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, $202,143,000, to remain available until expended: Provided, That of such amount, $25,123,000 shall be available until September 30, 2024, for program direction. *(Energy and Water Development and Related Agencies Appropriations Act, 2021.)*

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 2021 Enacted	FY 2022 Annualized CR	FY 2023 Request
156,000	156,000	202,143

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 secure U.S. energy infrastructure against all hazards, reduce the risks of and impacts from cyber events and other disruptive events, and assist with 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, 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.

The energy sector plays a critical role across Federal, State, and local jurisdictions, and with nearly all other critical infrastructures relying on the power and fuel to operate. CESER programs work in an integrated manner with industry, state, local, tribal, and territorial (SLTT) governments, as well as with federal departments and agencies, to enhance the resilience - the ability to withstand, maintain critical function and quickly recover from disruptions - and security - the ability to reduce risks in the protection system assets and critical functions from unauthorized access and actions - of the U.S. energy infrastructure for all Americans. Secure and resilient energy infrastructure is critical to U.S. national security and economic security.

CESER leads, coordinates, and provides technical expertise related to cybersecurity and resilience across the various DOE offices to ensure that all of DOE's efforts are designed or executed with these in mind. For example, CESER is implementing its cybersecurity-by-design strategy, in which cybersecurity considerations are incorporated into new clean energy technologies as they are developed by the applied energy offices. CESER also provides indispensable industry-specific technical assistance across the intra-agency that enables the administration to guide critical decisions aimed at ensuring reliability, resilience, and security of national energy infrastructure, as well as assisting our international partners, as necessary.

Within the appropriation, CESER funds will:

- Develop and deliver game-changing tools and technologies to help the energy sector, including owners and operators, manufacturers, state and local energy officials, third-party integrators, and others, to secure and reduce risks to critical infrastructure from cyber, physical, and natural hazard threats. As the U.S. moves to a carbon-pollution free energy sector by 2035, CESER will work closely with clean energy providers and integrators to ensure that cybersecurity and resilience are core components. Finally, DOE will continue to strengthen the supply chain security and resilience of the sector.
- Lead public and private-sector partnerships to inform energy sector security and resilience policies at the Federal and State levels. Further, CESER will support capacity-building through activities such as exercises, training, technical assistance, and workforce development initiatives.
- Expand its risk analysis capabilities, which will inform the develop of policies, tools and technologies, and response and recovery efforts across CESER, the Department, and the broader sector.
- Lead Emergency preparedness and response, supporting the energy sector, to pursue enhancements to national efforts, in cooperation with public and private-sector stakeholders, for preparedness, resilience, and recovery of U.S. energy infrastructure from all threats and hazards.

Highlights and Major Changes in the FY 2023 Budget Request

- **Information Sharing, Partnerships, and Exercises** ($28,000,000), whose functions are performed under the Preparedness, Policy, and Risk Analysis Division, supports energy sector security and resilience through coordination with government and industry partners. These efforts will advance the Department's efforts to support the SLTT community and energy industry in preparing for, mitigating, and recovering from all threats and hazards facing the U.S.

energy sector. CESER will achieve this through information sharing, risk assessments, capacity building in planning and resilience, and targeted training and exercises. The requested increase will support CESER's increased workload given the rapidly-evolving cyber threats that all industries are facing as a result of an increase in connectedness of the lives of Americans. It will also support exciting new workforce- and supply chain-related activities that CESER is leading, and it will provide resources for studies of, and support to, economically disadvantaged communities for response and recovery. This increase will also support training for the next generation workforce on energy sector risks and developing the workforce through training and exercises.

- **Risk Management Tools and Technologies** ($125,020,000) supports the development of tools and technologies to address cyber, physical, natural hazard, and other threats to the U.S. energy sector. CESER will invest in frameworks, tools, and technologies to identify, protect, prevent, mitigate, and respond to threats to energy systems. This will include establishing an Energy Cyber Sense program, which will consist of 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 (SBOMs) and hardware bill of materials (HBOMs), and other similar efforts. Risk Management Tools and Technologies (RMT) will develop and maintain the Environment for Analysis of Geo-Located Energy Information (EAGLE) situational awareness monitoring program. This line of effort will also continue to lead cross-cutting cybersecurity research, development, and deployment efforts and coordinate cybersecurity across DOE's applied energy and science offices. This program will also continue to address threats such as geomagnetic disturbances (GMD) and electromagnetic pulse (EMP). Finally, it 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.

