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

| FY 2024 Enacted | FY 2025 Enacted | FY 2026 Request | FY 2026 Request vs FY 2025 Enacted |
|---|---|---|---|
| 200,000 | 200,000 | 150,000 | -50,000 |

**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, $150,000,000, to remain available until expended: Provided, that of such amount, $23,000,000 shall be available until September 30, 2027, for program direction.

**Mission**

The resilience and security of the energy sector is essential to America's economic prosperity and national security. While the federal government has designated energy as one of sixteen critical infrastructure sectors, the energy sector is also uniquely critical as it enables every other critical infrastructure sector, including the defense industrial base. The energy sector is confronted with a continuously evolving threat landscape, rapid technological advancements, and vulnerabilities in supply chain cybersecurity. The security of our energy systems is not only vital to our national economic security and military readiness, but also crucial for U.S. 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 resilience and security of America's energy sector by providing federal leadership in detecting, mitigating, countering, and responding to U.S. energy sector threats and emergencies through wide-ranging programs, activities, and collaborations with industry, regional, and state, local tribal and territorial (SLTT) entities.

The Secretary of Energy delegated CESER with statutory authority to represent the U.S. government (USG) and act on behalf of DOE as the Sector Specific Agency for the energy sector per the 2015 Fixing America's Surface Transportation Act. CESER assumes the critical roles as lead agency for Emergency Support Function #12 (Energy), or ESF #12, under the National Response Framework, and fulfills DOE's role as the Sector Risk Management Agency (SRMA) for the energy sector pursuant the 2002 Homeland Security Act (as amended). Accordingly, CESER has responsibility for protection of the U.S. energy critical infrastructure, risk management, sector coordination, incident management, and emergency activities. 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.

In these capacities, CESER employs a risk-informed approach to identify, assess, mitigate, and prevent foreseeable consequences to energy reliability, which includes hardening of the U.S. energy infrastructure and adoption of advanced technologies and practices for energy resilience. 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 demand from AI data centers, resilience and security must be prioritized. Likewise, CESER will develop an overarching program called AI-FORTS (Artificial Intelligence for Operationally Resilient Technologies and Systems) to advance three goals: secure the energy sector for AI, secure the energy sector with AI, and secure the energy sector from AI. 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 tools and technologies and engages with USG-industry energy sector councils on electricity, oil, and natural gas to ensure the security of new systems, applications, and components. Through enduring constructive partnerships with industry owners and operators, SLTT entities, USG agencies, U.S. manufacturers, academic institutions, and international counterparts, CESER accomplishes all facets of its mission

Accordingly, the FY 2026 budget request for CESER focuses on the following priorities:

- **Bolster Energy Dominance through Infrastructure Resilience and Security:** Strengthen the resilience and security of critical energy infrastructure assets, including pipelines, refineries, power plants, transmission, and distribution systems against physical and cyber threats to ensure uninterrupted energy production and delivery. To support the development of AI, ensure the resilient and secure grid integration of large electric loads, including data centers. Prioritize projects that implement Cyber-Informed Engineering principles to integrate security considerations into the concept, design, development, and operation of cyber-physical systems.
- **Protect Defense Critical Energy Infrastructure (DCEI):** Recognizing the critical link between energy and national security, CESER will prioritize the security and resilience of energy infrastructure that supports military installations and defense activities. This includes conducting vulnerability assessments, implementing security upgrades, and enhancing cybersecurity measures to protect these vital assets from all threats. It also includes sponsored exercises focused on response and restoration of defense critical energy infrastructure. The Cyber ARMOR program (Advanced Resilience Measures for Operational Readiness) is established to accelerate cybersecurity improvements for resource-constrained energy entities critical to national security.
- **Counter Cyber Threats to Energy Systems and Build AI-FORTS:** Enhance 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. Build the AI-FORTS program (Artificial Intelligence for Operationally Resilient Technologies and Systems), which will use AI to develop defensive cyber tools, implement active defense measures to disrupt, deter, and recover from cyber attacks, and characterize and counter AI-enabled offensive cyber capabilities from threat actors.
- **Expand the Energy Threat Analysis Center (ETAC):** The Department operationalized the Energy Threat Analysis Center (ETAC) in FY 2025 to address the increasingly active and sophisticated cyber threats to the U.S. energy sector through operational collaboration. The ETAC will continue to leverage insights from energy sector owners and operators, the DOE National Laboratories, and the Intelligence Community to exchange data, 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, predictive threat analysis, and coordinated response capabilities.
- **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, cyberattacks, 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.
- **Build Capacity within State and Local Communities:** Provide technical and financial assistance to SLTT entities through tools and capability uplift that help state, local, tribal, and territorial governments boost emergency preparedness and strengthen response coordination to support state-led, risk-informed investments in energy sector risk mitigation and resilience. This includes supporting efforts to diversify energy sources, improve grid resilience, and enhance cybersecurity capabilities. The goal is to empower States and local communities to take ownership of their energy security.

