Cybersecurity, Energy Security, and Emergency Response

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, $245,475,000, to remain available until expended: Provided, That of such amount, $32,475,000 shall be available until September 30, 2025, for program direction.

(Energy and Water Development and Related Agencies Appropriations Act, 2023.)

Public Law Authorizations
Public Law 95–91, "Department of Energy Organization Act", 1977
Public Law 109-58, "Energy Policy Act of 2005"
Public Law 110-140, "Energy Independence and Security Act, 2007"
Public Law 114-94, "Fixing America's Surface Transportation Act", 2015
Public Law 110-246, "Division Z Energy Act", 2020

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

FY 2022 Enacted	FY 2023 Enacted	FY 2024 Request
185,804	200,000	245,475

Overview

The U.S. Department of Energy's (DOE's) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) leads the Department's efforts to strengthen the security and resilience of U.S. energy infrastructure against all threats and hazards, mitigate impacts from cybersecurity, physical, supply chain, and climate-based events, and assist with response and restoration activities. CESER is the Office responsible for DOE's responsibilities as lead agency for Emergency Support Function #12 (Energy), or ESF #12, under the National Response Framework, the Sector Risk Management Agency (SRMA) for the energy sector per the 2002 Homeland Security Act (as amended), and the Sector Specific Agency (SSA) for the energy sector per the 2015 Fixing America's Surface Transportation Act. In those roles, DOE leads national efforts to enhance the preparedness, resiliency, and recovery of the U.S. energy infrastructure from all threats and hazards.

As climate-based and cybersecurity risks continue to grow exponentially, CESER plays a critical role in conducting advanced risk analysis; representing the Department at National Security Council (NSC) meetings on national-level security and resilience policies; mitigating risks by informing Federal and State, Local, Territorial, and Tribal (SLTT) national security and resilience policies; researching, developing, and demonstrating (RD&D) tools and technologies; and supporting energy sector (electricity, oil, and natural gas) emergency preparedness and response efforts. CESER accomplishes its mission through strong partnerships with energy sector owners and operators, States and local communities, intra-agency partners, interagency partners, manufacturers, technology companies, academia, and international partners.

The U.S. energy sector is considered one of the "lifeline sectors" since nearly all other critical infrastructure sectors rely on the reliable delivery of electricity, oil, and natural gas. This includes hospitals, military installations, water and wastewater facilities, communications, and transportation. Further, as the U.S. energy sector rapidly evolves to address the impacts of climate-based risks through the historic investments under the Infrastructure Investment and Jobs Act (IIJA) and the Inflation Reduction Act (IRA), it is more important to ensure those next-generation energy systems are designed and deployed with security and resilience in mind.

With that in mind, CESER's fiscal year 2024 (FY 2024) Request spans three divisions: Preparedness, Policy, and Risk Analysis[a]; Risk Management Tools and Technologies, and Response and Restoration. The three divisions work together from preparing the U.S. energy sector through advanced risk analysis and policy development to informing the RD&D of next generation tools and technologies and then leveraging the analysis and tools to respond during an emergency. The response, whether it's the Colonial Pipeline cyberattack or Hurricane Fiona in 2022, informs CESER and Department-wide preparedness, recovery, and RD&D priorities. Finally, the Office of Petroleum Reserves (OPR) is the newest division in CESER and is detailed in a separate request. OPR is one of the strongest tools in the U.S. government's toolbox to address critical fuel supply constraints, particularly in the face of domestic and global issues and threats, affecting the availability of oil, heating oil, and gasoline across the country and is an integral part of CESER.

CESER's FY 2024 Request will:

- **Strengthen U.S. energy sector security and resilience through advanced risk analysis** by leveraging the analytical capabilities of DOE's National Laboratories and through partnerships with industry and the SLTT community. As the energy sector's SRMA, CESER is tasked with understanding and addressing the sector's growing climate-based and cybersecurity risks. In FY 2024, CESER will strengthen these capabilities, which will not only assist industry and SLTT

[a] Legacy Information Sharing, Partnerships and Exercises (ISPE) became Preparedness, Policy, and Risk Analysis in FY24

entities to better address risks, but also help other DOE offices as they design and deploy next generation energy systems such as solar, wind, and hydrogen or continue to expand transmission, nuclear, and battery storage across the country. This work will also support national security efforts to strengthen Defense Critical Energy Infrastructure (DCEI) in light of growing cybersecurity threats.

- **Integrate cybersecurity and resilience into the energy sector industrial base** through partnerships with manufacturers, technology companies, standards organizations, and academia. In June 2022, CESER released the National Cyber-Informed Engineering (CIE) Strategy that outlines specific goals to achieve "security by design" in U.S. energy systems. In addition to executing the CIE Strategy, CESER is committed to strengthening its supply chain risk management initiatives under the Energy Cyber Sense program. The Energy Cyber Sense program will look at everything from supply chain standards (e.g., NIST) and policies (e.g., North American Electric Reliability Corporation's Critical Infrastructure Protection standards) to building the capabilities, resources, and guidance that enables energy industrial base to strengthen hardware and software security and inform the design of next generation systems. This supports a long-term vision of developing secure and trusted supply chains domestically.

- **Reduce risks to the electricity, oil, and natural gas systems through threat-informed research, development, and demonstration** of next generation tools and technologies that provide U.S. energy companies cutting-edge protection, monitoring, detection, response, containment, forensics, and recovery capabilities. U.S. energy systems are evolving rapidly to address the impacts of climate-based risks, meet customer expectations for reliability and resiliency, and ensure safety and efficiency. Therefore, it is imperative that CESER invest in tools and technologies that keep pace with those systems and work with States and communities on hardening measures. In 2022, the energy sector experienced increased physical security threats to grid infrastructure. CESER's FY 2024 Budget Request seeks to develop frameworks, tools, and technologies to support grid owners and operators to mitigate physical security threats. Finally, CESER invests in both next generation tools and technologies to address cybersecurity threats, climate-based risks (e.g., wildfires), and high-impact, low frequency (HILF) events such as geomagnetic disturbances (GMD) and electromagnetic pulse (EMP).

- **Build security and resiliency capacity across industry and SLTT entities through exercises, training, technical assistance, and workforce development initiatives.** To build security and resilience at all levels, it is critical that CESER partners with the energy sector community in States and local communities as well as with industry. To that end, CESER will expand sponsoring industry, State and regional exercises, develop and expand cybersecurity training for owners and operators to address emerging cybersecurity threats, and strengthen the resilience of energy systems that feed critical defense facilities. Further, CESER will invest in cybersecurity workforce development to ensure that the energy sector has a strong, trained workforce to meet the cybersecurity challenges today and those ahead.

- **Strengthen emergency preparedness and response capabilities by enhancing CESER's ability to address all hazards impacting or potentially impacting the energy sector**, by reducing those impacts at the regional and State levels, in coordination with industry partners. CESER will expand its regional presence to increase the value provided to sector, regional, and SLTT partners during steady State through activities such as State Energy Security Planning, joint training and exercises, and other activities to develop and grow the strong relationships necessary during active emergency response. To meet these needs, CESER will increase regionally based federal staffing, and explore mission needs, requirements, and alternatives for CESER regionally based response centers. Further, CESER will continue to develop the Energy Threat Analysis Center (ETAC) pilot in partnership with industry, National Laboratories, the intelligence community, and the Cybersecurity and Infrastructure Security Agency's (CISA) Joint Cyber Defense Collaborative.

Highlights and Major Changes in the FY 2024 Budget Request

- **Preparedness, Policy, and Risk Analysis** ($39,000,000) engages in collaborative risk management with the energy industry and SLTT partners to enhance energy sector security and resilience. These efforts will advance the Department's efforts to analyze, prepare for, mitigate, and recover from all threats and hazards facing the U.S. energy sector. CESER will achieve this through information sharing, strategic industry engagements, risk assessments, capacity building in planning and resilience, and targeted training and exercises. The increased funding will allow for an expanded risk and resilience analysis capability and actions to mitigate and, in some cases even avoid, the impacts of energy supply disruptions, with a focus on ensuing the most vulnerable and underserved communities' needs are addressed in energy security planning, response, risk assessment, and mitigation actions. A key focus of the analysis will be local, State, and regional risk assessments to identify critical energy infrastructure and asset vulnerabilities as well as any single points of failure. Key upstream dependencies and downstream dependent markets would also be identified as well as mitigation strategies. As the SRMA for energy, this work will allow a thorough understanding of risks that are a priority for the energy sector and collaborate with partners to buy down this risk for a more secure and resilient energy infrastructure, including, but not limited to, climate adaptation, hurricanes/severe weather, wildfires, earthquakes, cyberattacks, electromagnetic interference, third-party and supply chain risks, risks arising out of cybersecurity workforce shortages and emerging risks to renewable energy generation and distributed energy resources (DERs).

- **Risk Management Tools and Technologies** ($135,000,000) leads the research, development, and demonstration for the Department focused on tools and technologies to address cybersecurity, physical, natural hazard, and other threats to the U.S. energy sector. This division also leads efforts to integrate cybersecurity across DOE's applied energy and science offices. CESER will invest in frameworks, tools, and technologies to identify, protect, prevent, mitigate, and respond to threats to energy systems. The funding will focus on emerging cybersecurity risks including: security for operational technology (OT) environments with increased grid integration and cloud adoption, securing the diverse communications networks and protocols, and hardening energy systems for a post-quantum world. Additionally, an expanded focus on the Energy Cyber Sense program, will allow for a range of supply chain security efforts as the Cyber Testing for Resilient Industrial Control Systems (CyTRICS) initiative, development of a framework for energy sector software bill of materials and hardware bill of materials, and other similar efforts. RMT will also address risks such as geomagnetic disturbances (GMD) and electromagnetic pulse (EMP) and physical threats to critical energy infrastructure. RMT will include a renewed focus on developing tools and technologies to mitigate risks facing the energy sector from increasing hurricanes, wildfires, flooding, and other natural hazards. Finally, the RMT funding includes establishing the Cyber and Energy Resilience Center of Excellence.

- **Response and Restoration** ($39,000,000) coordinates a national effort to ensure the sector can respond to and restore energy systems from emergencies resulting from natural hazards, cyberattacks, physical attacks, and other threats facing energy infrastructure. This line of effort leads DOE and CESER's roles as Emergency Support Function (ESF) #12 – Energy and SRMA/SSA in support of Presidential Policy Directive (PPD)-41 *United States Cyber Incident Coordination*. CESER works with partners in the energy sector to assess the impacts of disasters on local and regional energy infrastructure; provide situational awareness updates to Federal, State, and private sector partners; facilitate legal and regulatory waivers to accelerate restoration of damaged energy systems; and provide technical expertise on energy damage assessment, restoration, mitigation, and logistical assistance. CESER's analytical capabilities to assess and mitigate risks and threats to energy infrastructure has proven critical during events such as Hurricane Ida, Colonial Pipeline ransomware cyberattack, and others, and increased funding will allow for additional situational awareness capabilities through the Situational Awareness Watch Office. The Environment for Analysis of Geo-Located Energy Information (EAGLE) situational awareness monitoring program is critical capability that has been moved from CESER's RMT program as the tool has matured and is now being fully implemented with the R&R division. CESER's response and restorations are often carried out close partnership with agencies such as the FEMA, DHS/CISA, Federal Bureau of Investigation (FBI), and the Intelligence Community. An expansion of CESER's regionally based operations and increased integration with the PPRA divisions' SLTT program will enhance the partnerships and relationships necessary for effective and efficient emergency response. Finally, R&R includes funding for the ETAC pilot, which will act as a hub for DOE's cybersecurity threat joint collaboration with the energy sector. The ETAC pilot, which has broad support by the energy sector owners and operators, the White House, interagency partners such as CISA, and others, will enable DOE to more closely partner with the sector on cybersecurity threat situational awareness and response.

FY 2022 Key Accomplishments

CESER had a number of accomplishments FY 2022, which are having a demonstrable impact on the security and resilience of the sector:

- Continued to support industry on cybersecurity risk identification and mitigation across a number of functions including:
    - Completed 5-year planning process with Electricity Information Sharing and Analysis Center (E-ISAC) on the future of Cybersecurity Risk Information Sharing Program (CRISP). CRISP is the flagship information sharing program for the electric sector, and allows private sector entities to share information about their internet perimeters with E-ISAC and DOE for the purpose of provide awareness of nation State level threats that may be targeting that entity. DOE supports the program by providing funding that prioritizes visibility for entities that have a nexus with national critical infrastructure priorities and funds research and development to ensure technology used is in line with existing practices for network monitoring. CRISP members also contribute to the program through the E-ISAC, who leverage PNNL as the prime contractor. CESER sponsors the CRISP effort in partnership with the E-ISAC, bringing together resources from across the DOE Complex and coordination with industry stakeholders to provide visibility into cybersecurity threats targeting United States critical electric infrastructure. CESER also completed development of the next generation Information Sharing Device, which is the sensor used by CRISP, providing greater interoperability and capability that is standard with the interagency.