- **Response and Restoration** ($24,000,000) coordinates a national effort to ensure that the sector is able to respond and restore from emergencies resulting from natural hazards, cyber-attacks, physical attacks, and other threats facing energy infrastructure. This line of effort lead DOE and CESER's roles as ESF #12 – Energy and SRMA/SSA in support of Presidential Policy Directive-41 United States Cyber Incident Coordination. CESER will work 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 analytical capabilities to assess and mitigate risks and threats to energy infrastructure has proven critical during events such Hurricane Ida, Colonial Pipeline ransomware cyber-attack, and others. These efforts are in close partnership with agencies such as the FEMA, DHS/CISA, FBI, and the Intelligence Community.

FY 2021 Key Accomplishments

CESER made notable progress this fiscal year that is rooted in the strategic partnerships it has fostered across the energy sector in executing its mission. In 2021, CESER:

- Continued to ensure the reliability of critical energy infrastructure during the COVID-19 pandemic, in close coordination with the States and energy system owners and operators, and facilitated the response as lead agency for Emergency Support Function #12 to multiple nationwide and regional energy disruptions and emergencies in close coordination with interagency partners and state and local governments.
- Launched the 100-Day Electricity Sector Industrial Control Systems Cybersecurity Initiative with DHS and the National Security Council and gained commitments from more than 155 electric utility companies (serving more than 75 million American customers) to advance technologies that will make the industrial control systems that operate the nation's electricity operations more cyber-secure.
- Executed various funding activities including a Funding Opportunity Announcement for $8M to conduct university-based research and development. Setting up agreements with industry to provide technical support and training to municipal and cooperative utilities to deploy detection and monitoring technologies to improve visibility on operational networks.
- Awarded $4 million for four National Laboratory projects focused on developing and deploying solutions to risks posed by EMP attacks and naturally occurring GMD events.

- Continued to enhance the Department-wide cyber vulnerability testing program, leveraging unparalleled technical expertise from the National Labs, to assess digital components in energy systems. The program has participation agreements with critical energy sector manufacturers and asset owners and is testing components of priority policy and security importance.
- Completed 20 research and development projects and launched seven new projects along with transitioning seven technologies into practice at energy companies.
- Expanded the Operational Technology (OT) Defender Fellowship, offering middle- and senior-level OT security managers in the U.S. energy sector an opportunity to more fully understand the cyber strategies and tactics that adversarial state and non-state actors use in targeting U.S. energy infrastructure.
- 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.
- Identified use cases and developed tools to enhance detection of malicious cyber activity in OT networks and expanded tools to include application in the wind industry.
- Released Version 2.0 of the C2M2, which better addresses new technologies like cloud, mobile, and artificial intelligence and evolving threats such as ransomware and supply chain risks. The update was guided by the Energy Sector C2M2 Working Group, which included 145 information technology and OT cybersecurity experts representing 77 energy sector and cybersecurity organizations.
- Hosted "Conquer the Hill - Adventurer Edition" competitions as part of CyberForce, an element of DOE's workforce development program. CyberForce started in 2016 as an annual collegiate level competition where teams defend simulated energy infrastructure from cyber-attacks. Since 2016, the main event, CyberForce Competition® has grown from eight competing teams in 2016 to one hundred teams in 2019 and more than 200 individual students competing virtually in 2020. The next CyberForce Competition will be held in November 2021.
- Responded to the severe winter storms in Texas in February 2021, Colonial Pipeline cyber-attack in May 2021, Hurricane Ida, and other events throughout the year.

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

	FY 2021 Enacted	FY 2022 Annualized CR	FY 2023 Request	FY 2023 Request vs FY 2021 Enacted ($)	FY 2023 Request vs FY 2021 Enacted (%)
Cybersecurity for Energy Delivery Systems	96,000	0	0	-96,000	-100.0%
Infrastructure Security and Energy Restoration	0	0	0	0	N/A
Information Sharing, Partnerships, and Exercises	11,402	0	28,000	+16,598	+145.6%
Risk Management Tools & Technologies	30,615	95,000	125,020	+94,405	+308.4%
Response and Restoration	5,983	48,000	24,000	+18,017	+301.1%
Program Direction	12,000	13,000	25,123	+13,123	+109.4%
Total, Cybersecurity, Energy Security, and Emergency Response	**156,000**	**156,000**	**202,143**	**+46,143**	**+29.6%**
Federal Full Time Equivalent Employees (FTEs)	21	44	93	+72	+342.9%
Additional FE FTEs at NETL supporting CESER[a]	9	9	11	+2	+22.2%
Total CESER-funded FTEs	**30**	**53**	**104**	**+74**	**+246.7%**