**Summary Funding Table by Budget Control**
**($K)**

| | FY 2024 Enacted | FY 2025 Enacted | FY 2026 Request | FY 2026 Request vs FY 2025 Enacted | |
|---|---|---|---|---|---|
| | | | | $ | % |
| Policy, Preparedness, and Risk Analysis | 26,500 | 26,500 | 27,000 | +500 | +2% |
| Risk Management Tools & Technologies | 113,000 | 113,000 | 74,000 | -39,000 | -35% |
| Response and Restoration | 32,500 | 32,500 | 26,000 | -6,500 | -20% |
| Program Direction | 28,000 | 28,000 | 23,000 | -5,000 | -18% |
| **Total, Cybersecurity, Energy Security, and Emergency Response** | **200,000** | **200,000** | **150,000** | **-50,000** | **-25%** |

## Preparedness, Policy, and Risk Analysis (PPRA)

### Overview

The Preparedness, Policy, and Risk Analysis (PPRA) division cultivates strong partnerships across all levels of government and private industry, with insights and support from academia and the DOE National Laboratories to identify, assess, and manage risk. PPRA works to build critical energy security and resilience infrastructure capacity by sharing information, enhancing preparedness, and promoting learning and adaptation through training and exercises. PPRA's overarching goal is to buy down risks to the energy sector through the activities described in this Request. Within CESER, PPRA provides a point of entry for State, Local, Tribal, and Territorial (SLTT) governments and energy sector private partners when collaborating with DOE and the Federal Government on critical energy infrastructure protection including cybersecurity, energy security, risk mitigation, resilience, and emergency preparedness. In recognition of the critical link between energy and national security, CESER prioritizes the resilience and security of Defense Critical Energy Infrastructure (DCEI) companies and facilities. PPRA's extensive partnerships across energy stakeholders, Federal agencies, academia, National Laboratories, information sharing and analysis centers (ISACs), collectively enhance preparedness and resilience amid evolving threats, technological advancements, and energy system trends.

### Highlights of the FY 2026 Budget Request

The FY 2026 Budget Request identifies a new baseline for CESER's activities to enhance the resilience and security of the Nation's critical energy infrastructure systems from a risk-informed threat perspective. This program not only fosters partnerships across the energy sector with owners and operators of energy critical infrastructure assets and systems and SLTT partners, but also develops risk assessments, enhances capacity of stakeholders, and supports targeted training and preparedness exercises.

**Planning, Preparedness, and Resilience ($21 million)**

This program line provides $11 million for SRMA planning, preparedness, risk analysis, and risk management activities to enhance the resilience and security of the Nation's critical energy infrastructure, addressing a diverse range of evolving risks, including severe weather, wildfires, cyber incidents, and supply chain vulnerabilities. This includes funding collaborative risk management activities such as:

- Engaging energy sector industry stakeholders through sector coordinating councils and associated working groups to foster public-private partnerships and cultivate trusted relationships.
- Assessing emerging and adaptive risks to energy infrastructure systems from risk-informed threats.
- Building capacity at SLTT partners; and
- Assessing the security of defense critical energy infrastructure assets and systems supporting critical defense facilities.

Key outcomes that will be completed during Fiscal Year 2026 include:

- Enhancement of CESER's Analysis of Risk in the Energy Sector (ARES) products that evaluate and characterize potential consequences from emerging or adaptive threats affecting the entire energy sector (electricity and oil and natural gas subsectors).
- Continue collaborative risk management activities with sector stakeholders to enable real, tangible risk reduction outcomes.
- Development of analysis products that respond to stakeholder needs and requirements for emerging and persistent threats and hazards, providing immediate risk and resilience analyses to mitigate and avoid the impacts of energy supply disruptions.
- Development of robust analytical products that support Department and Administration decision-making on national security or sensitive matters.
- In prioritizing defense critical energy infrastructure, develop a suite of assessment products that can support planning and operational decision-making for owners and operators that provide energy services to critical defense facilities.