    - Engaged with energy sector partners at the unclassified and classified levels to identify risks posed by Russia's unprovoked and unjust invasion of Ukraine. CESER developed a number of products to advise the energy sector of those risks and provided them to the owners and operators. Further, CESER was instrumental in providing grid equipment and cybersecurity support to Ukrainian energy companies in collaboration with of DOE's Office of International Affairs.

    - Developed a report on *Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid*. This report provides an overview of cybersecurity considerations that should be considered by the electric sector, including utilities and distributed energy resource (DER) operators, providers, integrators, developers, and vendors, as well as policymakers as we embark on this transformational change to the U.S electric grid. This report will help inform future risk analysis, RD&D, and emergency response efforts going forward. For the release, CESER held a webinar with industry partners and participated in media outreach (e.g., podcasts) to educate them on the importance of the findings. Industry feedback has been extremely positive, and the report has facilitated outreach into these critical DER communities.

- Partnered with the Electricity Subsector Coordinating Council (ESCC) on critical issues on energy resilience and cybersecurity including launching a Supply Chain Tiger Team in response to concerns repeatedly expressed by the electric utilities regarding increased supply chain risk, with a focus on distribution transformers. Another key focus area has been on solutions focused on wildfires risk mitigation. By facilitating a whole of government approach, to the ESCC wildfire working group was able to work towards a host of solutions, including Bureau of Land

Management and Department of Interior establishing a new permitting process for the master special use permits with utilities.

- Continued to partner with SLTT governments and industry partners on preparedness activities. Highlights include:
    - Over 4,000 State energy officials, governors, energy advisors, public utility commissioners, State legislators, and emergency managers participated in CESER-supported events and training for energy security, resilience and cybersecurity planning in FY 2022.

    - In partnership with the National Association of State Energy Officials, released an Energy Emergency Response Playbook to provide State and territory energy officials with a starting point for energy emergency response planning. The playbook includes a framework for evaluating energy emergencies, guidance, and templates for response actions, as well as planning, monitoring, and response resources. The playbook is designed to be customized by States and align with their State Energy Security Plans (SESPs).

    - CESER supported States in their effort to develop a SESP that met the criteria of IIJA Section 40108 by developing and releasing SESP framework and guidance, nine "drop-in" SESP resources. SESPs describe the State's energy landscape, people, processes, and the state's strategy to build energy resilience. More specifically, the plans detail how a State, working with energy partners, can secure their energy infrastructure against all physical and cybersecurity threats; mitigate the risk of energy supply disruptions to the State; enhance the response to, and recovery from, energy disruptions; and ensure that the State has secure, reliable, and resilient energy infrastructure. The requirement to propose methods to strengthen energy security abilities of the State can be used to inform policy, legislation, and budget priorities to mitigate the State's energy sector risks. Over 50% of states who updated their plans in 2022 utilized the CESER drop-in resources.

    - Partnered with the National Association of Regulatory Utility Commissioners (NARUC to support cybersecurity training to State public service commissioners and their staff. 82% of participants demonstrated gains in cybersecurity knowledge post-training.

    - Sponsored and supported over 40 preparedness exercises, including at least 500 participants from the energy sector (industry), State, local, federal, and other critical infrastructure partners. These exercises focused on improving energy resilience, security and cybersecurity. CESER's capstone annual all-hazards Clear Path exercise series included a focus on DOE and the energy sector's multi-hazard response capabilities, resulting in defined resource and supply chain areas. The series also included a resilient communications drill and a social media drill focusing on coordinated responses to mis-, dis-, and mal-information campaigns. CESER successfully conducted its cyber-focused exercise Liberty Eclipse, which leverages a physical testbed environment replicating the electric grid and the operational technology found at substations throughout the Nation. This testbed provides a hands-on training environment opportunity for industry partners to test and evaluate their deployed cybersecurity defenses against a simulated adversary consisting of National Laboratory personnel. Follow-on analysis and corrective action discussions between industry and the simulated adversary provides opportunity to modify and recognize follow-on attack strategies, which can be included in a utility's real-world operating system and procedures.

      CESER's cybersecurity training programs successfully supported industry partners' cybersecurity resilience and preparedness domestically and internationally. As an example, CyberStrike^{TM}, CESER's professional cybersecurity training for operational technology environments was delivered 16 times in FY 2022 (includes both domestic and international deliveries). The hands-on training opportunities CyberStrike^{TM}

helps the existing cybersecurity workforce to understand how adversaries conduct cybersecurity campaigns against industrial control systems used in the energy sector and the skills needed to counteract these threats.

In response to recommendations by the U.S. Cyberspace Solarium Commission and to support the needs of energy sector senior level operational technology security managers, CESER conducted its second year of the Operational Technology Defender Fellowship (OTDF) and expanded the cohort to 15 participants (which included diverse representation from DER-focused company) and in-person sessions with critical cybersecurity and U.S. Intelligence Community partners. The increased engagement opportunities allowed participants to more fully understand the cybersecurity strategies and tactics adversarial State and non-state actors use in targeting U.S. energy sector infrastructure; the roles and capabilities of U.S. departments and agencies to support critical infrastructure owners and operators; and serves as a bi-directional information and idea exchange forum between government and energy sector experts, contributing to the collective advancement of improved cybersecurity and information sharing capabilities and processes. Participants attend four in-person sessions, including a scenario-driven capstone exercise where the cohort will demonstrate the understanding of key federal cybersecurity policies, roles and responsibilities, public and private collaborative programs and themes, and other takeaways learned throughout the year.

  - As part of CESER's Defense Critical Energy Infrastructure (DCEI) program, partnered with the U.S. Department of Defense on risk assessments of energy infrastructure supporting critical defense facilities. This all-hazards assessment is looking at cybersecurity, physical, climate, weather, and other threats to the installations for completion in FY 2023.

- Completed 20 research and development (R&D) projects along with transitioning seven technologies into practice at energy companies. The General Electric "Cyber-Physical Resilience for Wind Power Generation" R&D project completed a three-week demo of new cyber-physical security system for wind turbines and successfully detected the presence of attacks and located the sensor signals being manipulated in the testing. The CESER SEL Ambassador project successfully transitioned to practice a solution architecture for reducing cybersecurity risks and enhancing situational awareness for utility providers and industrial operations.

- RMT funded research using quantum communications to protect power grid control signals from third party infiltration was announced as finalist for the prestigious R&D 100 Award.

- Released a $45M Funding Opportunity Announcement (FOA) to strengthen the cybersecurity of next generation energy systems through RD&D that will create, accelerate, and test technology to protect our energy systems from cyberattacks. Further, CESER executed a $12M FOA to establish a network of university-based, regional cybersecurity R&D centers across the nation. Finally, CESER awarded $12M for six university-based RD&D projects focused on the development of cutting-edge cyber-physical platform tools and technologies that can detect and mitigate incidents in electric power systems.

- Released version 2.1 of the globally adopted Cybersecurity Capability Maturity Model (C2M2) along with supplemental guidance and an online tool. The new version was developed with inputs from 145 cybersecurity experts from 77 energy sector and cybersecurity organizations and pilot validation at nine energy companies. In the months following the release of C2M2 version 2.1, an average of more than 2,500 monthly unique users accessed the HTML-based C2M2 tools. The C2M2 is used both domestically and abroad by organizations in energy and other critical infrastructure sectors.

- Continued engagement with the Securing Energy Infrastructure Executive Task Force to convene key stakeholders from all levels of government, industry, academia, and the National Labs to jointly address priority technical vulnerabilities in energy systems. The Task Force developed a National Cyber-Informed Engineering Strategy and identified cybersecurity standards for OT environments.

- Funded initiative to leverage Artificial Intelligence to improve the accuracy of wildfire risk predictions was showcased by the Frontier Development Lab.

- In FY 2022, the Cyber Testing for Resilient Industrial Control Systems (CyTRICS) program tested 11 systems leveraging unparalleled technical expertise from the National Labs. The program has participation agreements with critical energy sector manufacturers and asset owners and is testing components of priority policy and security importance and expanded participation by adding a vendor. CyTRICS testing has identified 28 vulnerabilities, which have been mitigated in current systems and are informing more secure designs for future models. But more importantly, close coordination with vendors during testing helped to reduce the average cycle time from vulnerability discovery to mitigation and asset owner notification by 71% from the 2021 baseline.

- ESF #12 team spent 169 days activated during 2022 responding to two hurricanes, two tropical storms, flooding in Kentucky, wildfires in New Mexico, sargassum seaweed overgrowth in the United States Virgin Islands, and six National Special Security Events.

- Expanded products and tools including the use of the Survey 123 application to gather photos and videos during damage assessments during four 2022 response events, with more than 50 surveys submitted from the field, enabling real-time situational awareness reporting, and more informed decision making related to infrastructure damage.

- Implemented a targeted ESF #12 recruitment plan, which made an immediate impact during the 2022 response season. The Energy Response Organization (ERO) conducted targeted recruitment from DOE divisions such as the Grid Deployment Office (GDO) who can complement the CESER ERO mission by providing specialized expertise with transmission, grid modernization, and power generation. The GDO knowledge was critical to separate response and restoration activities from recovery activities, and transition of mission requirements seamlessly within DOE.

- In 2022, ESF #12 trained 96 responders, including 12 new to the program for various response functions, including Energy Specialist, Energy Unit Lead, and Catastrophic Incident Response Team.

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

	FY 2022 Enacted	FY 2023 Enacted	FY 2024 Request	FY 2024 Request vs FY 2023 Enacted ($)	FY 2024 Request vs FY 2023 Enacted (%)
Preparedness, Policy, and Risk Analysis[a]	19,000	26,857	39,000	+12,143	+45.2%
Risk Management Tools & Technologies	129,804	125,000	135,000	+10,000	+8.0%
Response and Restoration	18,000	23,000	39,000	+16,000	+69.6%
Program Direction	16,000	25,143	32,475	+7,332	+29.2%
Congressionally Directed	3,000	0	0	0	0.0%
Total, Cybersecurity, Energy Security, and Emergency Response	**185,804**	**200,000**	**245,475**	**+45,475**	**+22.7%**
Federal Full Time Equivalent Employees (FTEs)	44	93	113	+20	21.5%
Additional FE FTEs at NETL supporting CESER[b]	9	11	11	0	0.0%
Total CESER-funded FTEs	**53**	**104**	**124**	**+20**	**19.2%**

SBIR/STTR:

- FY 2023 Enacted: SBIR/STTR: $2,482
- FY 2024 Request: SBIR/STTR: $2,491

[a] Legacy Information Sharing, Partnerships and Exercises (ISPE) became Preparedness, Policy, and Risk Analysis in FY24

[b] CESER funds FTEs at FECM's National Energy Technology Laboratory who are FECM employees, but support CESER activities. The FTEs are in FECM's FTE totals and are not included in the CESER's FTE totals shown on the "Federal Full Time Equivalent Employees (FTEs)" line.

Infrastructure Investment and Jobs Act ($K)

Appropriated Funding Organization	FY 2022 IIJA Funding	FY 2023 IIJA Funding	FY 2024 IIJA Funding	Managing Organization
Cybersecurity, Energy Security, and Emergency Response (CESER)				
Rural and Municipal Utility Adv Cybersecurity Ass Sec. 40124	50,000	50,000	50,000	CESER
Cybersecurity for the Energy Sector RD&D Sec. 40125b	50,000	50,000	50,000	CESER
Energy Sector Op Support for Cyberresilience Sec. 40125c	50,000	0	0	CESER

- **Rural and Municipal Utility Advance Cybersecurity Assessment Sec. 40124:** The goal of this investment is to enhance the security posture of rural, municipal, and small investor-owned electric utilities through investments in operational capabilities, services, technology deployments, and threat intelligence information-sharing. The FY 2024 planned activities will provide funding and technical assistance to eligible entities to: harden their cybersecurity systems and processes; improve cybersecurity incident preparedness and incident response capabilities; improve the knowledge, skills, and abilities of utility staff through cybersecurity training and technology deployments, with a specific focus on utilities serving military installations; and increase the participation of eligible utilities in threat information sharing programs. These activities will accelerate the ability of eligible entities to protect against, detect, respond to, and/or recover from a cybersecurity threat.
- **Cybersecurity for the Energy Sector RD&D Sec. 40125b:** The goal of this investment is to enhance energy sector cybersecurity through research development and demonstration of emerging technologies that are scalable and through identifying and reducing cybersecurity workforce gaps. The FY 2024 planned activities will continue to support research, development, and demonstration (RD&D) projects securing energy delivery systems. Additionally, this program will support workforce development activities for energy sector cybersecurity.
- **Energy Sector Operational Support for Cyberresilience Sec 40125c:** The goal of this investment is to enhance the Department's emergency response capabilities and testing in coordination with the other agencies, National Labs and private industry and provide technical assistance to municipal and cooperative utilities to improve cybersecurity maturity levels. Additionally, this investment is for increased intelligence community sharing and enhanced/expanded tools for monitoring the status of the energy sector. The FY 2024 planned activities are primarily centered on the ETAC Pilot. The ETAC Pilot will bring subject matter experts from the federal government and energy sector together to analyze and address threats and risks to the energy system, provide timely and actionable warnings to the energy sector and develop whole-of-sector recommendations for mitigations and defensive measures, and support DOE's emergency response functions as Sector Risk Management Agency and lead for Emergency Support Function #12 (Energy).
- 40125d: CESER's Preparedness, Policy, and Risk Analysis will manage the funds originally appropriated to the Electricity appropriations account.