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

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

	FY 2021 Enacted	FY 2022 Annualized CR	FY 2023 Request	FY 2023 Request vs FY 2021 Enacted ($)	FY 2023 Request vs FY 2021 Enacted (%)
Cybersecurity for Energy Delivery Systems	96,000	96,000	0	-96,000	-100.0%
Infrastructure Security and Energy Restoration	48,000	48,000	0	-48,000	-100.0%
Information Sharing, Partnerships, and Exercises	0	0	28,000	+28,000	+100.0%
Risk Management Tools & Technologies	0	0	125,020	+125,020	+100.0%
Response and Restoration	0	0	24,000	24,000	+100.0%
Program Direction	12,000	12,000	25,123	+13,123	+109.4%
Total, Cybersecurity, Energy Security, and Emergency Response	**156,000**	**156,000**	**202,143**	**+46,143**	**+29.6%**
Federal Full Time Equivalent Employees (FTEs)	21	44	93	+72	+342.9%
Additional FE FTEs at NETL supporting CESER[a]	9	9	11	+2	+22.2%
Total CESER-funded FTEs	**30**	**53**	**104**	**+74**	**+246.7%**

SBIR/STTR:

- FY 2021 Enacted: SBIR/STTR: $1077
- FY 2023 Request: SBIR/STTR: $1301

Bipartisan Infrastructure Law and Programmatic Realignment

CESER was appropriated funds through the Bipartisan Infrastructure Law (BIL) (P.L. 117-58). In FY 2023, CESER will continue to execute the following funded BIL programs:

- Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance Program (Section 40124)
- Cybersecurity for The Energy Sector Research, Development, And Demonstration Program (Section 40125(b))

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

- Energy Sector Operational Support for Cyberresilience Program (Section 40125(c)) (note that funds from this provision will be provided all in FY2022)

In addition to the funded BIL provisions listed above, CESER will also continue to support other offices where resources are made available to CESER for implementation of programs where CESER was not appropriated specific funding, including State Energy Plans (Section 40108), Modeling and Assessing Energy Infrastructure Risk/Advanced Energy Security Program to Secure Energy Networks (Section 40125(d)), and Cybersecurity Plan (Section 40126). Finally, CESER will continue its existing work on existing programs that have been funded under regular appropriations under Enhancing Grid Security Through Public-Private Partnerships (Section 40121), Energy Cyber Sense (Section 40122), and Incentives for Advanced Cyber Technology Investment (Section 40123).

Future Years Energy Program (FYEP)

($K)

	FY 2023 Request	FY 2024	FY 2025	FY 2026	FY 2027
Cybersecurity, Energy Security, and Emergency Response	$202,143	$207,000	$211,000	$216,000	$221,000

Major 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 2024 - FY 2027. The outyear funding levels use the growth rates from and match the outyear account totals published in the FY 2023 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 address real-world threats
- Overcome cyber 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

Risk Management Tools and Technologies (RMT)

Overview

The U.S. Department of Energy (DOE) is the Sector Risk Management Agency (SRMA) for the energy sector and the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) is responsible for carrying out the duties and responsibilities of that role, which include identifying, analyzing, and addressing risks to energy systems. CESER's Risk Management Tools and Technologies (RMT) division works closely with the energy sector to reduce risks from cyber and non-cyber hazards by researching, developing, demonstrating, and deploying tools and technologies that will be essential to fostering a clean and secure energy supply chain.

RMT will partner with National Laboratories, private sector, and academia to advance tool development, demonstration, and deployment projects in the private sector. These initiatives will leverage emerging technologies and techniques for critical energy infrastructure security to test and identify vulnerabilities; monitor, detect, and protect critical energy infrastructure and networks from threats; and enable automated assessment, situational awareness, and response to the threats to the sector. RMT will develop tools and technologies that incorporate rapid dissemination and processing of energy sector data for identification and characterization of threats for intelligence analysis, assessments, products, and services in unclassified and classified environments required to support CESER's operational cyber and energy security responsibilities. These specialized tools will use analytics to understand, enrich, and fuse data and enable intelligence-driven action to improve resilience for the energy sector. Further, RMT will work to address risks through tool development and intra-agency coordination on risks such as wildfires, hurricanes, and other natural hazards. The dynamic threat landscape, climate crisis, advances in energy system technologies, and the use of legacy devices in an aging infrastructure underscore the importance of this program.

