Cybersecurity, Energy Security, and Emergency Response

Cybersecurity, Energy Security, and Emergency Response
($K)

FY 2025 Enacted	FY 2026 Enacted	FY 2027 Request	FY 2027 Request vs FY 2026 Enacted
200,000	190,000	160,173	-29,827

Proposed Appropriation Language

For Department of Energy expenses including the purchase, construction, and acquisition of plant and capital equipment, and other expenses necessary for energy sector cybersecurity, energy security, and emergency response activities in carrying out the purposes of the Department of Energy Organization Act (42 U.S.C. 7101 et seq.), including the acquisition or condemnation of any real property or any facility or for plant or facility acquisition, construction, or expansion, $160,173,000, to remain available until expended: Provided, that of such amount, $24,173,000 shall be available until September 30, 2029, for program direction.

Mission

The security and resilience of the energy sector is essential to America's energy dominance and national security. While the federal government has designated energy as one of sixteen critical infrastructure sectors, the energy sector is unique in it enables every other critical infrastructure sector, including the defense industrial base. The energy sector is confronted with a continuously evolving threat landscape, growing energy demand, and rapid technological advancements. The security of our energy systems is not only vital to our national economic security and military readiness, but also crucial for United States. competitiveness in emerging fields such as artificial intelligence (AI), which require energy infrastructure that must be resilient and secure. The U.S. Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) strengthens the security and resilience of America's energy sector by detecting, identifying, analyzing, mitigating, countering, and responding to U.S. energy sector threats and emergencies through wide-ranging programs, activities, and collaborations with industry and state, local, tribal, and territorial (SLTT) entities.

The Secretary of Energy delegated CESER the statutory authority to represent the U.S. government (USG) and act on behalf of DOE as the Sector Risk Management Agency (SRMA), formerly the Sector Specific Agency, for the energy sector per the 2015 Fixing America's Surface Transportation Act and the 2002 Homeland Security Act (as amended). CESER also fulfills the Department's responsibilities as the lead agency for Emergency Support Function #12 (Energy), or ESF #12, under the National Response Framework.

Accordingly, CESER is responsible for enabling U.S. energy critical infrastructure protection through threat analysis, incident response, infrastructure hardening, and technology development. CESER also exercises delegated authority for energy sector emergency preparedness, response, and recovery under the Stafford Act, for energy national security under the Defense Production Act (as amended), and for emergency relief orders under the Federal Power Act (as amended), among other delegations. Through integrated planning, CESER has also developed a comprehensive set of federal programs and deploys subject matter experts to assess and manage critical events caused by severe weather, wildfires, earthquakes, cyber and physical security breaches, electromagnetic interference, and supply chain interruptions.

Overview

CESER is at the forefront of transformations shaping the energy sector, including growing energy demand, the rapid construction of data centers, and the evolution of AI technologies. To build the energy infrastructure necessary to support the growing energy demand, resilience and security must be prioritized. Likewise, CESER

will develop an overarching program called Project ARMOR (Advanced Resilience Measures for Operational Readiness) to harden and secure energy infrastructure servicing critical defense facilities. Given the rapidly evolving threat and technology landscape, CESER programs adapt to ever more sophisticated threats affecting critical infrastructure and supply chains. For example, CESER experts advise and assist industry and SLTTs in replacing outmoded systems and aging architectures with practical, advanced technologies and security measures. Consistent with delegated authorities, CESER conducts energy sector risk analysis relevant to owners and operators; provides technical assistance to federal and SLTT partners on security, risk management, and resilience plans; performs wide-ranging exercises and training; and supports cybersecurity and energy resilience workforce development.

In collaboration with DOE National Laboratories and industry experts, CESER designs and deploys new technologies and engages with USG-industry energy sector councils on electricity, as well as oil and natural gas, to ensure the security of new systems, applications, and components. CESER executes on all facets of its mission through enduring constructive partnerships with industry owners and operators, SLTT entities, USG agencies, U.S. manufacturers, academic institutions, and international counterparts.

Accordingly, the FY 2027 budget request for CESER focuses on the following priorities:

- **Harden and Secure Defense Critical Energy Infrastructure (DCEI) through Project ARMOR**: Activities include conducting vulnerability assessments, implementing security upgrades, and enhancing measures to protect civilian energy assets and systems from a range of advanced threats. Project ARMOR accelerates resilience improvements to maintain energy availability from civilian energy infrastructure for identified critical defense facilities nation-wide.
- **Bolster Energy Dominance through Energy Infrastructure Security and Resilience:** These investments at DOE's National Laboratories, private sector research partners, and others are in alignment with administration efforts to build a resilient and secure energy sector. Activities support the development of AI tools and ensure the secure and resilient grid integration of large electric loads, which include data centers. CESER will prioritize projects that implement Cyber-Informed Engineering principles to integrate security considerations into the concept, design, development, and operation of cyber-physical systems.
- **Mature the Energy Threat Analysis Center (ETAC):** The ETAC will continue to mature its capabilities, focused on leveraging insights from energy sector owners and operators, the DOE National Laboratories, and the Intelligence Community. The partners share knowledge and best practices, identify risks and threats to critical energy infrastructure, and develop mitigation strategies and technical advisories that help energy owners and operators protect their systems from adversaries. As foreign adversaries increasingly view energy infrastructure as a strategic target, ETAC plays a pivotal role in national security by providing near real-time intelligence and predictive threat analysis.
- **Counter Cyber Threats to Energy Systems and Build AI-FORTS:** Continue enhancing efforts to detect, respond, recover, and mitigate cyber threats from nation-state adversaries and cyber criminals targeting U.S. energy infrastructure. Strengthen partnerships with the intelligence community and private sector to share risk information and develop proactive defense strategies. Support the AI-FORTS program (Artificial Intelligence for Operationally Resilient Technologies and Systems), which will use AI to develop defensive cyber technologies, implement active defense measures to disrupt, deter, and recover from cyber attacks, and characterize and counter AI-enabled offensive cyber capabilities from threat actors.
- **Secure the Energy Supply Chain from Foreign Adversaries:** Implement measures to secure the energy supply chain from foreign adversaries and mitigate vulnerabilities to supply chain security. This includes screening domestic and foreign equipment used in U.S. energy infrastructure, with an emphasis on equipment from countries that pose a national security risk. The goal is to ensure that the energy supply chain is resilient and secure against potential disruptions.

- **Enhance Emergency Response Capabilities for Energy Disruptions:** Strengthen CESER's ability to respond to hazards impacting the energy sector, including natural disasters, cyber attacks, and physical threats. Enhance coordination with SLTT entities and industry partners to ensure a swift and effective response to energy disruptions. This includes developing operate-through-compromise plans for various energy emergencies.

Cybersecurity, Energy Security, and Emergency Response
Funding by Budget Control ($K)

	FY 2025 Enacted	FY 2026 Enacted	FY 2027 Request	FY 2027 Request vs FY 2026 Enacted	
				$	%
Policy, Preparedness, and Risk Analysis	26,500	26,500	-	-26,500	-100%
Risk Management Technology and Tools	113,000	109,500	-	-109,500	-100%
Response and Restoration	32,500	30,000	-	-30,000	-100%
Threat Analysis and Incident Response	-	-	39,000	+39,000	+100%
Infrastructure Hardening and Technology Development	-	-	97,000	+97,000	+100%
Program Direction	28,000	24,000	24,173	+173	+1%
Total, Cybersecurity, Energy Security, and Emergency Response	**200,000**	**190,000**	**160,173**	**-29,827**	**-16%**

FY 2026 Enacted Comparability Matrix ($K)

	FY 2027 Budget Structure			
	Threat Analysis and Incident Response	**Infrastructure Hardening and Technology Development**	**Program Direction**	**Total**
FY 2026 Budget Structure				
Policy, Preparedness, and Risk Analysis	4,862	21,638	-	26,500
Risk Management Technology and Tools	3,120	106,380	-	109,500
Response and Restoration	30,000		-	30,000
Program Direction	-	-	24,000	24,000
Total, Cybersecurity, Energy Security, and Emergency Response	**37,982**	**128,018**	**24,000**	**190,000**

FY 2027 Request Comparability Matrix ($K)

	FY 2027 Budget Structure			
	Threat Analysis and Incident Response	**Infrastructure Hardening and Technology Development**	**Program Direction**	**Total**
FY 2026 Budget Structure				
Policy, Preparedness, and Risk Analysis	8,000	20,000	-	28,000
Risk Management Technology and Tools	7,000	77,000	-	84,000
Response and Restoration	24,000	-	-	24,000
Program Direction	-	-	24,173	24,173
Total, Cybersecurity, Energy Security, and Emergency Response	**39,000**	**97,000**	**24,173**	**160,173**

Infrastructure Hardening and Technology Development

Overview

The Infrastructure Hardening and Technology Development program develops cutting edge technologies to mitigate all-hazard threats and deploy them to harden critical energy infrastructure. Infrastructure Hardening focuses on assessing and fortifying critical energy infrastructure against cyber, physical, natural, and supply chain threats. Technology Development focuses on research and development (R&D) to address the most pressing cybersecurity, physical, natural. and supply chain threats in the energy sector, through collaboration with industry, DOE National Laboratories, academia, and other federal agencies.