Future Years Energy Program (FYEP)
($K)

	FY 2024 Request	FY 2025	FY 2026	FY 2027	FY 2028
Cybersecurity, Energy Security, and Emergency Response	245,475	251,000	256,000	262,000	268,000

Outyear Priorities and Assumptions

In the FY 2012 Consolidated Appropriations Act (P.L. 112-74), Congress directed the Department to include a future-years energy program (FYEP) in subsequent requests that reflects the proposed appropriations for five years. This FYEP shows outyear funding for each account for FY 2025 - FY 2028. The outyear funding levels use the growth rates in outyear account totals published in the FY 2024 President's Budget for both the 050 and non-050 accounts. Actual future budget request levels will be determined as part of the annual budget process.

CESER priorities in the outyears include the following:

- Invest in industry and State capacity building to manage risk
- Establish training and exercises to include leveraging cyber-physical testbed and ranges to address real-world threats
- Overcome cybersecurity workforce challenges
- Promote energy justice through studies of economically disadvantaged communities for response and recovery
- Development of risk management tools, and advanced threat information sharing tools for sector wide awareness
- Expanded regional approach to emergency response efforts
- Development of Cyber-Physical emergency response expertise

Preparedness, Policy, and Risk Analysis (PPRA)

Overview

The U.S. energy sector is characterized by widely diverse infrastructure components, a multifaceted operational environment, and complex ownership and regulatory structures. As one of the priority enabling functions upon which all other critical infrastructure sectors rely, the Nation's security, public health and safety, and economy depend on energy. With the sector facing evolving threats and risks, such as natural disasters, changing conditions, cybersecurity and physical security threats, aging and evolving technologies in infrastructure, and shortage of a skilled cybersecurity workforce, a critical component of preparedness is working with the energy sector to assess risk. As the Sector Risk Management Agency (SMRA) for energy, the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) continuously assesses priority energy sector risks, including, but not limited to, hurricanes/severe weather, wildfires, climate adaptation, earthquakes, cyberattacks, electromagnetic interference, third-party and supply chain risks, risks arising out of cybersecurity workforce shortages, and emerging risks to renewable energy generation and distributed energy resources (DERs).

Within CESER, the Preparedness, Policy, and Risk Analysis (PPRA)[a] division is focused on cultivating strong partnerships across all levels of government and private industry, with insights and support from academia and laboratory partnerships to identify, assess, and manage risk. PPRA also works to build sector capacity to support security and resilience of critical energy infrastructure and the communities that rely on it through sharing information, building preparedness, and promoting learning and adaption through strategic partnerships. PPRA's overarching goal is risk reduction in the energy sector with efforts that aim to buy down this risk through the activities described in this Request.

PPRA is the 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 energy critical infrastructure protection, energy security, risk mitigation, resilience, emergency preparedness, and recovery efforts.

The Department has emphasized support for Executive Order 13636, Section 9 companies[b], Defense Critical Energy Infrastructure (DCEI) companies, and investor owned, municipal, and cooperative utilities in addition to SLTT energy agencies in this request. PPRA's partnerships—with energy owners and operators, manufacturers, & trade associations; with other Federal agencies; across SLTT governments; with academia and the National Labs; and with the energy information sharing and analysis centers (ISACs)—help to advance collective preparedness and resilience to the growing landscape of threats, technology developments, and energy system trends.

Highlights of the FY 2024 Budget Request

The FY 2024 Budget Request supports a continued expansion of energy sector security and resilience activities in coordination with government and industry partners. By seeding public-private partnerships and cultivating trusted relationships, this program will advance the Department's efforts to support SLTT and industry in preparing for, mitigating, and recovering from all threats and hazards facing the U.S. energy sector through information sharing, risk assessments, capacity building in planning and resilience, and targeted training and exercises.

Planning, Preparedness, and Resilience ($30 million)

- **Manage Energy Sector Risk and Enable Sector Risk Management ($10 million):** PPRA will continue to lead the Department's activities on sector-wide energy security policy and represent DOE at the National Security Council and across the interagency for cross-sector energy security policy and risk management. This includes leading interagency risk management activities for the energy critical infrastructure including policy development. Through the Risk Management program, PPRA will:

[a] Legacy Information Sharing, Partnerships and Exercises (ISPE) became Preparedness, Policy, and Risk Analysis in FY 2024

[b] The Department of Homeland Security (DHS), in coordination with relevant SRMAs, annually identifies and maintains a list of critical infrastructure entities that meet the criteria specified in Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, Section 9(a) ("Section 9 entities") utilizing a risk-based approach. Section 9 entities are defined as "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."

- Build on existing mechanisms for risk identification and mitigation development and extend new capabilities to identify systemically important energy sector entities, perform intelligence-informed risk analysis, and coordinate with other DOE offices, the National Labs, Federal agencies, and relevant critical infrastructure sectors. As the SRMA lead, CESER will further develop its capacity to support the energy sector's (e.g., owners and operators, trade organizations, subsector coordinating councils, SLTT, Section 9) need for a cohesive and coordinated set of resources, enable sector entity risk mitigation actions through knowledge exchange, and provide for more collaborative engagement opportunities to inform risk analysis.
- Complete a risk analysis strategy and the release of CESER Investments in Risk Mitigation Publication to ensure the stakeholder community maximizes its ability to leverage the capability developed by CESER. As the diversity of resources interconnected to the energy system grows CESER will prepare and provide action-oriented, intelligence-informed threat briefings to support energy system investment and decision-making.
- Establish new coordination and relationship-building opportunities to identify and eliminate barriers to energy security information sharing across governments and industry, including for renewable and distributed energy resources (DERs). This includes developing immediate risk and resilience analyses and actions to mitigate and, in some cases even avoid, the impacts of energy supply disruptions. These products will address key knowledge gaps to improve stakeholder capacity to develop and implement policies, regulations, and training programs that support incorporating critical energy security, cybersecurity, and resilience into infrastructure systems.

- **Support Post-Disaster Recovery and Resilience ($2 million):** When a major disaster strikes, the restoration of energy systems depends on the planning and coordinated effectiveness of local, Tribal, territorial, regional, and national responses. In FY 2024, the program will expand the capability for risk analysis, energy security and resilience planning technical assistance engagements across federal, State and local response entities to improve preparedness to all-hazards including hurricanes, wildfires, fuel emergencies, cybersecurity events, and impacts from the growing threat of climate change. CESER will enhance, aggregate, and deliver dynamic data and analysis products to SLTT energy and emergency officials. These products build on lessons learned from exercises and real-world energy disruptions to improve the inclusion of security and resilience into policy and investment decisions. In addition, CESER will support communities during the recovery phase following major disasters by facilitating access to technical resources that will help them to build resilience, protect critical energy infrastructure, and reduce or avoid future incident impacts.

- **Enhance State, Local, Tribal, and Territorial Energy Security, Resilience and Emergency Preparedness Capacity ($16 million)**: Keeping the lights on and fuel flowing is a priority for governors, legislators, State energy offices, regulators, emergency management agencies, and Tribal and local governments. Energy security planning can ensure a State has a reliable, secure, and resilient energy supply. As climate change and manmade threats continue to pose greater risks to energy infrastructure, States must adapt their plans and policies, prepare for emergencies, pursue resilient and pre-hazard mitigation energy projects, and make risk-informed investment decisions. PPRA will assist SLTT entities to enhance their capacity to manage risks, mitigate threats, and prepare and respond to emergencies. In FY 2024, increased funding will support additional deployment of CESER resources across the United States to SLTT partners to provide them with actionable advice, plan templates, as well as opportunities to collaborate with local, regional, Tribal, and intrastate partners more effectively. PPRA will provide planning and preparedness support to SLTT entities through the following efforts:

    - In response to State requests for CESER to support more State and regional-led initiatives, PPRA will provide technical support, policy strategy, and risk mitigation strategies to CESER's Regional liaisons who reside locally, understand region specific hazards, interdependencies and can provide dedicated technical assistance. This direct engagement will include support for implementation of State energy security plans, hazard mitigation planning with State and FEMA officials, participation in State energy emergency exercises, facilitation of regional coordination efforts and other technical assistance efforts aimed at improving SLTT preparedness and resilience.

    - To fulfill repeated requests from local and Tribal governments for specific local resources, PPRA will develop customizable energy security and fuel planning resources. PPRA anticipates that over 200 local and Tribal governments will develop plans utilizing these tailored resources.

- State Emergency Support Function (ESF) 12 responders have been activated more often in in recent years to respond to energy emergencies. To best prepare this group to respond, PPRA will expand its successful but limited virtual State ESF-12 training to include regional workshops that will provide in-depth training and multi-state coordination.

- Designing systems with security embedded will be essential for the clean energy transition and to protect distributed energy resources (DERs) and electric vehicle supply equipment, included those deployed through funding from IIJA and IRA. PPRA will prepare States to build-in security from the start with guidance, procurement language examples and facilitated collaboration across State agencies to enable coordination and process changes that are required to accomplish the secure clean energy transition. PPRA anticipates 30 States and territories will adopt security guidelines based on PPRA assistance and uptake of previous offerings.

- PPRA will develop an All-Hazard Vulnerability and Threat Scoring Framework to help SLTT and industry partners quickly identify critical risks to energy infrastructure in the face of an unfolding threat and identify quickly implementable mitigation measures. This Framework will be developed alongside SLTT, industry, and federal partners, with the goal of ensuring that it can produce common baseline understandings of threat, vulnerability, and risk that serve the needs of the energy sector – informing planning/preparedness efforts and expenditures (including State Energy Security Plans, and long-term infrastructure planning), and supporting coordinated incident response. The Framework will begin implementation through case-by-case pilot assessments conducted by DOE and partners, with the aim of scaling to a publicly-released tool that can be used by all energy stakeholders.

- PPRA will incorporate Energy Justice (EJ) as a key component in resources developed. Specifically, model energy security programs which include input from and benefit to energy justice communities. Activities will include Energy Security Roundtable discussions (with Tribes, EJ communities, others), guidance for engagement, and model programs. PPRA anticipates producing 5-10 model programs suited for broad adoption across the 56 States and territories.

- **Defense Critical Energy Infrastructure (DCEI) ($2 million)**: The DCEI program's objective is to strengthen energy infrastructure systems for national security purposes. The DCEI program will identify, evaluate, prioritize, and assist in developing executable strategies to strengthen the energy infrastructure systems that supply critical infrastructure needed to ensure continuity of defense activities following severe natural and manmade disasters. Specifically, these investments will enable an increased confidence that necessary energy resources will be available to designated Critical Defense Facilities. CESER will continue to implement DOE's DCEI strategic plan by applying previously validated successful methods to additional critical defense facilities, increasing national defense and security readiness against power supply interruptions.

<u>Exercises, Cybersecurity Training, and Cyber Workforce Development ($9 million)</u>

In support of CESER's mission to be prepared for, respond to, and recover from, threats and hazards causing energy disruptions, this program is designed to elevate the collective sector preparedness through platforms such as relevant cybersecurity training, exercises, and cybersecurity workforce development programs.