**Cybersecurity Advanced Resilience Measures for Operational Readiness (Cyber ARMOR) Program ($10 million)**

The Cyber ARMOR Program is a targeted initiative supporting CESER's core mission to enhance the cybersecurity defense and operational resilience of energy asset owners and operators critical to national security. These organizations often face heightened cybersecurity risks as a direct consequence of their national security role yet may lack the resources or capacity to address these risks independently. Cyber ARMOR is designed to offset the "negative

externality" of increased cyber risk borne by these entities due to their service to military, defense industrial base and other national security related installations. The program provides direct support to help them meet elevated security requirements and address unique threat profiles associated with their critical roles.
The program streamlines application and reporting processes to reduce the administrative burden for smaller or resource-constrained utilities, ensuring equitable access to federal support.
The $20 million in funding is split between the Preparedness, Partnerships, and Response Assistance (PPRA) and Risk Management Tools (RMT) divisions.
PPRA: Focuses on tailored technical assistance, grants, and hands-on training for utilities and energy organizations. This includes incident response exercises, tabletop drills, and the development of organization-specific playbooks for high-risk scenarios.
RMT: Supports the applied research, development, and adoption of advanced resilience technologies specifically tailored for smaller, high-risk utilities. These efforts include areas such as development and deployment of lightweight, cost-effective monitoring and anomaly detection solutions suitable for limited-resource environments, development of rapid recovery and continuity-of-operations protocols for facilities with minimal IT staff, development and enhanced threat information sharing mechanisms designed for organizations with limited cybersecurity infrastructure.

**Exercises, Training, and Workforce Development ($6 million)**

In support of CESER's mission to be prepared for, respond to, and recover from, threats and hazards causing energy disruptions, this program line will elevate energy sector preparedness through platforms such as targeted cybersecurity training, exercises, and workforce development programs. Directed funding is provided for a new grants pilot program for cybersecurity upgrades, and related support to energy producers and distributors, that prioritizes owners and operators of assets critical to national security and who have limited resources.

- **Exercise, Training, and Workforce Development Programs ($6 million):** CESER's exercise, training, and workforce development programs focus on the preparation and collaboration of Emergency Support Function #12 and CESER's SRMA responsibilities. These programs support collaboration with the electricity and oil and natural gas subsectors, other Federal partners, and SLTT governments and organizations. Sponsored exercises (e.g. Clear Path and Liberty Eclipse) focus on the response and restoration missions leveraging realistic and complex scenarios that include physical security, cybersecurity, logistics and supply chain integrity, and defense critical electric infrastructure. The exercise scenarios and the cyber training programs (e.g. CyberStrike and OT Defender Fellowship) are directly influenced by trusted classified and unclassified reports and sources, with the goal to provide the identification, validation, and employment of mitigation efforts and actions in advance of a potential threat, hazard, or attack, resulting in additional security and resilience to energy sector infrastructure. Working with RMT, these programs continue to incorporate the use of new technologies to include the emergence of AI within the energy cybersecurity response domain. CESER's framework for promoting the energy sector's cybersecurity workforce development is aimed at expanding the talent pool by providing opportunities such as hosting cybersecurity competitions, promoting apprenticeships, and upskilling efforts.

**Preparedness, Policy, and Risk Analysis (PPRA) ($K)**

| | FY 2024 Enacted | FY 2025 Enacted | FY 2026 Request | FY 2026 Request vs FY 2025 Enacted | |
|---|---|---|---|---|---|
| | | | | $ | % |
| **Preparedness, Policy, and Risk Analysis** | | | | | |
| Planning, Preparedness, and Resilience | 17,500 | 17,500 | 21,000 | +3,500 | +20% |
| Exercises, Training and Workforce Development | 9,000 | 9,000 | 6,000 | -3,000 | -33% |
| **Total, Preparedness, Policy, and Risk Analysis** | **26,500** | **26,500** | **27,000** | **+500** | **+2%** |

**Explanation of Changes for Preparedness, Policy and Risk Analysis**

The addition of $3.5M for the Planning, Preparedness, and Resilience line is specifically directed for the referenced new activity to improve the cybersecurity of owners and operations of energy assets that are critical to national security. The funding increase will be used to harden systems, increase cybersecurity resiliency, and expand participation in information sharing resulting in decreased national security risks, improved grid security and energy reliability. Defense Critical Energy Infrastructure activities will see an increase, as well as associated activities to develop Risk Analysis products for energy sector stakeholders.