IHTD focuses on:

- Enhancing the physical security, cybersecurity, and operational resilience of energy asset owners and operators critical to energy and national security. These organizations often face heightened risk because their customer base includes military, defense industrial base, and national security-related facilities.
- Providing direct support to energy asset owners and operators of critical energy infrastructure that have elevated security needs and must be equipped to address sophisticated threat profiles. Ultimately Project ARMOR aims to reduce the "negative externality" of increased risk from sophisticated threats.
- Mitigating supply chain risks to U.S. energy systems through the CyTRICS program by identifying high-priority ICS/OT components or systems and conducting cyber vulnerability and forensic analyses.
- Preparing the current and future energy sector workforce to counter sophisticated, all-hazards threats through specialized training.
- Ensuring the resilience of critical energy infrastructure by identifying vital functions and using an intelligence-driven approach to engineer out the most severe consequences of potential cyber incidents.
- Leveraging AI to significantly enhance the security and resilience of U.S. energy systems.
- Conducting cutting edge research into managing the risks from natural hazards and physical threats.

Infrastructure Hardening leads CESER's effort to harden the U.S. energy infrastructure against cyber, physical, natural, and supply chain threats. The FY 2027 budget request will advance infrastructure hardening activities by investing in resilience at energy utilities (electricity and oil and natural gas) that support critical national security facilities. Project ARMOR will execute targeted site assessments and hardening projects for critical energy partners whose customer bases include national-security organizations and civilians. Beyond the Department of War's (DOW's) traditional installation energy planning activities, and in coordination with the Department of Homeland Security (DHS) and DOW, CESER is performing comprehensive evaluations (outside fenceline) of energy security and resilience parameters to evaluate operational resilience under a variety of operational and national security conditions. Additionally, CESER's supply chain programs will proactively test and mitigate vulnerabilities in operational technology, conduct rapid OT risk assessments, and work directly with utilities and manufactures of OT equipment to advance the practice of supply chain risk management across the energy sector. These efforts are reinforced by advanced training and workforce development programs like CyberForce, which ensure the future energy sector has skilled personnel to defend against sophisticated cyber and physical threats.

Technology Development deploys innovative approaches and technologies to enhance the security and resilience of energy infrastructure. Working closely with the energy sector, academia, and National Laboratories, the FY 2027 request supports an economically competitive, secure, and resilient U.S. energy system. This funding streamlines research and development efforts to focus on enhancing critical infrastructure cybersecurity through AI-driven solutions and addressing the risks posed by natural and manmade hazards. This includes AI-FORTS (Artificial Intelligence for Operationally Resilient Technologies and Systems), an overarching program which uses AI to develop defensive cyber tools, characterize and counter AI-enabled offensive cyber capabilities from threat actors, and ensure the security of AI-based systems used in U.S. energy systems. The FY 2027 budget request furthers CESER's shift from more traditional cybersecurity R&D to

focused research on AI dominance and develop technologies and frameworks to enable energy companies to "operate through compromise" and maintain delivery of services. "Operate through compromise" in the energy sector acknowledges that despite robust security measures, a persistent adversary may eventually breach defenses, requiring organizations to develop strategies to maintain essential functions and resilience even when systems are partially or fully compromised. The FY 2027 budget request also continues critical research into natural and manmade hazards with an emphasis on cutting edge tools to support industry partners in addressing threats such as from wildfire and physical attacks on energy infrastructure.

Highlights of the FY 2027 Budget Request

Infrastructure Hardening ($70 million)
IH leads efforts to harden critical U.S. energy infrastructure against cyber, physical, natural, and supply chain threats.

In FY 2027, IH will concentrate on:

- Conducting 3-7 specialized site assessments for energy sector owners and operators that provide service to facilities that enable energy and national security missions. DOE performs these assessments in coordination with DHS and the DOW, as well as, the energy sector stakeholder.
- Enhancing the physical security, cybersecurity and operational resilience of energy asset owners and operators of critical energy infrastructure, vital to energy and national security mission. These organizations often face heightened security risks as a direct consequence of their national security role yet may lack the resources or capacity to address these risks independently. Providing hardening support to at least two energy asset owners and utility operators responsible for critical energy infrastructure.
- Providing tailored technical assistance and training to 30-40 critical utilities, including incident response exercises and enhanced threat information sharing, ensuring sustained defense against evolving cyber risks.
- Increasing testing capacity in the CyTRICS (Cybersecurity Testing for Resilient Industrial Control Systems) program by 10% annually, measured by a year-over-year increase in the number of critical equipment systems tested, through new partnerships and expanded engagement with industry and university research partners. Expanding partnerships with equipment manufacturers and asset owners/operators to support prioritization and provision of critical systems for testing, while maintaining DOE's ability to procure high-risk components as needed and leveraging these engagements to enhance industry supply chain risk management practices through improved data and insights.
- Enumerating and analyzing critical grid components to identify potential supply chain attack vectors that could manifest as system vulnerabilities and working directly with manufacturers and impacted stakeholders to develop and deploy rapid mitigations.
- Prioritizing new equipment manufacture and asset owner and operator partnerships to expand the range of equipment examined in CyTRICS with a greater focus on systems used in oil and natural gas and nuclear industries.
- Develop standardized frameworks that empower partners to make coordinated, risk-informed investments in grid resilience.
- Enhance the abilities of the energy sector workforce to prepare for cyber incidents impacting operational technology through the delivery of CyberStrike training; Train at least 200 public and private sector partners, develop and incorporate new training modules on defending against AI-enabled offensive cyber capabilities.
- Continue the OT Defender Fellowship program and expand the partnership with graduating Fellows by enhancing engagement with applicable CESER programs.
- Advance the awareness of the energy sector's need for a skilled cybersecurity workforce by conducting the CyberForce Program, to include an in-person cyber defense competition.