- **Non-cyber Exercises and Training ($2 million):** Exercises are an important component of preparedness, by providing the energy sector with the opportunity to shape planning, assess and validate capabilities, and address areas for improvement. CESER supports exercises that prepare participants for all-hazards that could affect energy delivery alongside partners from federal, SLTT, oil, natural gas, and electricity subsectors, and other interdependent critical infrastructure sector organizations. In addition to cybersecurity-focused exercises, CESER will tailor upcoming exercise objectives to include the following themes: energy sector security, climate adaptation and resilience, physical security, and logistics and supply chain integrity. Clear Path is CESER's annual cornerstone all-hazards energy security and resilience exercise series. The Clear Path series is the principal forum for enhancing the energy sector's ability to coordinate and support each other in response to catastrophic incidents including terrorism, wildfires, earthquakes and impactful weather events. The series examines the energy sector's response and restoration roles, responsibilities, and plans and procedures following a major incident, stressing interdependencies between multiple critical infrastructure sectors. Each year, Clear Path presents response officials with a diverse array of challenging exercise scenarios, allowing them to build upon and validate improvements and mitigation tactics implemented and derived from lessons learned from previous exercises and real-world incidents. A key component of exercise effectiveness is CESER's continuous improvement planning cycle which includes thorough after-action review of identified areas to sustain and/or improve. These areas and the associated corrective actions are integrated into emergency response plans and procedures as well as into future exercises for training and validation. Through final after-action reports, exercise results are shared with participants, providing clear guidance on how plans, policies, and procedures can be augmented to reduce risk and increase overall preparedness.

- **Cybersecurity Exercises, Training and Workforce Development ($7 million):** The energy sector is experiencing a significant increase in vacant cybersecurity jobs. In the attempt to mitigate the workforce gap, CESER is developing a cybersecurity workforce framework that will identify options to support the expansion of the qualified talent pipeline, broadening opportunities for non-traditional and underrepresented groups, hosting cybersecurity defense competitions, and emphasizing the concepts of apprenticeships and upskilling. In the near term, CESER's CyberForce Competition, a collegiate cybersecurity defense competition in which students defend a simulated cybersecurity -physical infrastructure against professional red-team attackers, is bringing together energy sector industry and government partners with hiring priorities and the Nation's future cybersecurity defenders. The CyberForce Program extends and encourages students from Minority Serving Institutions and from underrepresented communities to participate. To further reduce the consequences of cybersecurity -enabled sabotage, CESER has prioritized the development and delivery of cybersecurity training to the energy sector, federal, and SLTT partners through hands-on training efforts such as its CyberStrike Training program and the Operational Technology (OT) Defender Fellowship. Through hands-on training, the CyberStrike platform enhances the ability of energy sector owners and operators to prepare for a cybersecurity incident impacting operational technology. FY 2024 improvements will enhance the curriculum to expand threats by demonstrating real-world attacks attributed to nation-states and those on DERs and renewable infrastructure, such as solar and wind inverters. The OT Defender Fellowship program offers senior-level OT security and operations managers an opportunity to understand high-level strategies and tactics adversarial state and nonstate actors employ in targeting U.S. energy infrastructure. The program serves as a bi-directional information and idea exchange forum between government and energy sector experts, contributes to the collective advancement of improved cybersecurity and information sharing capabilities and processes. To validate cybersecurity training, the need for hands-on capabilities to test and evaluate cybersecurity processes, plans, procedures, incident response capabilities, and technologies is best demonstrated through preparedness exercises which incorporate testbed environments. The use of testbeds that closely mirror real-world electrical grid substations, provide direct transferable findings from experimental environments to real-world operations. The Liberty Eclipse Exercise, DOE's annual cybersecurity-focused series, leverages this testbed environment, affording industry an extremely unique and customizable opportunity. Following success of 2022's effort, DOE intends to develop opportunities to expand industry partnership, and develop a training model that is available to reach utility partners with less resources and mature plans and procedures. Through these unique DOE efforts, CESER will continue to explore emerging threats and apply educational training models to rapidly and broadly disseminate awareness of, and defensive measures against, future cybersecurity threats.

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

	FY 2022 Enacted	FY 2023 Enacted	FY 2024 Request	FY 2024 Request vs FY 2023 Enacted ($)	FY 2024 Request vs FY 2023 Enacted (%)
Preparedness, Policy and Risk Analysis[a]					
Planning, Preparedness, and Resilience	12,000	17,857	30,000	+12,143	+68.0%
Training and Exercises	7,000	9,000	9,000	0	0.0%
Total, Information Sharing, Partnerships and Exercises	**19,000**	**26,857**	**39,000**	**+12,143**	**+45.2%**

Preparedness, Policy, and Risk Analysis (PPRA)
Explanation of Changes ($K)

	FY 2024 Request vs FY 2023 Enacted
• Planning, Preparedness, and Resilience - Identify systemically important entities and perform intelligence-informed risk analysis, incorporate diversity, inclusion and energy justice in methods, approaches and tools available to the energy sector, enhance State Energy Security Plans previously submitted and incorporate renewable and DER in plans, improve mitigation and emergency preparedness through training workshops and tabletop exercises, and expand State cybersecurity incident response planning.	+12,143
• Exercises, Cybersecurity Training and Cyber Workforce Development - Conduct internal and external exercises with the federal interagency, SLTT governments, and industry on both cybersecurity and natural hazards, provide cybersecurity training for operational technology and industrial control systems, enhance the CyberForce Competition, and establish a Cyber Workforce Development effort within CESER.	+0
Total, Preparedness, Policy, and Risk Analysis (PPRA)	**+12,143**

[a] Legacy Information Sharing, Partnerships and Exercises (ISPE) became Preparedness, Policy, and Risk Analysis in FY 2024

Preparedness, Policy, and Risk Analysis

Activities and Explanation of Changes ($)

FY 2023 Enacted	FY 2024 Request	Explanation of Changes FY 2024 Request vs FY 2023 Enacted
Preparedness, Policy, and Risk Analysis (PPRA) $26,857,000	**$39,000,000**	**+$12,143,000**
Planning, Preparedness, and Resilience $17,857,000	*$30,000,000*	*+$12,143,000*
• Identify systemically important entities and perform intelligence-informed risk analysis, prepare and provide action-oriented, intelligence-informed threat briefings and eliminate barriers to government-industry information sharing and operational coordination, inform State and industry, including DCEI, investment decisions and improve mitigation and emergency through dynamic risk analyses, and provide technical assistance in support of State energy security planning. • Scale DOE's DCEI risk efforts by applying successful methods incubated and validated in FY 2022 to more critical defense facilities from DOE's designated list, increasing national defense and security readiness against power supply interruptions. Expand, aggregate, and deliver intelligence-informed and actionable data and analysis to SLTT energy and emergency officials and industry via dynamic risk analyses. • Incorporate diversity, inclusion and energy justice in methods, approaches and tools that will enable SLTT governments to enhance and exercise energy security plans and regulatory models, incorporating	• Define and manage an understanding of systemic risks in the energy sector in partnership with labs and SCCs and Section 9 companies in particular. Manage a risk register to define and document critical infrastructure risks. • Develop capabilities to identify critical energy companies (electricity, oil, and natural gas) in the U.S. in support of SRMA mission. • Manage the Department's Critical Energy Infrastructure Information program. • Lead SRMA engagement activities, facilitating information sharing, policy development, and risk management activities with the critical infrastructure stakeholders and interagency. • Develop analytic capabilities that can dynamically identify and prioritize energy infrastructure in support of Defense Critical Energy Infrastructure. • Identify and /or Assess resilience options that could be implemented to accomplish DOE and Administration strategic goals on securing energy delivery systems from all hazards. Development of ARES reports	• Enhance State Energy Security Plans submitted in FY 2023 to ensure secure, reliable, and resilient energy infrastructure in a changing threat and operational environment. Develop guidance and provide technical assistance for local and Tribal governments for energy security and fuel plans. Incorporate renewable and distributed energy resources into State plans and technical assistance efforts. • Use updated tools to conduct local, State, and regional risk assessments to identify critical energy infrastructure and asset vulnerabilities and assist States with identifying and implementing mitigation measures that will reduce risks. • Launch regional Emergency Support Function 12 (ESF-12) training workshops and tabletop exercises for States to enhance emergency preparedness and regional collaboration. • Work with at least 10 States to expand their cybersecurity incident response plan to include response to a cyberattack that could result in physical consequences to energy delivery.

FY 2023 Enacted	FY 2024 Request	Explanation of Changes FY 2024 Request vs FY 2023 Enacted
cybersecurity, hardening, and other resilience measures and incentives.	and other risk analysis products and communication tools. • Assist SLTT entities to enhance their capacity to manage risks, mitigate threats, and prepare and respond to emergencies. • Facilitate access to technical resources that will help build resilience, protect critical energy infrastructure, and reduce or avoid future incident impacts.	
Exercises, Cybersecurity Training and Cyber Workforce Development $9,000,000	*$9,000,000*	*+$0*
• Training and Exercises: Conduct internal and external exercises with the interagency, SLTT governments, and industry on cybersecurity and natural hazards, provide cybersecurity training for operational technology and industrial control systems, and expand the scope of the CyberForce Competition.	• Conduct internal and external exercises with the federal interagency, SLTT governments, and industry on both cybersecurity and natural hazards. • Expand cybersecurity exercises and training by enhancing and leveraging existing testbed environments which can provide realistic simulation capabilities, allowing for advanced training and efficiencies. • Scale cybersecurity training for operational technology and industrial control systems by increasing CyberStrike deliveries and enhance the renewable variation. • Enhance the CyberForce Competition to include multiple competitive events throughout the year leading to a multi-day capstone competition event, while also emphasizing the internship and job fair opportunity.	• Continue internal and external exercises with the interagency, SLTT governments, and industry on cybersecurity and natural hazards, provide cybersecurity training for operational technology and industrial control systems, and expand the scope of the CyberForce Competition. • Establish a Cyber Workforce Development framework

FY 2023 Enacted	FY 2024 Request	Explanation of Changes FY 2024 Request vs FY 2023 Enacted
	• Establish a Cyber Workforce Development framework with the intent to decrease the workforce gap in energy cybersecurity jobs.	

Risk Management Tools and Technologies (RMT)

Overview

The dynamic threat landscape, climate crisis, advances in energy system technologies, increasing supply chain cybersecurity risks, and the use of legacy devices in an aging infrastructure are all continuous challenges to the resilience of the energy sector. Further, while we advance the energy sector by integrating new sources of generation (e.g., solar, wind), new architectures (e.g., virtual power plants, cloud resources, artificial intelligence), and new systems (e.g., grid management systems, automated management systems), we have to ensure these systems and technologies are designed and built with resilience to the growing climate, cybersecurity, and physical risks. The Office of Cybersecurity, Energy Security, and Emergency Response's (CESER) Risk Management Tools and Technologies (RMT) division does just that.

The RMT division focuses on research, development, and demonstration (RD&D) of tools, technologies, and techniques that address cybersecurity, physical, electromagnetic pulse, geomagnetic, and climate-based risks facing the energy sector. RMT spearheads innovation through partnerships that include asset owners and operators, academia, manufacturers, DOE National Laboratories, and other Federal agencies. This approach has led RMT to demonstrate and deploy a number of innovative approaches and technologies to strengthen the security and resiliency of electricity, oil, and natural gas hardware and software. The division's RD&D efforts develop tools that monitor, detect, and protect critical energy infrastructure and networks from threats; and enable automated assessments, situational awareness, and response to threats to the sector. RMT leverages state of the art national lab infrastructure and capabilities to test systems; identify vulnerabilities; and develop mitigations. The division also works closely with sector partners to transition developed technologies to practice through commercialization, and to enable sector adoption of recommended processes and practices through frameworks and guidance.

In addition to working closely with industry, RMT is leading the integration of 'cybersecurity by design' in DOE's RD&D efforts across the Department's science and applied energy offices. This approach means offices performing RD&D of energy delivery system will integrate cybersecurity requirements in their activities resulting in energy delivery systems of the future being inherently more secure. CESER facilitates this integration, as well as coordination of Research and Development (R&D) for securing legacy and emerging energy delivery systems where there are unmet needs (e.g., addressing cybersecurity needs stemming from the proliferation of EV infrastructure and other distributed energy resources). Improved coordination and integration of cybersecurity R&D will also enable CESER to prioritize RD&D of tools and technologies which apply across multiple energy systems (e.g., renewables, fossil, nuclear domains) and focus on activities such as encryption, forensics, and monitoring.