The DOE is instituting cybersecurity by design approach across DOE's science and applied energy offices. This approach means that offices that perform research and development of energy delivery system will integrate cybersecurity requirements in their R&D activities. CESER will coordinate this integration and continue research and development 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 Research, Development and Demonstration of tools and technologies that 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 2023 Budget Request

Working closely with energy sector and government partners, the budget request for CESER RMT supports a more economically competitive, environmentally responsible, secure, and resilient U.S. energy infrastructure focusing on following activities:

- **ADVANCE TOOLS TO SUPPORT CYBER THREAT SITUATIONAL AWARENESS AND ANALYTICS ($45M)**
    - **<u>R&D on Cyber Tools and Technologies for Energy Systems ($35M)</u>**
      Research, develop, demonstrate and transition to practice next generation cyber tools that provide industry protection, monitoring, detection, response, containment, forensics, and recovery capabilities. Furthermore, these efforts will leverage grid and pipeline operational data and physics of energy delivery to inform owners and operators of anomalous cyber activities on their networks. These efforts will primarily be executed through funding opportunity announcements (FOA) that we require energy company, academia, national laboratory, and/or manufacturers.

Situational Awareness & Analytics ($10M) Research, develop, demonstrate, deploy, and transition to practice next generation cyber situational awareness tools and technologies that enable information sharing, and U.S. Government awareness of cyber threats through correlation with intelligence community information.

- **RISK MITIGATION TOOLS AND SITUATIONAL AWARENESS FOR NON-CYBER THREATS AND HAZARDS ($30M)**

  - **EAGLE-I, Situational Awareness & Response Capabilities ($10M)**
    To ensure that CESER can fulfill DOE's responsibilities as the SRMA for the energy sector and as the coordinating agency for Emergency Support Function (ESF) #12, CESER needs to maintain continuous situational awareness of threats and incidents impacting, or potentially impacting, U.S. energy systems, as well as capabilities to support timely preparedness, response, and recovery efforts. The necessary capabilities include modeling of potential power outages from severe weather (e.g. hurricanes) and remote sensing to quickly identify damaged energy sector infrastructure. To fulfill these requirements, the department uses EAGLE-I Platform to provide situational awareness across the energy sector and collaboration during a response.

    The FY 2023 budget request will enable CESER to 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 situational awareness of retail fuel availability, as well as remote sensing and modeling to support energy sector preparedness, response, and recovery effort related to wildfire, flooding, and no-notice incidents (e.g. earthquakes). Efforts will also focus on ensure existing capabilities are seamlessly integrated into EAGLE-I and support awareness of interdependent impacts across FEMA Lifeline 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. Finally, CESER will work to integrate relevant situational awareness from CESER cyber programs into EAGLE-I to ensure that EAGLE-I supports response efforts across all-hazards.

  - **EMP and GMD ($5M)**
    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 EMP vulnerability assessments of critical assets and identifying and estimating the cost of several mitigation options for each asset; performing EMP and GMD system assessments; testing critical generation components (setting up future testing on the most expensive critical components) to determine withstands to EMP and GMD; and partnering with industry (through cost shares) to field deploy an increased number of innovative cost-effective mitigation options for EMP and GMD based on results of vulnerability assessments.

  - **Non-Cyber Risk Mitigation Tools and Technologies ($15M)**
    Additionally, RMT will tackle other risks and hazards to the energy sector due to the impacts of climate change such as wildfires, severe hurricanes, flooding, and droughts. RMT will focus on the development of tools and risk characterization effort for early detection and mitigation from these types of risks to energy infrastructure. Finally, the RMT work will also address physical threats to infrastructure such as the Metcalf Substation physical attack.

- **SUPPLY CHAIN RISK MANAGEMENT ($30M)**

  - **Cybersecurity Testing for Resilient Industrial Control Systems (CyTRICS) ($20M)**
    CyTRICS is DOE's program for cybersecurity supply chain vulnerability testing, digital subcomponent enumeration, forensic analysis, and mitigation. 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. CyTRICS 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.