## Risk Management Tools and Technologies (RMT)

### Overview

The Risk Management, Tools, and Technologies (RMT) division focuses on research and development (R&D) to address risk-based cybersecurity, physical, electromagnetic, and geomagnetic threats and hazards in the energy sector, through collaboration with industry, DOE National Laboratories, academia, and other federal agencies. RMT deploys innovative approaches and technologies to enhance the security and resilience of energy infrastructure. Furthermore, RMT develops tools to monitor and protect critical energy infrastructure, enabling automated threat analysis and response, while also identifying vulnerabilities and devising mitigation strategies. RMT supports industry partners in adopting new technologies and integrating improved processes and practices, while simultaneously leading Cyber-Informed Engineering across DOE's R&D initiatives, ensuring the enhanced inherent security of future energy systems.

### Highlights of the FY 2026 Budget Request

Working closely with the energy sector, academia, and National Laboratories, the FY2026 request supports an economically competitive, secure, and resilient U.S. energy infrastructure. This funding focuses on specific areas, such as enhancing critical infrastructure cybersecurity through research and development, AI-driven solutions, supply chain risk management, and implementing tools to manage risk-based vulnerabilities and threats. This includes AI-FORTS (Artificial Intelligence for Operationally Resilient Technologies and Systems), an overarching program which will use AI to 1) develop defensive cyber tools, 2) implement active defense measures to disrupt, deter, and recover from cyber attacks, and 3) characterize and counter AI-enabled offensive cyber capabilities from threat actors. RMT will shift from more traditional cybersecurity R&D to focused research on AI dominance and an ability to operate through compromise.

**Advance Tools to Manage Cyber Risks ($34.5 million)**

- **R&D of Cybersecurity Tools and Technologies ($21.5 million)** CESER is strengthening the cybersecurity posture of the energy sector by advancing the development of next-generation artificial intelligence solutions through AI-FORTS, as well as the implementation of resilient operational strategies that enable energy systems to operate through compromise. AI-FORTS will drive the creation and deployment of AI-powered tools for enhanced protection, continuous monitoring, rapid detection, effective response, robust containment, thorough forensics, and swift recovery. By leveraging the physics of energy delivery and applying advanced AI analytics to operational data, CESER will equip owners and operators with actionable intelligence to detect and respond to anomalous cyber activities within industrial control systems and networks. Proactive initiatives, such as a dedicated AI testbed, will rigorously assess the security of AI deployments, ensuring energy systems remain resilient against AI-enabled threats and identifying vulnerabilities before they can be exploited. CESER is also prioritizing the ability to operate through compromise in recognition of the growing sophistication of Advanced Persistent Threats. Rather than relying solely on perimeter defenses, CESER's R&D will focus on developing tools and protocols that ensure essential energy functions can continue—even in the presence of active cyber intrusions. These efforts include designing containment strategies, forensic capabilities, and resilient architectures that limit adversary impact and enable rapid restoration of normal operations. A continuously evolving cybersecurity R&D gap analysis will guide these efforts to ensure maximum relevance and impact against the evolving threat landscape.

- **Cybersecurity Advanced Resilience Measures for Operational Readiness (Cyber ARMOR) Program ($10 million):** The Cyber ARMOR Program is a targeted initiative supporting CESER's core mission to enhance the cybersecurity defense and operational resilience of energy asset owners and operators critical to national security. These organizations often face heightened cybersecurity risks as a direct consequence of their national security role yet may lack the resources or capacity to address these risks independently. Cyber ARMOR is designed to offset the "negative externality" of increased cyber risk borne by these entities due to their service to military, defense industrial base and other national security related installations. The program provides direct support to help them meet elevated security requirements and address unique threat profiles associated with their critical roles.

  The program streamlines application and reporting processes to reduce the administrative burden for smaller or resource-constrained utilities, ensuring equitable access to federal support.
  The $20 million in funding is split between the Preparedness, Partnerships, and Response Assistance (PPRA) and Risk Management Tools (RMT) divisions.
  PPRA: Focuses on tailored technical assistance, grants, and hands-on training for utilities and energy

organizations. This includes incident response exercises, tabletop drills, and the development of organization-specific playbooks for high-risk scenarios.

RMT: Supports the applied research, development, and adoption of advanced resilience technologies specifically tailored for smaller, high-risk utilities. These efforts include areas such as development and deployment of lightweight, cost-effective monitoring and anomaly detection solutions suitable for limited-resource environments, development of rapid recovery and continuity-of-operations protocols for facilities with minimal IT staff, development and enhanced threat information sharing mechanisms designed for organizations with limited cybersecurity infrastructure.

- **R&D of Cybersecurity Situational Awareness & Information Sharing ($3 Million**): In support of CESER's mission to enhance cybersecurity threat awareness and information sharing within the U.S. energy sector. These funds will facilitate the modernization of 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. This investment strengthens threat information sharing tools and technologies for critical energy systems, advancing their capabilities for proactive threat detection. Modernizing CRISP ensures that the energy sector remains resilient against evolving cyber threats.