Highlights of the FY 2024 Budget Request

Working closely with energy sector, academia, and National Laboratories, the FY 2024 Budget Request for RMT supports a more economically competitive, environmentally responsible, secure, and resilient U.S. energy infrastructure focusing on following activities:

- **ADVANCE TOOLS TO MANAGE CYBER RISKS ($45 million)**

  - **<u>RD&D of Cybersecurity Tools and Technologies ($30 million)</u>**
    Research, develop, demonstrate and transition to practice next generation cybersecurity tools and technologies that provide energy companies protection, monitoring, detection, response, containment, forensics, and recovery capabilities. These tools will leverage operational data and the physics of energy delivery to inform owners and operators of anomalous cybersecurity activities on their industrial controls systems and networks. These efforts will primarily be executed through competitive funding opportunities and research calls for energy companies, academia, National Laboratories, and/or manufacturers. This work focus on tools that enable individual utilities to manage cybersecurity risks to next generation energy systems, such as microgrids, automated OT infrastructure, virtual power plants, and cloud-connected systems, positioning the industry to stay ahead of the threat.

- **RD&D of Cybersecurity Situational Awareness & Information Sharing ($10 million)**
  In addition to developing tools to address cybersecurity risks at individual organizational level, RMT is also focused on research, development, and demonstration of technologies that enable sector-wide information sharing, and USG situational awareness of cybersecurity threats through analysis and correlation with intelligence community information. This work will result in improving cybersecurity situational awareness and analysis capabilities not present today. CESER will work with National Laboratories on novel tools for collaborative defense, correlating various data sets to detect anomalous activity, and enabling real-time dissemination of threat intelligence to both DOE and owners and operators. RMT will evaluate and, where applicable, propose potential uses of these technologies by entities such as States and industry associations.

- **Energy Cybersecurity Center of Excellence ($5 million)**
  The **DOE Energy Cybersecurity Center of Excellence (CCoE)** will provide energy cybersecurity expertise and capabilities to the other DOE offices ensuring cybersecurity is integrated by design in the energy delivery systems of tomorrow and other energy projects funded by DOE. The CCoE, led by CESER, will provide DOE offices shared cybersecurity resources and services drawing from CESER programs and National Laboratory expertise. As the office responsible for energy sector cybersecurity, the establishment of the CCoE is a critical component in hardening the systems (hardware, software, virtual, etc.) that are built and deployed for use in the energy sector. CESER will also function through CCoE as the critical connection point between experts at relevant National Labs with program offices deploying funding, projects, or programs that need cybersecurity support. Using an applied approach to cybersecurity and RD&D done within CESER, the CCoE will provide cybersecurity expertise to all DOE RD&D where applicable and to integrate practices across policies, programs, and funding opportunities.

- **UNIVERSITY-BASED RD&D AND ENERGY CYBERSECURITY R&D CENTERS ($5 million)**
  RMT will expand the network of university cybersecurity R&D centers across the Nation. These university cybersecurity RD&D Centers will enable collaboration among regional utilities, National Laboratories, and regulatory bodies to perform RD&D that combines multi-disciplinary expertise including but not limited to power system engineering and the computer science of cybersecurity. This includes innovate and transition capabilities that reduce the risk of power disruption resulting from a cybersecurity incident for energy delivery systems. Academic RD&D involves unbiased, technology focused activities that, when combined with industry priorities and guidance, results in real-world, impactful solutions. Additionally, the Centers will enable integration of DOE initiatives and resources such as Cybersecurity Capability Maturity Model (C2M2) and CyOTE into university energy cybersecurity programs. This will not only provide discovery and innovation but will also contribute to energy cybersecurity learning and teaching across different communities in the country.

- **ADVANCE TOOLS TO MANAGE RISKS FROM NATURAL HAZARDS AND NON-CYBER THREATS ($20 million)**

  - **RD&D of Risk Management Tools and Technologies for Natural Hazards ($10 million)**
    RMT will address non-cybersecurity risks and hazards to the energy sector, such as those due to climate change, extreme weather, and seismic events. RMT will leverage emerging technologies to develop tools that help identify, characterize, detect and mitigate risks to energy infrastructure, such as hurricanes, flooding, droughts, and earthquakes. These tools will enable long term planning allowing the industry to more effectively prepare for and respond to these incidents.

  - **RD&D of Tools and Technologies for energy infrastructure resilience to wildfires ($4 million)**
    RMT will partner with industry, private sector RD&D partners, the National Laboratories, and other DOE offices to research, develop, and demonstrate technology solutions that enable the prevention, detection, and dynamic mitigation of 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 advance sensors, grid data analytics, satellite imagery, drones, and application of artificial intelligence.

- **<u>RD&D of Tools and Technologies for addressing physical threats to energy systems</u> ($1 million)**
  RMT will work with industry and interagency partners to develop and tailor tools and technologies that address physical and other man-made non-cybersecurity threats to electricity, oil, and gas infrastructure such as Metcalf Substation-style physical attacks, unmanned aerial systems (UAS), and positioning, navigation, and timing risks. Using prizes, RMT will work closely with other DOE offices, private sector research organizations, and the National Laboratories to incentivize advancements in physical security technology development, demonstration, and adoption for hardening risk prioritized infrastructure such as transmission substations and oil and natural gas pipelines.

- **<u>Electromagnetic Pulse and Geomagnetic Disturbances</u> ($5 million)**
  DOE will continue to engage in efforts to address the risks associated with electromagnetic pulse (EMP) and geomagnetic disturbances (GMD). These will include activities such as performing vulnerability assessments of critical assets; identifying mitigation options and estimated costs; and partnering with industry (through cost shares) to field deploy innovative cost-effective mitigation options based on results of vulnerability assessments.

- **SUPPLY CHAIN CYBERSECURITY RISK MANAGEMENT ($45 million)**

  - **<u>Energy Cyber Sense and Cyber Testing for Resilient Industrial Control Systems (CyTRICS)</u> ($35 million)**
    The Energy Cyber Sense program is CESER's overarching supply chain cybersecurity risk management effort. The program comprises a range of activities including the CyTRICS testing. In Q1 FY 2023, CESER completed the Energy Cyber Sense Implementation Plan and 5-Year Operating Plan. The program comprises four pillars of excellence: Understand criticality, test and establish digital supply chain transparency, aid in application of standards, norms, and best practices, and improve technology and system designs (both legacy and new). This vision of the program will enable CESER to execute more effectively on Congressional direction and assist the Energy Sector Industrial Base (ESIB) in enhancing the resilience of critical infrastructure.

    As the testing component of the broader Energy Cyber Sense program CyTRICS is focused exclusively on testing and will dovetail with Cyber Sense capabilities of identification and prioritization of critical equipment, provenance, mitigation solutions, and vulnerability disclosures. CyTRICS partners across energy sector manufacturers and asset owners to apply classified threat intelligence, identify high priority operational technology (OT) components, perform expert testing, share information about vulnerabilities in the digital supply chain, and inform improvements in component design and manufacturing. CESER leverages best-in-class test facilities and analytic capabilities at six DOE National Laboratories (INL, PNNL, SNL, NREL, ORNL, and LLNL) and strategic partnerships with technology developers, manufacturers, asset owners and operators, and interagency partners.

    FY 2024 funding will enable CESER RMT to expand the reach of the CyTRICS testing activities; with a focus on risk-based prioritized systems and components. RMT will develop partnerships with the operational technology manufacturers and integrate the testing pipeline with the broader Energy Cyber Sense program. RMT will work with interagency partners and industry on a pilot effort to research, design and develop cybersecurity label for an industrial IoT technology in the energy sector. The labeling pilot will not include enforcement or certification but will include work on promotion through standards and guidance. The CyTRICS program will also work to analyze no less than 15% of critical components in energy sector systems; and expand manufacturers participating in the program to cover no less than 30% of the market share of critical components. CyTRICS is rapidly expanding its testing capacity across six DOE National Labs and growing our vendor partnerships. This expansion will allow CyTRICS to not only test more components, but also test a greater diversity of critical systems in the energy sector. RMT will work with interagency partners and industry on a pilot effort to research, design and develop cybersecurity label for an industrial IoT technology in the energy sector. The labeling pilot will not include enforcement or certification but will include work on promotion through standards and guidance.

- **Cybersecurity of Distributed Energy Resources** **($5 million)**
  CESER will work with the National Labs to conduct cybersecurity research and related supply chain risk management of distributed energy resources (DERs). As DERs become pervasive energy sector stakeholders must increase investment in the cybersecurity of those components (e.g., solar, storage, controllable loads, etc. based on risk and technology landscape). In some communities across the U.S., DERs will begin to supply 100% of generation by 2030; consequently, it is a priority to research and address cybersecurity risks and the impacts to broader resilience to the grid. This work will be closely coordinated with technology specific research being performed in the Office of Energy Efficiency and Renewable Energy and storage research performed in the Office of Electricity. In FY 2024, this work will include demonstration pilots of cybersecurity measures being pursued in close collaboration with the Office of Energy Efficiency and Renewable Energy; research to strengthen the cybersecurity of communication protocols in the DER space; and development of tools and capabilities that ensure risks from DERs in the cloud environments are mitigated. Activities that may continue include the Clean Energy Cyber Accelerator (pilot) and Renewable Energy and Storage Cybersecurity Research (RESCue) project, which is research focused on the cybersecurity of hybrid power plants that are inclusive of wind, solar, and energy storage.

- **Cybersecurity of Electric Vehicle Charging Infrastructure** **($5 million)**
  RMT is focused on ensuring cybersecurity is an integral part of the Nation’s clean energy transition, to include the shift to EVs. RMT will deliver solutions that mitigate cybersecurity risks and advance EV charging infrastructure resilience and performance. CESER’s EV cybersecurity portfolio of work is done in close collaboration with the Joint Office of Energy and Transportation and the Vehicles Technologies Office. RMT will work with public and private partners to support development and promotion of cybersecurity standards across the EV and EVSE ecosystem and identify opportunities for harmonization; work towards the cybersecurity attributes needed for the emerging EV and EVSE ecosystem; and conduct targeted cybersecurity R&D for the EV and EVSE ecosystem.

- **CYBER RISK ASSESSMENTS, FRAMEWORKS, AND R&D COORDINATION ($20 million)**

  - **Cyber-Informed Engineering (CIE)** **($4 million)**
    The National CIE Strategy includes foundational principles to help lead the Nation's effort to integrate cybersecurity and engineering practices. RMT works with stakeholders to implement the CIE strategy in the energy sector. In FY 2024, RMT will aid energy research programs to embed CIE security by design principles into the research and development process to ensure that cyber defenses are embedded into foundational future technology design. RMT will also create the tools and technologies to enable better application of CIE principles, and to validate the effectiveness of infrastructure upgrades and mitigations. Additionally, RMT will Identify and analyze design patterns for energy sectors leading to enhanced engineering protections and drive multi-stakeholder awareness and acceptance for these design methodologies.

    In FY 2024, RMT will expand implementation of CIE into the core engineering curriculum at major U.S. research universities and work with asset owners and operators to enable CIE principles within their engineering design and infrastructure improvement efforts.

    Consequence-Driven Cyber-Informed Engineering (CCE) **($4 million)**
    RMT will continue implementing CCE to enable Critical Function Assurance (CFA) of high risk infrastructure that is strategically critical for energy sector and national security, such as infrastructure that if compromised, could disrupt critical fuel/electricity supplies. The CCE assessments evaluate an organizations’ key functions for improvements across people, processes, and technologies such that the consequences of any compromise is

significantly reduced. The CCE program will be completing the research and development phase with the goal to potentially transfer the steady operational services to commercial partners and another division of CESER.

Development of Cyber Frameworks and Reference Architectures ($4 million)
RMT will continue to leverage methodologies like the Cybersecurity for Operational Technology Environment (CyOTE) to further early detection of anomalous behavior and threats in OT environments. FY 2024 funding will enable RMT to further the underlying CyOTE research and innovation; transition the CyOTE tool to practice with new features and functionality; and refine training for OT and non-OT stakeholders. Specifically, advancing from methodology research the program will focus on smart data mining, reporting insights to industry, and expanding understanding of additional technical domains that matters to industry. New R&D tasking will include stress testing reference architectures of various OT environments for primary stakeholders.

- **Quantification of Cyber Risk and Cyber Risk Profiles for Critical Systems and Technologies ($3 million)**
  RMT will develop capabilities and tools that can be used by energy industry enterprise risk managers to use cybersecurity assessments with quantitative and qualitative risk data. The tool will enable risk-informed cybersecurity investment decisions allowing for optimal utilization of limited resources. RMT will continue to development 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.

- **Grid Modernization Laboratory Consortium (GMLC) and Lead Cyber RD&D Coordination Across DOE Offices ($5 million)**
  The Grid Modernization Initiative (GMI) is a DOE cross-departmental effort to coordinate the development of technology, modeling analysis, cybersecurity, and physical security strategies to facilitate grid modernization. The initiative provides mechanism to enable grid modernization RD&D through joint funding opportunities by multiple offices. CESER will be a voting member of GMLC committing to drive cybersecurity across DOE GMLC efforts. As a voting member CESER has committed to at least $3 million annually for GMLC Lab calls. In FY 2024 RMT plans to participate in a 3-year lab call.