- Performing on-site risk assessments essential for fuel and electricity supply at DCEI, evaluating personnel, processes, and technologies to significantly reduce compromise consequences.
- Continuing collaboration with standards organizations to build CIE into the standards that guide the development and deployment of secure energy infrastructure.

Technology Development ($27 million)

TD investigates and develops technologies that make U.S. energy systems more resilient and secure.

In FY 2027, TD will concentrate on:

- Enhancing the AI-FORTS program to advance the development of next-generation artificial intelligence solutions.
- Leveraging the physics of energy delivery and applying advanced AI analytics to operational data to develop tools to detect and respond to anomalous cyber activities within industrial control systems and networks.
- Refining and pilot AI-powered tools that enable operation through compromise to ensure essential energy functions can continue—even in the presence of active cyber intrusions from Advanced Persistent Threats.
- Furthering development of cybersecurity AI testbeds, coupled with additional industry engagement to leverage the testbeds, to rigorously assess the security of AI deployments.
- Ensuring the security of AI-based systems used to operate, control or defend US energy systems.
- Advancing technology to manage risks from Natural Hazards, Physical Threats, and EMP/GMD.
- Developing technology to help identify, characterize, detect, and mitigate risks to energy infrastructure from extreme winter weather, seismic events, and hurricanes, allowing industry to more effectively prepare for and respond to incidents.
- Continuing research that enables the prevention, detection, and dynamic mitigation of growing wildfire risks, with a focus on developing and validating technologies that utilize real-life information to more accurately determine probable equipment and infrastructure failures.
- Advancing technologies to address physical attacks on energy infrastructure, such as substation shootings and the use of unmanned aerial systems (UAS).
- Conducting modeling studies to understand these hazards and developing innovative cost-effective mitigation options to mitigate risks from electromagnetic pulse (EMP) and geomagnetic disturbances (GMD).

Infrastructure Hardening and Technology Development (IHTD)
($K)

	FY 2025 Enacted	FY 2026 Enacted	FY 2027 Request
IHTD – Infrastructure Hardening			70,000
IHTD – Technology Development			27,000
Total, Infrastructure Hardening and Technology Development			**97,000**

Explanation of Changes for Infrastructure Hardening and Technology Development

The Infrastructure Hardening and Technology Development (IHTD) program incorporates programs from the Risk Management Technology and Tools Division and strategically aligns defense critical energy infrastructure and workforce development programs from the division formerly named Preparedness, Policy, and Risk Analysis. This change streamlines the CESER budget to align with the administration's priorities.

Infrastructure Hardening

- Increases hardening efforts to secure critical energy infrastructure against sophisticated threats and build system-wide resilience to ensure continuous energy availability for national defense missions.
- Advances the readiness of the energy sector's cybersecurity workforce through bespoke training programs informed by emerging risks and threats and brings awareness to build a pipeline for the future of the energy sector's cybersecurity workforce.
- Maintain emphasis on the mitigation of supply chain risks to high-priority ICS/OT systems by conducting cyber vulnerability and forensic analyses, and engineering out cyber risk by informing improvements in component design, manufacturing, and procurement practices.

Technology Development

- Refocuses research, development, and demonstration of multi-hazard risk mitigation tools to enhance the security and resilience of energy infrastructure and focus on critical risks and priorities.
- Streamlines resource allocation towards advancing AI, natural hazard, and physical security research, development, and implementation to bolster the resilience of owners and operators of critical energy assets.