**Advance Tools to Manage Risks from Natural Hazards, Physical Threats, and EMP/GMD ($11.5 million)**

- **RD&D of Risk Management Tools and Technologies for Natural Hazards ($4 million)** RMT will conduct research and development that is targeted toward weather-related risks such as extreme winter weather, seismic events, and hurricanes. RMT will leverage emerging technologies to develop tools that help identify, characterize, detect, and mitigate risks to energy infrastructure. These tools will enable long term planning, allowing the industry to more effectively prepare for and respond to incidents.
- **RD&D of Tools and Technologies for Energy Infrastructure Resilience to Wildfires ($4 million)** RMT will develop technology solutions that enable the prevention, detection, and dynamic mitigation of growing wildfire risks. RMT will focus on developing and validating technologies that utilize real-life information to more accurately determine probable equipment and infrastructure failures. These investments will result in advancements in technologies and approaches such as advanced sensors, grid data analytics, satellite imagery, drones, and application of artificial intelligence.
- **RD&D of Tools and Technologies for Addressing Physical Threats to Energy Systems ($1.5 million)** RMT will develop and tailor tools and technologies to address physical attacks on energy infrastructure, such as substation shootings like those at the Metcalf Substation or in Moore County, the use of unmanned aerial systems (UAS) or drones, and positioning, navigation, and timing (PNT) risks.
- **Electromagnetic Pulse and Geomagnetic Disturbances ($2 million)** DOE will accelerate efforts to mitigate electromagnetic pulse (EMP) and geomagnetic disturbances (GMD) risks. These will include activities such as performing critical asset vulnerability assessments; conducting modeling studies to understand these hazards, developing innovative cost-effective mitigation options, and make minor lab operational costs and improvements.

**Supply Chain Cybersecurity Risk Management ($20 million)**

- **Energy Cyber Sense/ Cybersecurity Testing for Resilient Industrial Control Systems (CyTRICS) ($20 million)** CESER's Energy Cyber Sense program focuses on addressing supply chain cybersecurity threats to energy systems. The broader program will review national-level principles that develop tools and technologies, enable supply chain transparency, promote standards and best practices, and enhance technology and system designs. The CyTRICS program specializes in testing. It focuses on identifying and prioritizing critical equipment, tracking provenance, offering mitigation solutions, and disclosing vulnerabilities. As foreign adversaries and cybercriminal organizations continue to target critical energy infrastructure, CyTRICS is essential in proactively identifying, testing, and mitigating systemic vulnerabilities before they can be exploited. CyTRICS collaborates with energy sector manufactures and asset owners, leveraging classified threat intelligence for expert testing.

  In FY 2026, the program will expand the CyTRICS approach through a risk-based prioritization of systems and component testing. Partnerships with operational technology manufacturers will be developed, integrating the testing pipeline into the Energy Cyber Sense program. By integrating cybersecurity protections at the engineering level, enhancing threat intelligence collaboration, and modernizing industrial security standards, CyTRICS is fortifying the U.S. energy sector, including burgeoning technologies such as geothermal energy systems, against adversarial cyberattacks, systemic supply chain risks, and emerging threats to industrial resilience.

**Cyber Risk Assessments, Frameworks, and R&D Coordination ($8 million)**

- **Cyber-Informed and Consequence Driven Engineering ($5 million)** The Consequence-Driven Cyber-Informed Engineering (CCE) initiative is a key component of national defense ensuring energy critical infrastructure remains operational, secure against geopolitical conflicts and resilient against adversarial manipulation –leveraging the CIE framework, focuses on ensuring the resilience of critical energy infrastructure. CCE identifies vital functions and potential adversary actions to implement targeted risk mitigation. Operational CCE assessments enhance Critical Function Assurance (CFA) for high-risk assets essential for fuel and electricity supply and national security, evaluating personnel, processes, and technologies to significantly reduce compromise consequences. As cyber threats evolve, CCE will remain one of the most critical national security programs, providing the technical foundation to protect America's energy independence, military readiness, and economic stability. By combining engineering excellence, cybersecurity best practices, and intelligence-driven risk mitigation, CIE ensures that the U.S. remains at the forefront of global energy dominance.
- **Risk Management Guidance and Frameworks ($3 million)** RMT will continue to develop guidance, tools, and capabilities that can be used by the energy industry to integrate cybersecurity maturity evaluations with quantitative and qualitative risk data. These frameworks and tools will enable risk-informed cybersecurity investment decisions allowing for optimal utilization of limited resources. RMT will also continue to develop and maintain the Cybersecurity Capability Maturity Model (C2M2) tool features and resources including user community forum, facilitated evaluations, and updates needed to align with Cybersecurity Framework (CSF) V2.0. RMT will also continue research of usage and impacts of NIST CSF, C2M2, and C2M2 derivatives.