  As directed by Congress in FY 2023, CESER will ensure cybersecurity research, development, and demonstration projects being performed across the Department are coordinated. CESER will establish a formal coordination structure to cybersecurity RD&D efforts across the department to ensure the Department is taking a strategic and coordinated approach going forward. CESER will work with relevant DOE program offices and develop a Multi-Year Cybersecurity RD&D Roadmap for Energy Sector Cybersecurity to guide DOE's overall efforts. CESER will lead regular coordination calls with relevant offices to ensure we are coordinated. Also, in CESER's role as the Sector Risk Management Agency (SRMA) for the energy sector, CESER will coordinate with CISA, industry, academia, and other external partners to ensure the cybersecurity RD&D continues to address the energy sector of the future.

Risk Management Tools & Technologies
Funding ($K)

	FY 2022 Enacted	FY 2023 Enacted	FY 2024 Request	FY 2024 Request vs FY 2023 Enacted ($)	FY 2024 Request vs FY 2023 Enacted (%)
Risk Management Tools & Technologies					
Advance Tools to Manage Cyber Risks	36,804	40,000	45,000	+5,000	+12.5%
University-Based RD&D and Energy Cybersecurity R&D Centers	9,000	2,000	5,000	+3,000	+150.0%
Advance Tools to Manage Risks from Natural Hazards & Non-Cyber Threats	37,000	30,000	20,000	-10,000	-33.3%
Supply Chain Cybersecurity Risk Management	25,000	30,000	45,000	+15,000	+50.0%
Cyber Risk Assessments, Frameworks, and R&D Coordination	22,000	23,000	20,000	-3,000	-13.0%
Congressionally Directed	3,000	0	0	0	0.0%
Total, Risk Management Tools & Technologies	**132,804**	**125,000**	**135,000**	**+10,000**	**+8.0%**

Risk Management Tools and Technology
Explanation of Major Changes ($K)

	FY 2024 Request vs FY 2023 Enacted
• Advanced Tools to Manage Cyber Risk: increase to establish the Cybersecurity Center of Excellence and deployment of tools & technology to the energy sector.	+5,000
• University Based RD&D and Energy Cybersecurity R&D Centers: Increase will provide one R&D center and one university-based project.	+3,000
• Advanced Tools to Manage Risks from Natural hazards & Non-Cyber Threats: The EAGLE-I and situational awareness tools work has moved from RMT to R&R.	-10,000
• Supply Chain Cybersecurity Risk Management: supply chain testing (CyTRICS) program will expand testing scale and capabilities; and launch labeling design initiative.	+15,000
• Cyber Risk Assessments, Frameworks, and R&D Coordination: CCE reduced needs as research and development phase completes, CIE development of the strategy completes and moves to implementation phase, and C2M2/Quantification effort completes development of the C2M2 product suite.	-3,000
Total, Risk Management Tools and Technology	**+10,000**

Risk Management Tools and Technologies

Activities and Explanation of Changes ($)

FY 2023 Enacted	FY 2024 Request	Explanation of Changes FY 2024 Request vs FY 2023 Enacted
Risk Management Tools and Technologies $125,000,000	**$135,000,000**	**+$10,000,000**
Advance Tools to Manage Cyber Risks $40,000,000	*$45,000,000*	*+$5,000,000*
• Work with National Labs, industry, and academia to research, develop, demonstrate, deploy and transition to practice next generation cybersecurity risk management technology and tools for broad adoption in energy industry.	• Work with National Labs, industry, and academia to research, develop, demonstrate, and transition to practice next generation cybersecurity risk management tools and technologies for adoption in energy industry.	• Establish DOE Energy Cybersecurity Center of Excellence to provide energy cybersecurity expertise and capabilities to the other DOE offices ensuring cybersecurity is integrated by design in the energy delivery systems of tomorrow. • Support deployment of cybersecurity tools & technologies that will provide sector-wide collaboration, information sharing, and situational awareness.
University-Based RD&D and Energy Cybersecurity R&D Centers $2,000,000	*$5,000,000*	*+$3,000,000*
• Collaboration with academia not only bolsters the overall security and resilience of the energy industry through technological innovations but also helps develop a cybersecurity workforce that is well versed in both engineering and cybersecurity disciplines.	• Collaboration with academia not only bolsters the overall security and resilience of the energy industry through technological innovations but also helps develop a cybersecurity workforce that is well versed in both engineering and cybersecurity disciplines.	• Increase will fund one additional R&D center and one additional university-based project.
Advance Tools to Manage Risks from Natural Hazards & Non-Cyber Threats $30,000,000	*$20,000,000*	*-$10,000,000*
• This work included outlays to develop and maintain the EAGLE-I and other situational awareness platform and tools. The funding in the past was for developing and updating capabilities for situational awareness and enhanced collaboration between deployed responders, personnel at DOE Headquarters, as well as industry, State, and interagency partners.	• Research and develop tools and technologies that address risks to energy systems from natural hazards, climate change and extreme weather. • Advance HEMP/GMD modeling tools, mitigation technologies and associated testing to support both and vulnerability assessments. • Begin program to increase physical security and support law enforcement forensics at electrical transmission and distribution substations.	• The EAGLE-I and situational awareness tools work has moved from RMT to R&R.

Supply Chain Cybersecurity Risk Management $30,000,000	*$45,000,000*	*+$15,000,000*
• This work is focused on supply chain testing and enumeration of critical energy delivery software and hardware. The work includes demonstration of security practices for emerging technologies such as Distributed Energy Resources in the energy sector.	• This work is focused on supply chain testing and enumeration of critical energy delivery software and hardware. The work includes demonstration of security practices for emerging technologies such as Distributed Energy Resources in the energy sector.	• Supply Chain testing (CyTRICS) program will expand testing scale and capabilities; and launch labeling design initiative.
Cyber Risk Assessments, Frameworks, and R&D Coordination $23,000,000	*$20,000,000*	*-$3,000,000*
• This work is focused on the cybersecurity standards, frameworks, and methodologies. CESER develops guidance and supporting tools and resources for energy sector owners and operators to apply in their environments to strengthen their cybersecurity posture.	• This work is focused on the cybersecurity standards, frameworks, and methodologies. CESER develops guidance and supporting tools and resources for energy sector owners and operators to apply in their environments to strengthen their cybersecurity posture. • Support additional development of CyOTE tool and training.	• CCE program decreased as it completes its research and development phase. • CIE effort decreased as the development of the strategy has been completed and is now in implementation phase. • C2M2 Quantification effort decreased as the program completes its development of the C2M2 product suite.

Response and Restoration

Overview

The U.S. Department of Energy (DOE) is the coordinating agency for Emergency Support Function (ESF) #12, under the National Response Framework, and the Sector Risk Management Agency (SRMA) for the energy sector, pursuant to Presidential Policy Directive (PPD) 21, PPD 41, Executive Order 13636, and the FAST Act. The Office of Cybersecurity, Energy Security, and Emergency Response (CESER) manages these responsibilities within the Department. CESER's Response and Restoration division leads all-hazard efforts related to ESF #12, PPD-21, PPD-41, and other energy sector response-functions, including situational awareness and analysis, for the Department, which supports CESER's preparedness, response, and restoration efforts in the energy sector, across Federal, State, Local, Tribal, and Territorial governments, private industry, trade associations, and non-governmental organizations. The Response and Restoration division also manages the Department's emergency authorities for the energy sector, including authorities delegated to CESER, by the Secretary of Energy, pursuant to the Federal Power Act, Clean Air Act, and the Defense Production Act.

During an incident requiring a coordinated federal response, CESER's Energy Response Organization is activated to manage ESF #12 and SRMA response activities, including deployment of responders and sector engagement. DOE also serves as a primary agency for the Infrastructure Systems Recovery Support Function, under the National Disaster Recovery Framework. ESF #12 provides technical expertise to Federal, State, Local, Tribal, Territories governments, and industry by collecting, evaluating, and sharing information on energy system damage and provides estimations on the effect of energy system outages within affected areas, as well as the potential state, regional, and national impact. It assists government and private sector stakeholders in overcoming inherent challenges associated with restoration of the energy system. To fulfill these responsibilities, CESER trains and coordinates a cadre of volunteer responders from across DOE to deploy virtually or physically to a disaster site upon the request of FEMA. DOE's ESF #12 volunteers perform several critical functions including conducting damage assessments, restoration planning, and technical assistance. CESER may also self-activate for energy emergencies using the Department's own authorities.

In addition, the Response and Restoration division coordinates DOE's response to cyber incidents impacting, or potentially impacting, the energy sector that require a coordinated response with industry and interagency partners, pursuant to PPD-41 and the National Cyber Incident Response Plan. The Department represents the energy sector as the SRMA and supports the Department of Homeland Security's government-wide approach. DOE can support Department of Homeland Security (DHS) cyber response teams, Federal Bureau of Investigation (FBI), and industry with energy sector subject matter expertise. This is support by subject matter experts in CESER, other offices across the Department, and specialized expertise at DOE's National Laboratories.

To ensure CESER can fulfill DOE's responsibilities, the Response and Restoration division maintains and develops capabilities to coordinate response operations, provide technical assistance, enhance situational awareness, and provide analysis of threats and incidents affecting the energy sector, including cyber threats during steady state and response operations.

In FY 2024, CESER will continue to strengthen its emergency response capabilities to support natural hazard, cyber, and physical incidents in the energy sector. The growing extreme weather (e.g., year-around wildfires, intense hurricanes, flooding), physical security incidents and threats, and increasing cyber threats by adversarial Nation-States (e.g., China, Russia, Iran, North Korea) and criminal actors (e.g., ransomware) are drivers for the increased capacity and new approaches to situational awareness, analysis, technical assistance, response, and restoration in support of one of the most complex and expansive critical infrastructure sectors in the United States.

Highlights of the FY 2024 Budget Request

CESER will enhance its robust all-hazards emergency response capabilities with cybersecurity-specific staffing, training, tools, threat analysis, and incident response protocols; build upon its regional response approach to include targeted recruitment, staffing, and operational/collaboration facilities in strategic U.S. regions including Puerto Rico and the USVI. Additionally, CESER internally transferred the EAGLE-I program from the Risk Management and Tools (RMT) division to the Response and Restoration (R&R) division for FY 2024. This will ensure alignment with mission requirements and build out of additional capabilities needed to maintain continuous situational awareness of the Nation's energy system and to support response operations.

- **ALL-HAZARDS INCIDENT RESPONSE, REGIONAL SUPPORT, AND SITUATIONAL AWARENESS ($22 million)**
  CESER must maintain an emergency all-hazards response baseline capability that ensures adequate resources and training are available to facilitate the reestablishment of damaged energy systems and components with potential impact to national and economic security. To fulfill this mission, CESER trains and coordinates a cadre of approximately 120 volunteer responders, from across the DOE enterprise. The cadre is organized into Regional Response Teams, aligned to the 10 FEMA regions, each led by an experienced Regional Coordinator. This concept has enabled CESER to respond to multiple, simultaneous, and back-to-back events. Long term commitment to the regionalization concept as an organizing structure for deployment coordination and annual refresher training will solidify current response capabilities, and provide a foundation for the expansion of skills, tools and products that improve responder effectiveness and add value and energy expertise at the regional, state, and local levels. Rather than fully relying on a volunteer response capability, the FY 2024 increase is focused on building regional capabilities and teams that will work directly with states and regions on emergency response, conduct joint exercises and training with the SLTT and industry as ESF #12 embedded responders, and strengthen DOE's partnerships with the energy sector. CESER's Response and Restoration division will also maintain baseline activities, continue to develop stakeholder relationships, and support day-to-day regional presence to work side-by-side with FEMA, interagency partners, SLTT, and industry stakeholders.

  The Response and Restoration division will also continue to recruit, train, and expand the Catastrophic Incident Response Team cadre to better support FEMA's Incident Management and Assessment Teams (IMAT), and provide specialized technical expertise in damage assessment and energy system restoration; specifically, to support island, earthquake, and other catastrophic response and restoration requiring federal assistance. The program will also build a retired reserve cadre – recruited from recently retired ESF #12 responders – available to support long term, remote, and/or catastrophic incidents that require additional subject matter expertise and support.