Threat Analysis and Incident Response (TAIR)

Overview

The Threat Analysis and Incident Response (TAIR) program leverages insights from energy sector owners and operators, the Intelligence Community, and knowledge of the DOE National Laboratories to identify, characterize, and mitigate risks and threats to critical energy infrastructure. TAIR leads CESER's efforts to respond to incidents impacting the U.S. energy sector. The program delivers a range of capabilities to ensure effective restoration of energy systems, this includes leveraging information sharing platforms to provide near real-time situational awareness, facilitating waivers to accelerate restoration, enabling impact assessments, and deploying critical assets during a crisis to Federal, state, and private sector partners. Additionally, TAIR analyzes risks to develop mitigation strategies, issuing technical advisories to energy sector partners to protect their systems, builds capacity through technical assistance, and disseminate security best practices. TAIR strengthens critical energy infrastructure and community resilience by developing comprehensive, threat-informed exercises focusing on preparedness, resilience, and emergency response. These events focus on testing response plans by validating the entities' preparedness and readiness to respond to all risks, threats, and hazards. Overall, TAIR helps reduce the impact of current and future risks, thereby strengthening the energy sector security and resilience through threat analysis, risk assessments, proactive information sharing, and targeted exercises focused on increasing response efficiency and effectiveness.

TAIR focuses on:

- Leading the coordination of national efforts to restore U.S. energy infrastructure following disruptions (from cyber, physical, and natural), addressing impacts efficiently, and assisting industry and government partners with response, recovery and restoration activities.
- Continuing collaborative risk management activities with sector stakeholders to enable real, tangible risk reduction outcomes.
- Delivering timely and actionable analysis, recommendations, and mitigation strategies that address risks and threats to the energy sector.
- Strengthening threat information sharing mechanisms and advancing the sector's ability to proactively detect threat.
- Operationally collaborate with industry to deliver a common operating picture of threats.
- Supporting CESER's Sector Risk Management Agency (SRMA) mission by providing dedicated program management, logistical support, and targeted technical assistance to Electricity, Oil & Natural Gas Subsector.
- Conducting incident response exercises to strengthen the sector's capabilities and CESER's response and restoration capacity.
- Ensuring the effective restoration of energy systems from all-hazards through a range of capabilities.
- Executing DOE's emergency authorities for the energy sector.

Threat Analysis ($18.5 million) identifies, analyzes, and enables mitigation of threats to America's critical energy infrastructure through a variety of processes, procedures, and capabilities. Threat Analysis operates the Energy Threat Analysis Center (ETAC), an operational collaborative that convenes experts from DOE, and industry to collectively identify, analyze, and mitigate threats to energy infrastructure. ETAC integrates industry data, context, and expertise with government intelligence to enable timely and actionable information sharing to disrupt threats to the energy sector. CESER delivers threat information sharing technologies, such as Cybersecurity Risk Information Sharing Program (CRISP), ensuring that the energy sector remains resilient against evolving cyber threats by deploying sensors that monitor Information Technology (IT) networks. This program identifies, quantifies, and analyzes risks to develop mitigation strategies and issues technical advisories to energy sector partners to protect their systems. Threat Analysis also supports CESER's SRMA mission through dedicated program management and logistical support for seamless public-private coordination within

the Electricity and Oil and Natural Gas sectors to advance the security of our nation's energy infrastructure.

Incident Response ($20.5 million) develops plans and deploys to help respond to and recover from incidents that cause a significant energy sector disruption. CESER prepares for and responds to disruptive incidents to include both Stafford Act and non-Stafford Act disasters. In addition to responding to incidents in the sector, CESER supports preparation and safety around National Special Security Events, as well as contributes manpower to the FEMA Surge Capacity Force. DOE's Energy Response Organization (ERO), led and managed by CESER, activates energy sector response efforts, shares critical information, provides subject matter expertise and technical assistance to Federal and SLTT government partners and industry stakeholders. When deployed, DOE's responder cadre conducts damage assessments, assists with restoration planning, and provides technical assistance to states and industry partners. Additionally, this division also carries out DOE's emergency authorities for the energy sector. These authorities include Federal Power Act section 202(c), as well as Grid Security Emergency under Federal Power Act section 215(a). CESER's exercises program creates real world scenarios to test an entity's response to emerging threats and risks, leveraging testbeds to closely resemble real world environments and complexity; therefore, enhancing the sector's response capabilities and capacity.
In FY 2027, CESER will continue to refine tools for the rapid analysis of novel threats and focused technical assistance for industry partners, designed to address the unique complexities of the energy sector. CESER will maintain its situational awareness, analysis, and technical capabilities to provide near continuous monitoring and analysis of incidents impacting, or potentially impacting, the U.S. energy sector. This includes but is not limited to maintaining the EAGLE-I platform. In FY 2027, EAGLE-I will be focused on expanding the eligible user base, refining data sources and improving data quality.

