminate barriers to bi-directional threat information sharing on all hazards across industry and governments.
- Bolster the financial and technical assistance provided to States and local governments for energy security planning and cyber risk mitigation to ensure continuous improvement, investment in security, and advancement of preparedness, response, and mitigation efforts.

GOAL 4: Enhance sector-wide situational awareness to inform decision-making in the energy sector

To effectively fulfill the SSA and ESF#12 missions, new and enhanced capabilities to maintain continuous situational awareness and analysis of threats and incidents affecting U.S. energy systems is a high priority. To meet this challenge, CESER will continue to expand development of tools and capabilities, including the use of predictive models and remote sensing to further support emergency preparedness, response, and recovery efforts for industry, interagency, and State partners. CESER will also refine threat information sharing to ensure industry is provided with relevant information to defend against cyber and physical threats.

Core Objectives

- Provide continuous monitoring and analysis of urgent threats, attacks, and disasters impacting the energy sector to support timely actions and coordination across industry and government to prevent and/or mitigate impacts.
- Continue to expand CESER's situational awareness platform to provide tools to industry, interagency, and State partners, including enhanced modeling, remote sensing, analysis, and assessment capabilities for incident preparedness, response, and recovery efforts.
- Deliver actionable, intelligence-informed, all-hazards threat information that is tailored to the unique and interdependent characteristics of critical energy infrastructure, systems, and operations.
- Develop rapid vulnerability assessment capabilities to conduct timely analysis of potential impacts to U.S. energy systems from present threats.

GOAL 5: Ensure effective and efficient emergency response and recovery efforts

CESER plays a critical role in response and recovery to all hazards, as the lead for DOE's responsibilities as the coordinating agency for ESF #12 and the SSA for the energy sector. During an incident requiring a coordinated Federal response, CESER activates the Energy Response Organization and/or the Cyber Crisis Action Team to manage response activities, including deployment of responders and sector engagement. CESER will continue to modernize DOE's response capabilities to ensure that DOE can support industry, interagency, State, local, tribal, and territory partners.

Core Objectives

- Leverage DOE's sector-specific expertise and capabilities to support all-hazards response and recovery in coordination with other Federal agencies, the energy industry, and State, local, tribal, and territory governments.

- Expand regional operations and presence to prepare for regional- and state-specific risks and hazards and improve responder readiness and coordination with partners.
- Continue to develop Catastrophic Incident Response Team capabilities to provide additional subject matter expertise for catastrophic incidents or incidents in remote locations.
- Continue to refine cyber incident response processes and procedures across ESF #12 and in coordination with Federal, industry, and State partners, including options to provide technical assistance to emerging crisis management needs.
- Assess DOE response authorities for currency and potential improvements to response plans in coordination with the energy sector.


SCANNING