  CESER will continue the expansion of Situational Awareness and Analysis Program and conduct a feasibility study to develop the concept of operations for a 24/7 CESER Watch Office at DOE Headquarters. To ensure CESER can fulfill the Department's responsibilities as the SRMA for the energy sector and as the coordinating agency for ESF #12, across all-hazards, CESER needs to maintain continuous situational awareness of threats and incidents impacting, or potentially impacting, U.S. energy systems, as well as capabilities for rapid analysis to help mitigate threats and ensure timely preparedness, response, and recovery efforts. Capabilities include modeling of potential power outages from extreme weather (e.g., hurricanes, wildfires, flooding), modeling restoration times of power outages, modeling cascading impacts of energy sector disruptions on other critical lifelines, increasing visibility of the oil and natural gas sector, modeling fuel disruptions, and remote sensing to quickly identify damaged energy sector infrastructure. When an incident impacts the U.S. energy sector, the Situational Awareness and Analysis Program provides authoritative reporting for interagency and state, local, tribal, and territorial partners, as well as industry stakeholders.

  A CESER Watch Office at headquarters is envisioned to expand on existing Situational Awareness Program to help continuously monitor and anticipate disruption to the energy sector, with the capability to quickly analyze and model potential impacts to the electric power, oil, natural gas, and the growing renewable energy infrastructure to include market impacts to the economy and to determine the effect and disruption on other critical infrastructure, including Defense Critical Energy Infrastructure. The Watch Office will also provide a single point of contact for CESER's situational awareness, analysis, and response activities and enable to Department to meet growing demand for awareness and analysis to all-hazards, in real time. The watch office will also provide 24/7 situational awareness and analysis reach back for deployed ESF #12 responders.

  To fulfill the Departments requirements, CESER utilizes EAGLE-I as the situational awareness platform for the energy sector to provide vital information across the U.S. Government, as well as state, local, tribal, and territorial partners. CESER will continue to develop and maintain the EAGLE-I platform. It will expand near real-time situational awareness of both electricity and oil and natural gas systems, as well as introduce new capabilities to the platform, such as situational awareness of the fuel supply chain and remote sensing and modeling to support energy sector preparedness, response, and recovery effort related to wildfire, flooding, hurricanes, and no-notice incidents (e.g.

earthquakes). Efforts will also focus on ensuring existing capabilities are seamlessly integrated into EAGLE-I and support awareness of interdependent impacts across FEMA Lifelines. Additionally, the EAGLE-I platform is being advanced to enhanced collaboration between deployed responders, personnel at DOE Headquarters, as well as industry, state, and interagency partners.

- **<u>CYBER INCIDENT RESPONSE AND CYBER SITUATIONAL AWARENESS</u> ($17 million)**
  CESER is the lead for the cybersecurity of the energy sector as the SRMA, pursuant to the FAST Act, Executive Order 13636, and Presidential Policy Directive-41 (PPD-41). CESER also supports federal response efforts, when there are significant cyber incidents impacting the energy sector, pursuant to the National Cyber Incident Response Plan (NCIRP), which notes that Sector Risk Management Agencies "leverage their particular knowledge and expertise to fulfill a number of information sharing, coordination, incident response, and technical assistance responsibilities to their assigned critical infrastructure sector(s)." To fulfill DOE's responsibilities, CESER will continue to develop and expand cyber situational awareness and response capabilities the current threat landscape to support the energy sector and to provide cyber response technical assistance and expertise unique to the energy sector. Additionally, as the Nation's energy infrastructure faces consciously evolving threats that require interdisciplinary expertise and coordination, DOE is looking to develop capabilities that will enable collaboration across multiple DOE Offices, leveraging subject matter experts from the DOE National Labs, as well as industry and interagency partners to help ensure the security of the energy sector.

  CESER's Response and Restoration division's FY 2024 Budget will continue enhancement of energy sector cyber situational awareness and build upon the results of a cybersecurity mission needs and capabilities study undertaken in 2021. Leveraging this enhanced cyber situational awareness, CESER will continue to develop cyber threat analysis to rapidly assess emerging threats, new malware, and novel tactics, techniques, and procedures from adversaries, to provide timely and actionable information to trusted industry partners. The cyber situational awareness program also works to provide initial review of any reports of cyber incidents in the energy sector, including reports to the Department or victim notification from DHS or FBI, and serves at the initial point of contact for coordination. Additionally, the cyber situational awareness program provides analysis of potential impacts from cyber incidents, potential incidents, and threats in the energy sector, including potential for cascading impacts that could impact other critical infrastructure.

  CESER will continue to work with the DOE National Laboratories on expertise to leverage during a cyber incident impacting the energy sector, including the development of tools and capabilities to provide focused technical assistance. These tools and capabilities will compliment efforts by other Federal Agencies, focusing on the unique aspects of the energy sector to provide technical assistance, subject matter expertise, and support cyber incident response at scale, if multiple energy sector entities are impacted by a cyber incident simultaneously. Additionally, the Department will coordinate with federal partners to be able to provide technical assistance and subject matter expertise to help assess unattributed incidents for potential cyber nexus. The FY 2024 budget will also build on training the Department's ESF #12 responder to continue to build a deeper knowledge of energy management systems (e.g., distributed energy resources, grid SCADA controls, etc.) to support a cyber response.

  Cyber situational awareness and analysis efforts will also be integrated into the Energy Threat Analysis Center (ETAC) pilot, to help develop mitigations and recommendations to address the unique operating requirements of the energy sector. The FY 2024 request includes $5 million to develop and expand the ETAC pilot in partnership with energy sector owners and operators, National Laboratories, the intelligence community, and DHS/CISA's Joint Cyber Defense Collaborative. The pilot program will provide the sector joint analysis of classified and unclassified cyber threats, inform the intelligence community's key intelligence questions process, and provide defensive measures to the thousands of energy companies, including electricity, oil, and natural gas, from across the country by leveraging analytics, subject matter expertise, and joint analysis. Leveraging this enhanced cyber situational awareness, CESER will continue to develop cyber threat analysis products that provide timely and actionable defensive cybersecurity information to trusted industry partners. The FY 2024 pilot activities, informed by the completed ETAC Feasibility Study and FY 2023 ETAC Pilot activities, will include: 1) establishing a government and industry operational collaborative capability to develop actionable operational intelligence and offer meaningful threat mitigation advice and actions to change the trajectory of our collective (government and industry) defense, response, and resilience of the U.S. energy sector; 2) enabling an information exchange among government and industry to address a shared problem, a process to connect the dots for national security, public health, safety and economy; 3) improving detailed understanding of national security risks associated with the energy sector which are or could be exploited by adversaries, including nation-states; 4) achieving a deeper understanding of threat actor tactics, capabilities, and activities with potential to impact systemic risks to the energy sector; and 5) facilitating increased intelligence-sharing between industry and government of actual acute threat activity, including incidents, to ensure U.S. energy security and resilience for all Americans.

Response and Restoration
Funding ($K)

	FY 2022 Enacted	FY 2023 Enacted	FY 2024 Request	FY 2024 Request vs FY 2023 Enacted ($)	FY 2024 Request vs FY 2023 Enacted (%)
Response and Restoration					
All-Hazards Incident Response, Regional Support, and Situational Awareness	10,400	11,000	22,000	+11,000	+100.0%
Cyber Incident Response and Cyber Situational Awareness	7,600	12,000	17,000	+5,000	+41.7%
Total, Response and Restoration	**18,000**	**23,000**	**39,000**	**+16,000**	**+69.6%**

Response and Restoration
Explanation of Major Changes ($K)

	FY 2024 Request vs FY 2023 Request
• All-Hazards Incident Response, Regional Support, and Situational Awareness - Sustain current response capabilities while expanding regional steady state and response presence in accordance with the 2021 Regional Response Operations Strategic Plan (2021-2026). Continue the development of collaboration tools and products to provide enhanced energy sector situational awareness to interagency and industry partners, and the CESER Response Team. Further develop operational concepts for a CESER Watch Office and conduct feasibility studies for a physical facility. Moves the EAGLE-I program from RMT to R&R, gaining access to dashboards for incidents across the nation for the energy industry.	+11,000
• Cyber Incident Response and Cyber Situational Awareness - Continue implementation of recommendations made in the 2021 CESER Cybersecurity Needs and Capabilities Assessment, a third-party study that identified recommendations to improve CESER's cybersecurity and cyber incident response posture. Efforts include enhancing capacities for rapid analysis of cyber threats to the energy sector and focused technical assistance to address unique challenges for cyber incident response in the sector. Continue development of the Energy Threat and Analysis Center (ETAC) operational concepts and implement recommendations from completed feasibility studies.	+5,000
Total, Response and Restoration	**+16,000**

Response and Restoration

Activities and Explanation of Changes ($)

FY 2023 Enacted	FY 2024 Requested	Explanation of Changes FY 2024 Request vs FY 2023 Enacted
Response and Restoration $23,000,000	**$39,000,000**	**+$16,000,000**
All-Hazards Incident Response, Regional Support, and Situational Awareness $11,000,000	*$22,000,000*	*+$11,000,000*
• Maintain current capabilities and expand the regional knowledge, skills, and abilities of the ESF #12 cadre of trained volunteer emergency responders, focusing efforts on hurricanes, wildfires, earthquakes, and cyber-attacks. • Focus on expanding training and capabilities to support remote and rural location responses, educating responders on regionally specific energy infrastructure in order to improve emergency response to ever changing energy and cross sector interdependencies; provide support and technical assistance to the SLTT State Energy Assurance planning. Expand access to available subject matter expertise across the DOE enterprise, to include the National Labs. • Execute CESER Regional Expansion Pilot program for full-time federal regional staff presence to include federal staff and regional facilities or share location in three FEMA regions. • Continued focus on and commitment to CESER's Regionalization model by expanding the Office's responder recruitment including Catastrophic Incident Response Team (CIRT) and cybersecurity responders. Expand steady-state operational capabilities to support regional and state day-to-day operations and preparedness efforts.	• Maintain current capabilities and expand the regional knowledge, skills, and abilities of the ESF #12 cadre of trained volunteer emergency responders, focusing efforts on hurricanes, wildfires, earthquakes, and cyber-attacks. • Focus on expanding training and capabilities to support remote and rural location responses, educating responders on regionally specific energy infrastructure in order to improve emergency response to ever changing energy and cross sector interdependencies; provide support and technical assistance to the SLTT State Energy Assurance planning. Expand access to available subject matter expertise across the DOE enterprise, to include the National Labs. • The Regional Expansion Pilot will conclude with recommendations for permanent implementation including staffing (teams), management, and facilities. • Continued focus on and commitment to CESER's Regionalization model by expanding the Office's responder recruitment including Catastrophic Incident Response Team (CIRT) and cybersecurity responders. Expand steady-state operational capabilities to support regional and state day-to-day operations and preparedness efforts. • Ensure CESER can fulfill the Department's responsibilities as the SRMA for the energy sector	• Due to the operational capability and technical maturity of EAGLE-I as the U.S. Government's situational awareness platform for the energy sector, CESER internally transferred the EAGLE-I program from the Risk Management and Tools (RMT) division to the Response and Restoration (R&R) division for FY 2024. • Increasing emergency responder capabilities and steady state regional working relationships to improve response effectiveness in an all-hazards environment through enhanced multi modal training, situational awareness products and tools, and continuity of the Federal missions and mission essential functions. • Build out three regionally focused response teams that will work with states and regions on emergency response, conduct joint exercises and training with the SLTT and industry as ESF #12 embedded responders and strengthen DOE's partnerships with the energy sector to focus on blue sky days for emergency response and state energy security planning. The current response capabilities and teams are a volunteer workforce. • This funding will allow CESER to conduct feasibility studies to build out a dedicated watch capability and have contracted staffing for day to day operations. The to expand on existing Situational Awareness Program to help continuously monitor and anticipate disruption to the energy sector,

FY 2023 Enacted	FY 2024 Requested	Explanation of Changes FY 2024 Request vs FY 2023 Enacted
• Develop the operational concepts for a dedicated CESER Watch Office to provide daily energy sector monitoring, reporting, and support to emergency response operations. • Adopt and integrate CESER's emergency authorities (DPA, Jones Act, FPA 202c) into standard operational processes and procedures; train DOE offices, contractors and external stakeholders; and provide accurate, comprehensive, and usable public information for those wishing to use these authorities.	and as the coordinating agency for ESF #12, across all-hazards, by maintain continuous situational awareness of threats and incidents impacting, or potentially impacting, U.S. energy systems, as well as capabilities for rapid analysis to help mitigate threats and ensure timely preparedness, response, and recovery efforts. • CESER will continue to develop and maintain the EAGLE-I platform, including efforts to expand near real-time situational awareness of both electricity and oil and natural gas systems, as well the development and integration of new and/or update capabilities, including enhanced situational awareness of the fuel supply chain, such as retail fuel availability, as well as remote sensing and modeling to support energy sector preparedness, response, and recovery efforts. • Conduct feasibility studies for a physical facility for a CESER Watch Office to expand on existing Situational Awareness Program to help continuously monitor and anticipate disruption to the energy sector, with the capability to quickly analyze and model potential impacts to the electric power, oil, natural gas, and the growing renewable energy infrastructure to include market impacts to the economy and to determine the effect and disruption on other critical infrastructure, including Defense Critical Energy Infrastructure. • Enhance guidance, informational products, communications, and stakeholder education/engagement around CESER's emergency authorities (DPA, Jones Act, FPA 202c) including onsite training for DOE site offices, laboratories, contractors and external stakeholders.	with the capability to quickly analyze and model potential impacts to the electric power, oil, natural gas. The Watch Office will also provide a single point of contact for CESER's situational awareness, analysis, and response activities and enable to Department to meet growing demand for awareness and analysis to all-hazards, in real time.