**Risk Management Tools & Technologies (RMT)**
**($K)**

| | FY 2024 Enacted | FY 2025 Enacted | FY 2026 Request | FY 2026 Request vs FY 2025 Enacted | |
|---|---|---|---|---|---|
| | | | | $ | % |
| Advance Tools to Manage Cyber Risk | 31,000 | 31,000 | 34,500 | +3,500 | +11% |
| Advance Tools to Manage Risks from Natural Hazards, Physical Threats, and EMP/GMD | 22,000 | 22,000 | 11,500 | -10,500 | -48% |
| Supply Chain Cybersecurity Risk Management | 29,000 | 29,000 | 20,000 | -9,000 | -31% |
| Cyber Risk Assessments, Frameworks and RD&D Coordination | 15,500 | 15,500 | 8,000 | -7,500 | -48% |
| University-based R&D and Cybersecurity Centers | 15,500 | 15,500 | 0 | -15,500 | -100% |
| **Total, Risk Management Tools & Technologies** | **113,000** | **113,000** | **74,000** | **-39,000** | **-35%** |

**Explanation of Changes for Risk Management Tools & Technologies**

A $39M decrease will be strategically redirected to streamline resource allocation towards advancing AI and Cyber Armor research, development, and implementation. This focused approach aims to accelerate cybersecurity defense innovations and bolster the resilience of owners and operators of critical energy assets.

## Response and Restoration (R&R)

### Overview

The Response and Restoration (R&R) division leads CESER's efforts to respond to incidents impacting the U.S. energy sector. The division maintains situational awareness, assesses threats, provides critical analysis of incident impact or potential impacts, and develops technical capabilities to support Federal interagency, State, Local, Tribal, and Territorial (SLTT), and industry partners. This division carries out DOE's emergency authorities for the energy sector. During a significant energy sector disruption requiring a coordinated Federal response, CESER's Energy Response Organization (ERO) activates to manage energy sector response efforts, share critical information, provide subject matter expertise and technical assistance to Federal and SLTT government partners and industry stakeholders.

### Highlights of the FY 2026 Budget Request

CESER will prioritize risk-informed response efforts and maintain its focus on regionally tailored support. CESER programmatic highlights include funding for EAGLE-I to maintain critical situational awareness of the Nation's energy system and support response operations, development of cyber response capabilities to address the growing cyber threats from nation-state and criminal actors.

**Incident Response ($3.5 million)**

- **Operations ($2.5 million)** CESER Incident Response Operations supports DOE's response to disruptive incidents affecting the energy sector, including Stafford Act and non-Stafford Act disasters, and manages CESER's support for National Special Security Events. In FY 2026, CESER will continue to deliver risk-informed, regionally focused support to help states and industry better prepare for and respond to region-specific threats. This includes delivering subject matter expertise to SLTT and industry partners via participation in exercises and direct support from Regional Coordinators and deployed responders. CESER will continue to train and coordinate a cadre of volunteer responders from across DOE to deploy virtually or physically to affected regions during disasters. When deployed, DOE's responder cadre conducts damage assessments, assists with restoration planning, and provides technical assistance to states and industry partners. CESER will also maintain its cadre of Regional Coordinators, who provide technical expertise to SLTT partners and other stakeholders year-round.
- **Logistics, Finance, and Administration ($1 million)** CESER will support energy sector emergency response and essential logistics, finance, and administration activities. 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.