Highlights of the FY 2027 Budget Request

Threat Analysis ($18.5 million)
Threat Analysis (TA) identifies, analyzes, and enables mitigation of threats to America's critical energy infrastructure through a variety of processes, procedures, and capabilities. In FY 2027, TA will concentrate on:

- Continuing to modernize the Cyber Risk Information Sharing Program (CRISP) sensors and architecture, enabling the collection of a wider range of data types, including cloud telemetry, as well as improving automated reporting capabilities.
- Continuing to conduct high-quality analysis of complex risks and cyber threats to critical energy infrastructure and disseminating effective mitigations through a portfolio of analytic products tailored to the unique needs of the energy sector.
- Developing and deploying analytic tools to improve the detection of malicious cyber activity in energy networks.
- Tracking and mitigating a broad spectrum of AI-enabled cyber-attacks.
- Continuing to refine tools and capabilities for the rapid analysis of novel threats and focused technical assistance for industry partners, designed to address the unique complexities of the energy sector.
- Outfitting the ETAC facility with secure information technology connections to protect government data holdings and enable robust, collaborative analysis across government and industry ETAC partners.
- Supporting CESER's SRMA mission by providing dedicated program management and logistical support to the Electricity and Oil and Natural gas sectors for seamless public-private coordination on energy security and resilience policy
- Developing and finalizing a comprehensive National Energy Sector Risk Register to systematically catalog and grade all-hazard threats across the energy sector, including supply chain vulnerabilities, interdependencies, and AI-enabled adversaries.
- Providing strategic risk insights and illumination of threats that could have impacts to all stakeholders by developing and disseminating a portfolio of analytical products through the Analysis of Risk in the Energy Sector (ARES) activity.

Incident Response ($20.5 million)

Incident Response (IR) coordinates federal response to restore energy during disruptions, deploys responders and technical experts to disaster sites, coordinates restoration efforts, and manages exercises to evaluate response, recovery and emergency procedures.

In FY 2027, IR will concentrate on:

- Delivering risk-informed, regionally focused support to help states and industry better prepare for and respond to region-specific threats.
- Continuing to train and coordinate a DOE responder cadre of volunteer responders from across DOE to deploy virtually or physically to affected regions during disasters.
- Modernize training methods for the DOE Responder cadre, Catastrophic Incident Response Team though self-paced online training accompanied with hands-on exercises and technical instructor lead courses.
- Continue efforts to increase efficiencies to support energy sector emergency response and essential logistics, finance, and administration activities.
- Building regional capabilities and teams that will work directly with states and regions delivering subject matter expertise on emergency response, to participate in and conduct joint exercises and training with the SLTT and industry stakeholders as Regional Energy Advisors with the support of regional coordinators to strengthen DOE's partnerships with the energy sector.
- Delivering readiness exercises (Clear Path, Liberty Eclipse, Rogue Intrusion) that focus on the response and restoration missions leveraging realistic and complex scenarios, influenced by trusted classified and unclassified reports and sources, that include emerging physical security, cybersecurity, supply chain integrity, and defense critical electric infrastructure threats and risks.
- Maintaining situational awareness, analysis, and technical capabilities efforts to provide near continuous monitoring and analysis of incidents impacting, or potentially impacting, the U.S. energy sector.
- Continuing vulnerability analysis of key infrastructure and locations to support rapid response, contingency planning, and coordination with partners, including the industry and the Department of War.
- Enhancing CESER's incident and emergency response capabilities within the sector, while simultaneously addressing resource adequacy and energy emergency directives as outlined in Executive Order 14156 by leveraging the Federal Power Act.
- Utilizing and maintaining the EAGLE-I platform, expanding the eligible user base, refining data sources and improving data quality.

CESER will continue to administer delegated DOE emergency authorities, including the Federal Power Act, Defense Production Act, Jones Act, and concurrence on energy-related actions managed by other Departments and Agencies, such as the Environmental Protection Agency, Department of Transportation, and Department of Homeland Security.

Threat Analysis and Incident Response (TAIR)
($K)

	FY 2025 Enacted	FY 2026 Enacted	FY 2027 Request
TAIR - Threat Analysis	-	-	18,500
TAIR - Incident Response	-	-	20,500
Total, Threat Analysis and Incident Response			**39,000**

Explanation of Changes for Threat Analysis and Incident Response

The Threat Analysis and Incident Response (TAIR) program incorporates programs from the Response and Restoration Division and strategically aligns preparedness and risk analysis activities from the divisions formerly named Preparedness, Policy, and Risk Analysis. This change streamlines the CESER budget to align with the administration's strategic priorities, consolidates similar readiness programs, demonstrating a logical progression from identified and analyzed risk to the development of tailored readiness efforts and the deployment of prepared response personnel.

Threat Analysis

- Continues support to Energy Threat Analysis Center to support administration priorities and focus on maximizing existing tools and equipment, with limited development of new tools.

Incident Response

- Operations will enhance training delivery methods to ensure courses are both effective and efficient, with a focus on prioritized risks.
- Expand the EAGLE-I eligible user base, refine data sources and improve data quality to further support Federal and state stakeholders.
- Enhances CESER's incident and emergency response capabilities within the sector, while simultaneously addressing resource adequacy and energy emergency directives as outlined in Executive Order 14156 by leveraging the Federal Power Act.