FY2023 funding will enable RMT and CESER to more broadly address supply chain risks to the energy sector as part of the Energy Cyber Sense program that was required as part of the Infrastructure Investment and Jobs Act (IIJA). This will include efforts such as the development of a software bill of materials (SBOM) and hardware bill of materials framework, furthering efforts related to Cyber-Informed Engineering (CIE), integrating supply chain research and testing with CESER's joint collaboration on threat analysis through the Energy Threat Analysis Center Pilot efforts, etc.

- **Cybersecurity of Distributed Energy Resources ($5M)**
  In FY2023, CESER will continue to prioritize efforts to improve the cybersecurity of distributed energy resources (DERs) and DER management systems. As introduction of DERs into the grid continues to accelerate, 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 cyber risks and the impacts to broader resilience to the grid.

- **Cybersecurity of Electric Vehicle Charging Infrastructure ($5M)**
  In FY2023, CESER's RMT program will continue its work to improve the cybersecurity of electric vehicle supply equipment (EV) charging infrastructure. The industry-led, whole-of-government-supported proliferation of EV charging infrastructure is a once in a generation opportunity to build cybersecurity and cyber resilience into a system that will serve Americans for decades. Therefore, it is critical for CESER's RMT program to understand the cyber risks, potential mitigation measures, and plausibility for implementation in communities. This can be affected through establishment of a program, continuing the pilot and demonstration of cybersecurity measures directed by FY 2021 appropriations, and developing a research and development strategy to pursue cybersecurity within this multi-program, multi-agency infrastructure deployment.

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

  - **Cyber-Informed Engineering and Consequence-Driven Cyber-Informed Engineering (CCE) ($5M)**
    CESER/Risk Management Tools and Technology will continue maturing cyber resilience of the nation's most critical energy infrastructure through engineering protections by way of CIE and CCE efforts, which has proven immensely successful in helping energy companies secure and guarantee critical functions even in the face of successful adversary cyber intrusions. CCE includes a crown jewel analysis and links it with known threat actor behavior/reporting to help energy companies better prioritize and protect those critical functions. CESER will implement recommendations from the National Cyber Informed Engineering (CIE) Strategy. CIE includes foundational principles to help lead the nation's effort to integrate cybersecurity and engineering practices. Widespread adoption of these security and engineering principles in both the private and public sectors, as well as in academia to develop the cyber/engineering workforce of the future, is critical to ensure hardening of the nation's energy infrastructure against catastrophic cyber-enabled sabotage.

  - **Tools leveraging methodologies and frameworks ($5M)**
    CESER/Risk Management Tools and Technology will leverage methodologies like the Cybersecurity for Operational Technology Environment (CyOTE) to further research and innovation to enable early detection of anomalous behavior and threats in OT network.

  -
  - **Quantification of Cyber Risk and Cyber Risk Profiles for Critical Systems and Technologies ($5M)**

Develop and transition to practice tools, guidance, and practices that help energy organizations' understanding and management of cybersecurity risk to systems, people, assets, data, and capabilities. CESER will advance cybersecurity risk profiles for cloud environments and other applications. CESER will also work with energy system owners and operators to develop cyber risk quantification efforts, and support energy sector Cybersecurity Capability Maturity Model (C2M2) user community with guidance and facilitated cyber maturity evaluations.

- **Grid Modernization Laboratory Consortium and Department-Wide Coordination on Cyber R&D ($5M)**
  Support Grid Modernization Laboratory Consortium (GMLC) initiatives. GMLC employs an integrated approach to ensure DOE funded study efforts are efficiently coordinated for the greatest return on taxpayer dollars. CESER has a central role in the Department's plan for integration of cybersecurity activities across CESER will coordinate with DOE offices through the GMLC to engage experts and resources at DOE National Laboratories.