**Situational Awareness, Analysis, and Technical Capabilities ($12.5 million)**

- **Situational Awareness and Analysis ($2.5 million)** CESER will maintain its situational awareness, analysis, and technical capabilities program to provide near continuous monitoring and analysis of incidents impacting, or potentially impacting, the U.S. energy sector to help ensure U.S. energy dominance. Funding will continue projects modeling potential impacts and rapid analysis to mitigate threats impacting U.S. energy systems, facilitating timely preparedness and response efforts across the full spectrum of hazards impacting the energy sector. CESER will further ongoing vulnerability analysis of key infrastructure assets and major metropolitan areas, which supports rapid response, contingency planning, and coordination with Federal partners, including the Department of Defense.
- **EAGLE-I and Situational Awareness Technical Capabilities ($6.1 million)** The Environment for Analysis of Geo-Located Energy Information (EAGLE-I) project encompasses both the flagship EAGLE-I data visualization web application and a number of associated initiatives and analytical capabilities to support energy sector situational awareness, predictive modeling, stakeholder exercises, and emergency response. CESER will continue to maintain the EAGLE-I situational awareness platform, expand the eligible user base, refine data sources and improve data quality, and use EAGLE-I as a training tool for Federal and state stakeholders. EAGLE-I will mature its remote sensing and modeling capabilities. EAGLE-I will continue to serve as a premiere energy sector situational awareness platform between deployed responders, DOE Headquarters personnel, and Federal and state stakeholders.
- **Cyber Technical Assistance Capabilities ($3.9 million)** The FY 2026 Budget ensures that CESER continues to provide leadership and energy sector cybersecurity expertise supporting significant energy sector cybersecurity incident response efforts, per the National Cyber Incident Response Plan (NCIRP) and other Administration

policies. Additionally, to fulfill DOE's responsibilities as the Sector Risk Management Agency for the energy sector, CESER will continue to develop and 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. These efforts ensure that the department can provide tailored support for cyber forensics in operational technology environments, analysis of malware, and conduct proactive and response focused cyber hunts with industry, to support the Departments national security mission.

**Energy Threat Analysis Center (ETAC) ($10 million)**

The Department operationalized the Energy Threat Analysis Center (ETAC) in FY 2025 to address the increasingly active and sophisticated cyber threats to the U.S. energy sector through operational collaboration. The ETAC will continue to leverage insights from energy sector owners and operators, the DOE National Laboratories, and the Intelligence Community to exchange data, 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, predictive threat analysis, and coordinated response capabilities.

- **ETAC Operations and Maintenance** CESER will continue to operate as a classified and unclassified collaboration hub that integrates government, industry, and national laboratories capabilities to detect and respond to emerging threats before they cause widespread disruption includes maintaining a partnership structure and environment for operational collaboration that provides a common understanding of threats to the energy sector. CESER will operate and expand the in-person ETAC hub that brings together government and industry analysts for real-time collaboration on threats. CESER will also maintain capabilities, such as a data platform, which facilitates the exchange of information and collective analysis between government and industry.
- **ETAC Tools and Technology** CESER will operationalize advanced tools and analytic capabilities to enhance the analysis of sophisticated cyber threats. The FY 2026 Budget will support the deployment of new analytic capabilities for data aggregation and threat identification. These technologies directly support the ETAC's ability to develop products with specific recommendations and mitigation techniques tailored to the unique needs of the energy sector. Future developments may include AI-enhanced cyber intelligence operations, deep-learning threat detection, and autonomous cyber defense systems to counteract increasingly sophisticated adversarial cyber campaigns. By integrating cutting-edge intelligence operations with real-time cybersecurity and emergency preparedness, ETAC ensures that the U.S. remains energy-secure, cyber-resilient, and fully prepared for future adversarial threats.

**Response and Restoration (R&R)**
**($K)**

| | FY 2024 Enacted | FY 2025 Enacted | FY 2026 Request | FY 2026 Request vs FY 2025 Enacted | |
|---|---|---|---|---|---|
| | | | | $ | % |
| **Response and Restoration** | | | | | |
| Incident Response | 7,000 | 7,000 | 3,500 | -3,500 | -50% |
| Situational Awareness, Analysis, and Technical Capabilities | 20,500 | 20,500 | 12,500 | -8,000 | -39% |
| Energy Threat Analysis Center (ETAC) | 5,000 | 5,000 | 10,000 | +5,000 | +100% |
| **Total, Response and Restoration** | **32,500** | **32,500** | **26,000** | **-6,500** | **-20%** |

**Explanation of Changes for Response and Restoration**

CESER will prioritize high-quality emergency response capabilities. CESER plans to realign R&R program controls to correspond with the organization and operational structure to support a more effective budget execution. While reduced, the Incident Response budget will provide contractor support and responder training, development, and recruitment. The Situational Awareness, Analysis, and Technical Capabilities enables continued operations for DOE's energy sector situational awareness platform (EAGLE-I), targeted refinement of tools and capabilities for rapid analysis of novel cyber security threats and allows for a smaller number of focused cyber technical assistance projects/activities with industry partners.

## 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, including 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 the interagency, and strengthening human resources, procurement and budget staff to support CESER programmatic activities.

**Travel** includes transportation, per diem, and incidental expenses allowing CESER to effectively deliver on its mission. Major drivers of travel include the need to oversee the development and deployment of risk management tools, programs, and projects in the field; attendance at industry, interagency and regional state government energy sector engagements as well as emergency response coordination meetings.