FY 2023 Enacted	FY 2024 Requested	Explanation of Changes FY 2024 Request vs FY 2023 Enacted
Cyber Incident Response and Cyber Situational Awareness $12,000,000	*$17,000,000*	*+$5,000,000*
• Funding will build on DOE's ESF#12 catastrophic response capabilities to add cybersecurity and cyber incident response capacity that better supports energy sector entities impacted by a cyber event. The enhanced capability will also improve and expand DOE's support to the Federal Government's coordinated cyber incident response as mandated by PPD-41 and the National Cyber Incident Response Plan. • Implement the findings and recommendations in the 2021 CESER Cybersecurity Needs and Capabilities Study, through contract support, looking at the national lab capabilities to support cyber incident response, and conducting follow on feasibility studies for physical watch offices and secure space to support cyber operations. • Develop Energy Sector Cybersecurity Response capabilities that can support CISA and FBI cyber incident response teams to provide energy sector subject matter expertise about energy systems. • Identify and equip dedicated CESER classified space to support cyber response operations. • Support a feasibility study and pilot for the Energy Threat Assessment Center (ETAC) concept, as part of a comprehensive approach leveraging DOE project management principles and best practices including DOE O 413.3B Program and Project Management for the Acquisition of Capital Assets.	• Continued enhancement of energy sector cyber situational awareness to rapidly assess emerging threats, new malware, and novel tactics, techniques, and procedures from adversaries, to provide timely and actionable information to trusted industry partners. • Initial review of any reports of cyber incidents in the energy sector, including reports to the Department or victim notification. • Analysis of potential impacts from cyber incidents, potential incidents, and threats in the energy sector, including potential for cascading impacts that could impact other critical infrastructure. • Tools and capabilities to provide focused technical assistance to address unique complexities of the energy sector. • Based on the FY22 ETAC pilot feasibility study and FY 2023 pilot actions with appropriate OMB and Congressional approvals, in FY 2024 CESER will begin to fully implement the ETAC in partnership with the Cybersecurity and Infrastructure Security Agency's (CISA) Joint Cyber Defense Collaborative (JCDC) to advance industry-government threat situational awareness, mitigation, and response.	• Funding will support the Energy Threat Analysis Center (ETAC) pilot focused on bringing together industry and government, intelligence and non-intelligence, and owners and operators and manufacturers to address the growing cyber threat to U.S. energy infrastructure from Nation-States and criminal groups. ETAC funding will help maintain and build on the pilot operations of the ETAC and will be implemented int close collaboration with CISA, energy sector owners and operators, and the intelligence community.

Program Direction

Overview

Program Direction provides for costs associated with federal workforce staffing to include salaries, benefits, travel, training, and other related expenses. Program Direction funds also provide for costs associated with contractor services managed under the direction of the federal workforce. Contractors support the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) mission. In an effort to retain and attract highly technical engineering and cybersecurity staff in the Federal government to address the growing cybersecurity, physical, and climate-based threats to energy system, CESER's FY 2024 request include cybersecurity incentives, cybersecurity training, and other measures to retain a highly-qualified staff.

Salaries and Benefits support federal employees who provide executive management, programmatic oversight, and analysis for the effective implementation of the CESER program. This includes staff at Headquarters and the National Energy Technology Laboratory (NETL) to support the overall mission of CESER. While CESER funds NETL staff within its budget, the NETL Federal employees are included within the full-time equivalent (FTE) total within the Fossil Energy Research and Development account.

CESER federal staff provide oversight for a wide range of energy security, resilience, cybersecurity, and emergency response functions and programs. These programs and functions include: guiding a multi-million dollar Risk Management Tools (RMT) program; staffing and managing the Department's all hazard energy sector emergency response function (ESF #12); training and coordinating a cadre of more than 100 volunteer energy sector emergency responders; overseeing annual programs of energy sector exercises, workshops, interagency and industry engagement, and coordination with states and localities before and during emergencies; and the development of reports and analyses on threats and hazards to the energy sector. An increased need is seen in the area of cybersecurity preparedness and incident response. CESER works closely with the Offices of the Chief Information Officer and Chief Human Capital Officer (OCHO) and other program offices as part of the DOE's Cyber Retention Program allowing cybersecurity incentives of up to 25% of the eligible employee's salary. Similar to programs implemented at the Cybersecurity and Infrastructure Security Agency (CISA), this provides a means to recruit and retain highly skilled cybersecurity talent at the Department. The cybersecurity field is in high demand across both public and private sectors. The Federal government salary in this field is significantly lower than the industry standard; we are finding it increasingly more difficult to recruit and retain qualified candidates. Federal staff also support crosscutting functions which include budget, procurement, contracts, and human resources.

When Presidential Disaster Declarations are issued CESER staff are called upon under the National Response Framework. Trained staff provide support for Federal Emergency Management Agency (FEMA) Emergency Support Function 12 (ESF #12) missions. Some of these trained responders may be ordinarily employed in other parts of DOE, such as the Office of Energy Efficiency and Renewable Energy or the Power Marketing Administrations. During ESF #12 activations CESER is reimbursed by FEMA for overtime expenses while CESER responder base pay is funded from the CESER Program Direction budget.

CESER's staffing efforts continues to focus on building core capabilities of partnerships with industry as the energy sector SRMA, capability building in the energy sector, risk analysis of cybersecurity, physical, and natural hazard risks, and emergency response activities. Further, the program direction will help strengthen CESER's budget and human resources staff to growing 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 development and deployment of risk management tools, programs, and projects in the field; attendance at industry, interagency and regional state government energy sector emergency response coordination meetings; and conducting emergency response training for responders in conjunction with Department of Homeland Security regional response centers. FEMA reimburses DOE for all travel associated with Presidential Disaster Declarations. CESER will continue to utilize virtual meetings and training to achieve savings.

Support Services include contractor support directed by Federal staff to perform administrative tasks and provide analysis to management. Additional support services may include support from Internship programs utilized through Oak Ridge Institute for Science and Education and DOE's Minority Educational Institution Student Partnership Program assignments.

Other Related Expenses include DOE's Working Capital Fund support, Energy Information Technology Services, minor construction, equipment purchases, upgrades, and replacements, office furniture, commercial credit card purchases using simplified acquisition procedures when possible, general and advanced training, and miscellaneous expenditures.

Highlights of the FY 2024 Budget Request

This budget request accounts for the increased FTE and 5.2% projected pay raise for federal employees, participation in the cybersecurity retention incentive program, and reconfiguring existing space for increased hybrid work environment, all of which are to ensure CESER is competitive in Federal government hiring and retention of a highly skilled workforce.

Program Direction
Funding ($K)

	FY 2022 Enacted	FY 2023 Enacted	FY 2024 Request	FY 2024 Request vs FY 2023 Enacted ($)	FY 2024 Request vs FY 2023 Enacted (%)
Program Direction Summary					
Washington Headquarters					
Salaries and Benefits	8,751	15,215	20,683	+5,468	+35.9%
Travel	254	295	250	-45	-15.3%
Support Services	2,143	4,211	3,791	-420	-10.0%
Other Related Expenses	1,392	1,763	3,771	+2,008	+113.9%
Total, Washington Headquarters	12,540	21,484	28,495	+7,011	+32.6%
National Energy Technology Laboratory					
Salaries and Benefits	1,658	1,754	2,115	+361	+20.6%
Travel	110	116	120	+4	+3.4%
Support Services	315	333	981	+648	+194.5%
Other Related Expenses	1,377	1,456	764	-692	-47.5%
Total, National Energy Technology Laboratory	3,460	3,659	3,980	+321	+8.8%
Total Program Direction					
Salaries and Benefits	10,409	16,969	22,798	+5,829	+34.4%
Travel	364	411	370	-41	-10.0%
Support Services	2,458	4,544	4,772	+228	+5.0%
Other Related Expenses	2,769	3,219	4,535	+1,316	+40.9%
Total, Program Direction	16,000	25,143	32,475	+7,332	+29.2%
Federal FTEs	44	**93**	113	+20	+21.5%
Additional FE FTEs at NETL supporting CESER[a]	9	11	11	0	0.0%
Total CESER-funded FTEs	**53**	**104**	**124**	**+20**	**+19.2%**

[a] 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.

	FY 2022 Enacted	FY 2023 Enacted	FY 2024 Request	FY 2024 Request vs FY 2023 Enacted ($)	FY 2024 Request vs FY 2023 Enacted (%)
Support Services and Other Related Expenses					
Support Services					
Technical Support	1,770	3,906	3,824	-82	-2.1%
Management Support	688	638	948	+310	+48.6%
Total, Support Services	2,458	4,544	4,772	+228	+5.0%
Other Related Expenses					
Other Services	832	1,580	1,551	-29	-1.8%
EITS Desktop Services	564	639	800	+161	+25.2%
WCF	1,373	1,000	2,184	+1,184	+118.4%
Total, Other Related Expenses	2,769	3,219	4,535	+1,316	+40.9%

Program Direction

Activities and Explanation of Changes

FY 2023 Enacted	FY 2024 Request	Explanation of Changes FY 2024 Enacted vs FY 2024 Request
Program Direction $25,143,000	**$32,475,000**	**+$7,332,000**
Salaries and Benefits $16,969,000	*$22,798,000*	*+$5,829,000*
• For 93 FTEs at HQ and 11 FTEs at NETL that provide executive management, programmatic oversight, and analysis for the effective implementation of the CESER program.	• For 93 FTEs at HQ and 11 FTEs at NETL that provide executive management, programmatic oversight, and analysis for the effective implementation of the CESER program.	• Increase of 20 FTEs, projected 5.2% pay raise and increase of recruitment and retention incentive value and quantity in participation with the DOE Cybersecurity retention incentive program to gain and maintain the highly technical engineering and cybersecurity staff required.
Travel $411,000	*$370,000*	*-$41,000*
• Travel includes transportation, subsistence, and incidental expenses that allow CESER to effectively facilitate its mission.	• Includes both international and U.S. travel for CESER mission needs.	• Reduced based on Mission needs and focus on workforce growth and mitigated by increased use of virtual meeting options and virtual training.
Support Services $4,544,000	*$4,772,000*	*+$228,000*
• Support Services includes contractor support directed by the federal staff to provide analysis to management.	• Includes support of budget, acquisition, human resources, communications, business systems, and administrative support needs.	• The increase is due to an increase in contractual costs.
Other Related Expenses $3,219,000	*$4,535,000*	*+$1,316,000*
• Includes equipment upgrades and replacements, office furniture, minor construction, commercial credit card purchases using simplified acquisition procedures when possible, and miscellaneous expenditures.	• Includes additional 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.	• Increase for additional support for staff, continued telework laptops and mobile devices and improved hoteling space and telecom resources. • Increase in specialized training, such as Certified Information Systems Security Professional or SANS training, to recruit and retain cybersecurity specialist. • Increase in WCF and EITS support associated with increased FTE.

Cybersecurity, Energy Security, and Emergency Response

Research and Development ($K)

	FY 2022 Enacted	FY 2023 Enacted	FY 2024 Request	FY 2024 Request vs FY 2023 Enacted ($)	FY 2024 Request vs FY 2023 Enacted (%)
Basic	0	15,000	12,000	-3,000	-20.0%
Applied	0	59,000	63,000	+4,000	+6.8%
Development	70,000	29,000	31,000	+2,000	+6.9%
Total, R&D	70,000	103,000	106,000	+3,000	+2.9%

Small Business Innovative Research/Small Business Technology Transfer (SBIR/STTR) ($K)

	FY 2022 Enacted	FY 2023 Enacted	FY 2024 Request	FY 2024 Request vs FY 2023 Enacted ($)	FY 2024 Request vs FY 2023 Enacted (%)
Risk Management Tools	1,278	2,482	2,491	+9	+0.4%