Program Direction (PD)

Overview

Salaries and Benefits support federal employees who provide executive management, programmatic oversight, and analysis for the effective implementation of the CESER program. This includes personnel at Headquarters in the National Capital Region and the National Energy Technology Laboratory (NETL) in West Virginia. While CESER funds NETL technical personnel within this budget, the salaries and benefits of NETL Federal employees are included within the full-time equivalent (FTE) total of the DOE Fossil Energy Research and Development account.

CESER's staffing efforts continue to focus on building core capabilities and partnerships with industry. As the energy sector SRMA, CESER continues to focus on infrastructure hardening, training, technical assistance, workforce development, SLTT support, risk analysis of cybersecurity, physical, and natural hazard risks, emergency response activities, long-term recovery efforts across the department and interagency.

Travel includes transportation, per diem, and incidental expenses allowing CESER to effectively deliver on its mission.

Support Services include contractor support to perform administrative and analytical tasks in support of CESER's mission. In addition, support services include assistance with communications and outreach to enhance external communications and engagement with the energy sector and other CESER stakeholders.

Other Related Expenses include DOE's Working Capital Fund support, Energy Information Technology Services (EITS), minor construction, equipment purchases, upgrades, and replacements, office furniture, commercial credit card purchases, general and advanced training, security clearances, and other miscellaneous expenditures.

Highlights of the FY 2027 Budget Request

This budget request accounts for essential personnel needed to execute CESER's national security and energy security mission that is focused on significant and increasing cyber, physical, and weather-based threats that face the U.S. energy system. The FY 2027 request ensures the Department has a strong federal team to manage these threats, and working in partnership with electricity, oil, and natural gas owners and operators, SLTT community, interagency partners, and other federal agencies to provide a secure and resilient energy sector for Americans.

Program Direction
($K)

	FY 2025 Enacted	FY 2026 Enacted	FY 2027 Request
Salaries and Benefits	17,045	15,037	15,037
Travel	400	380	380
Support Services	4,016	3,168	3,168
Other Related Expenses	2,739	2,603	2,762
Total, Washington Headquarters	**24,200**	**21,188**	**21,347**
Salaries and Benefits	2,000	1,468	1,468
Travel	115	20	20
Support Services	450	349	349
Other Related Expenses	1,235	975	989
Total, National Energy Technology Laboratory	**3,800**	**2,812**	**2,826**
Salaries and Benefits	19,045	16,505	16,505
Travel	515	400	400
Support Services	4,466	3,517	3,517
Other Related Expenses	3,974	3,578	3,751
Total, Program Direction	**28,000**	**24,000**	**24,173**
Technical Support	3,828	2,749	2,749
Management Support	638	768	768
Total, Support Services	**4,466**	**3,517**	**3,517**
Other Services	200	159	159
EITS Desktop Services	866	1,000	1,000
WCF	2,908	2,419	2,592
Total, Other Related Expenses	**3,974**	**3,578**	**3,751**
Federal FTEs	62	58	58
Additional HGEO FTEs at NETL supporting CESER[1]	11	9	9
Total CESER-funded FTEs	**73**	**67**	**67**

[1] CESER funds FTEs at Hydrocarbon and Geothermal Energy Office (HGEO)'s National Energy Technology Laboratory who support CESER activities. These 9 FTEs are in HGEO's FTE totals and are not included in the CESER FTE totals shown on the "Federal FTEs" line.

Program Direction
Activities and Explanation of Changes
($K)

FY 2026 Enacted	FY 2027 Request	Explanation of Changes FY 2027 Request vs FY 2026 Enacted
Program Direction		
24,000	**24,173**	**+173**
Salaries and Benefits		
16,505	*16,505*	-
Supports 58 FTEs at HQ and 9 FTEs at NETL that provide executive management, programmatic oversight, and analysis for the effective implementation of CESER programs.	Supports 58 FTEs at HQ and 9 FTEs at NETL that provide executive management, programmatic oversight, and analysis for the effective implementation of CESER programs.	Maintains steady rate of FTEs at HQ and NETL in alignment with the program activities.
Travel		
400	*400*	-
Includes transportation, subsistence, and incidental expenses that allow CESER staff to effectively facilitate its mission and oversee the portfolio.	Includes transportation, subsistence, and incidental expenses that allow CESER staff to effectively facilitate its mission and oversee the portfolio.	Increased technological capabilities and decreased capacity in recent years have reduced travel needs slightly. Expect net zero change due to decreased travel but increasing travel expenses.
Support Services		
3,517	*3,517*	-
Support Services includes contractor support directed by the federal staff to provide analysis to management.	Support budget, acquisition, human resources, communications, business systems, and administrative support needs.	Maintaining federal staff is the priority. Any increases in support service rates would be offset by decreased scope, resulting in net zero change.
Other Related Expenses		
3,578	*3,751*	*+173*
Includes equipment upgrades and replacements, office furniture, minor construction, commercial credit card purchases using simplified acquisition procedures when possible, and miscellaneous expenditures.	Includes equipment upgrades and replacements, office furniture, minor construction, commercial credit card purchases using simplified acquisition procedures when possible, and miscellaneous expenditures.	Increased WCF and EITS costs.