**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 2026 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 2026 request ensures that 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**
**Funding ($K)**

| | FY 2024 Enacted | FY 2025 Enacted | FY 2026 Request | FY 2026 Request vs FY 2025 Enacted | |
|---|---|---|---|---|---|
| | | | | $ | % |
| Salaries and Benefits | 17,045 | 17,045 | 13,800 | -3,245 | -19% |
| Travel | 400 | 400 | 300 | -100 | -25% |
| Support Services | 4,016 | 4,016 | 3,000 | -1,016 | -25% |
| Other Related Expenses | 2,739 | 2,739 | 2,450 | -289 | -11% |
| **Total, Washington Headquarters** | **24,200** | **24,200** | **19,550** | **-4,650** | **-19%** |
| | | | | | |
| Salaries and Benefits | 2,000 | 2,000 | 1,900 | -100 | -5% |
| Travel | 115 | 115 | 100 | -15 | -13% |
| Support Services | 450 | 450 | 350 | -100 | -22% |
| Other Related Expenses | 1,235 | 1,235 | 1,100 | -135 | -11% |
| **Total, National Energy Technology Laboratory** | **3,800** | **3,800** | **3,450** | **-350** | **-9%** |
| | | | | | |
| Salaries and Benefits | 19,045 | 19,045 | 15,700 | -3,345 | -18% |
| Travel | 515 | 515 | 400 | -115 | -22% |
| Support Services | 4,466 | 4,466 | 3,350 | -1,116 | -25% |
| Other Related Expenses | 3,974 | 3,974 | 3,550 | -424 | -11% |
| **Total, Program Direction** | **28,000** | **28,000** | **23,000** | **-5,000** | **-18%** |
| | | | | | |
| **Federal FTEs** | 62 | 62 | 57 | -5 | -8% |
| Additional FE FTEs at NETL supporting CESER[1] | 11 | 11 | 9 | -2 | -18% |
| **Total CESER-funded FTEs** | **73** | **73** | **66** | **-7** | **10%** |
| | | | | | |
| Technical Support | 3,828 | 3,828 | 2,750 | -1,078 | -28% |
| Management Support | 638 | 638 | 600 | -38 | -6% |
| **Total, Support Services** | **4,466** | **4,466** | **3,350** | **-1,116** | **-25%** |
| | | | | | |
| Other Services | 200 | 200 | 266 | +66 | +33% |
| EITS Desktop Services | 866 | 866 | 866 | 0 | 0% |
| WCF | 2,908 | 2,908 | 2,418 | -490 | -17% |
| **Total, Other Related Expenses** | **3,974** | **3,974** | **3,550** | **-424** | **-11%** |

[1] CESER funds FTEs at FE's National Energy Technology Laboratory who support CESER activities. These 11 FTEs are in FE'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 2025 Enacted | FY 2026 Request | Explanation of Changes FY 2026 Request vs FY 2025 Enacted |
|---|---|---|
| **Program Direction** | | |
| **$28,000** | **$23,000** | **-$5,000** |
| *Salaries and Benefits* | | |
| *$19,045* | *$15,700* | *-$3,345* |
| For 62 FTEs at HQ and 11 FTEs at NETL that provide executive management, programmatic oversight, and analysis for the effective implementation of CESER programs. | For 57 FTEs at HQ and 9 FTEs at NETL that provide executive management, programmatic oversight, and analysis for the effective implementation of CESER programs. | Reduces 57FTEs at HQ and 2 FTEs at NETL in alignment with the reduction in program activities. |
| *Travel* | | |
| *$515* | *$400* | *-$115* |
| Travel includes transportation, subsistence, and incidental expenses that allow CESER to effectively facilitate its mission. | Includes transportation, subsistence, and incidental expenses for both international and U.S. travel that allow CESER to effectively facilitate its mission. | Decreased due to decreased FTE count, and accounting for cost inflation and in-person travel needs. |
| *Support Services* | | |
| *$4,466* | *$3,350* | *-$1,116* |
| 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. | Decreased due to restructuring of support for efficiency and cost effectiveness. |
| *Other Related Expenses* | | |
| *$3,974* | *$3,550* | *-$424* |
| Includes equipment upgrades and replacements, office furniture, minor construction, commercial credit card purchases using simplified acquisition procedures when possible, and miscellaneous expenditures. | Includes required equipment upgrades and replacements for new and existing staff, office furniture, construction, commercial credit card purchases using simplified acquisition procedures when possible, general and advanced training, and miscellaneous expenditures. | Decreased WCF, EITS, and general training associated with Federal workforce growth. |