DEPARTMENT OF ENERGY
Funding by Site Detail
TAS_2250 - Cybersecurity, Energy Security and Emergency Response (CESER) - FY 2027
(Dollars in Thousands)

	FY 2025 Enacted	FY 2026 Enacted	FY 2027 Request
Argonne National Laboratory			
Risk Management Tools and Technologies (270)	700	2,355	1,163
Response and Restoration (270)	500	350	325
Preparedness, Policy, and Risk Analysis (270)	2,362	2,000	2,305
Total Argonne National Laboratory	**3,562**	**4,705**	**3,793**
Idaho National Laboratory			
Risk Management Tools and Technologies (270)	19,054	15,620	13,073
Response and Restoration (270)	1,900	1,100	1,141
Preparedness, Policy, and Risk Analysis (270)	3,130	3,800	3,661
Total Idaho National Laboratory	**24,084**	**20,520**	**17,875**
Lawrence Berkeley National Laboratory			
Risk Management Tools and Technologies (270)	400	1,500	724
Total Lawrence Berkeley National Laboratory	**400**	**1,500**	**724**
Lawrence Livermore National Laboratory			
Risk Management Tools and Technologies (270)	33,720	14,500	18,095
Response and Restoration (270)	4,610	3,240	2,998
Preparedness, Policy, and Risk Analysis (270)	4,424	5,050	5,005
Total Lawrence Livermore National Laboratory	**42,754**	**22,790**	**26,098**
Los Alamos National Laboratory			
Risk Management Tools and Technologies (270)	800	1,000	681
Total Los Alamos National Laboratory	**800**	**1,000**	**681**
National Energy Technology Lab			
Risk Management Tools and Technologies (270)	10,938	11,475	8,467
Response and Restoration (270)	3,123	1,952	1,934
Preparedness, Policy, and Risk Analysis (270)	1,161	2,000	1,670
Program Direction - CESER (270)	4,621	500	2,247
Total National Energy Technology Lab	**19,843**	**15,927**	**14,318**
National Laboratory of the Rockies			
Risk Management Tools and Technologies (270)	3,650	5,150	3,332
Response and Restoration (270)	1,528	608	807
Preparedness, Policy, and Risk Analysis (270)	1,015	1,200	1,170
Total National Laboratory of the Rockies	**6,193**	**6,958**	**5,309**
Oak Ridge National Laboratory			
Risk Management Tools and Technologies (270)	3,080	9,930	4,954
Response and Restoration (270)	9,500	12,210	8,392
Total Oak Ridge National Laboratory	**12,580**	**22,140**	**13,346**

DEPARTMENT OF ENERGY
Funding by Site Detail
TAS_2250 - Cybersecurity, Energy Security and Emergency Response (CESER) - FY 2027
(Dollars in Thousands)

	FY 2025 Enacted	FY 2026 Enacted	FY 2027 Request
Pacific Northwest National Laboratory			
Risk Management Tools and Technologies (270)	11,835	14,450	9,941
Response and Restoration (270)	3,125	2,000	1,954
Preparedness, Policy, and Risk Analysis (270)	315	0	166
Total Pacific Northwest National Laboratory	**15,275**	**16,450**	**12,061**
Richland Operations Office			
Response and Restoration (270)	3,057	5,100	3,169
Preparedness, Policy, and Risk Analysis (270)	75	0	40
Total Richland Operations Office	**3,132**	**5,100**	**3,209**
Sandia National Laboratories			
Risk Management Tools and Technologies (270)	14,730	16,020	11,620
Response and Restoration (270)	0	530	212
Total Sandia National Laboratories	**14,730**	**16,550**	**11,832**
Washington Headquarters			
Risk Management Tools and Technologies (270)	14,093	17,500	11,950
Response and Restoration (270)	5,157	2,910	3,068
Preparedness, Policy, and Risk Analysis (270)	14,018	12,450	13,983
Program Direction - CESER (270)	23,379	23,500	21,926
Total Washington Headquarters	**56,647**	**56,360**	**50,927**
Total Funding by Site for TAS_2250 - Cybersecurity, Energy Security and Emergency Response (CESER)	**200,000**	**190,000**	**160,173**