Risk Management Tools & Technologies
Funding ($K)

	FY 2021 Enacted	FY 2022 Enacted Annualized CR[a]	FY 2023 Request	FY 2023 Request vs FY 2021 Enacted ($)	FY 2023 Request vs FY 2021 Enacted (%)
Risk Management Tools & Technologies					
Advance Tools to Support Cyber Threat Situational Awareness and Analytics	59,925	59,925	45,000	-14,925	-24.9%
Risk Management Tools and Situational Awareness for Non-Cyber Threats and Hazards	11,295	11,295	30,000	+18,705	+165.6%
Supply Chain Risk Management	8,395	8,395	30,000	+21,605	+257.4%
Cyber Risk Assessments, Frameworks, and R&D Coordination	47,000	47,000	20,020	-26,980	-57.4%
Total, Risk Management Tools & Technologies	**126,615**	**126,615**	**125,020**	**-1,595**	**-1.3%**

SBIR/STTR:

- FY 2021 Enacted: SBIR/STTR: $0
- FY 2023 Request: SBIR/STTR: $1,301

[a] FY 2022 amounts shown reflect the P.L. 117–95 continuing resolution (CR) level annualized to a full year. These amounts are shown only at the "congressional control" level and above; below that level, a dash (–) is shown.

Risk Management Tools & Technologies
Explanation of Major Changes ($K)

	FY 2023 Request vs FY 2021 Enacted
• Advance Tools to Support Cyber Threat Situational Awareness and Analytics - R&D focus areas are informed by risk and threat landscape. Coordination and integration of cybersecurity by design will enable prioritization of cross-cutting tools and technologies and any unmet needs for legacy or emerging energy delivery systems.	-14,925
• Risk Management Tools and Situational Awareness for Non-Cyber Threats and Hazards - Expands the depth and scope of work to research, develop, demonstrate, deploy, and transition to practice tools and technologies.	+18,705
• Supply Chain Risk Management - More broadly address supply chain risks to the energy sector as part of the Energy Cyber Sense program that was required as part of the Infrastructure Investment and Jobs Act (IIJA).	+21,605
• Cyber Risk Assessments, Frameworks, and R&D Coordination - DarkNet transitioned to the Office of Electricity. Initial research has been completed and methodology published, activities such as CyOTE will transition to implementation across the DOE enterprise.	-26,980
• **Total, Risk Management Tools & Technologies**	**-1,595**

Risk Management Tools and Technologies
Funding

Activities and Explanation of Changes

FY 2021 Enacted	FY 2023 Request	Explanation of Changes FY 2023 Request vs FY 2021 Enacted
Risk Management Tools and Technologies **$126,615,000**	**$125,020,000**	**-$1,595**
Advance Tools to Support Cyber Threat Situational Awareness and Analytics $59,925,000	*$45,000,000*	*-$14,925*
• Research and develop cybersecure energy delivery systems • Advance threat information sharing initiatives to additional utilities to broaden the base to operationalize lessons learned • Continue to develop and deploy analytics for emerging adversary tools, techniques, and procedures under OT-focused initiatives • Appropriation included congressionally required $14M for Academia focused R&D activities	• Work with National Labs, industry, and academia to research, develop, demonstrate, deploy and transition to practice next generation **cyber risk management technology and tools** for broad adoption in energy industry	• R&D focus areas are informed by risk and threat landscape. Coordination and integration of cybersecurity by design will enable prioritization of cross-cutting tools and technologies and any unmet needs for legacy or emerging energy delivery systems • Reduced funding will result in fewer research and development awards

FY 2021 Enacted	FY 2023 Request	Explanation of Changes FY 2023 Request vs FY 2021 Enacted
Risk Management Tools and Situational Awareness for Non-Cyber Threats and Hazards $11,295,000	*$30,000,000*	*+$18,705,000*
• Work with National Labs, industry, and academia to research, develop, demonstrate, deploy, and transition to practice tools and technologies that reduce or mitigate risks from **non-cyber risks such as physical hazards, wildfires, floods, impacts of climate change, EMP and GMD.** This work includes outlays to maintain the EAGLE-I platform and develop/ update capabilities for situational awareness and enhanced collaboration between deployed responders, personnel at DOE Headquarters, as well as industry, state, and interagency partners	• Expand scope of work with National Labs, industry, and academia to research, develop, demonstrate, deploy, and transition to practice tools and technologies that reduce or mitigate risks from **non-cyber risks such as physical hazards, wildfires, floods, impacts of climate change, EMP and GMD.** This work includes outlays to maintain the EAGLE-I platform and develop/ update capabilities for situational awareness and enhanced collaboration between deployed responders, personnel at DOE Headquarters, as well as industry, state, and interagency partners	• Increase expands the depth and scope of work to research, develop, demonstrate, deploy, and transition to practice tools and technologies
Supply Chain Risk Management $8,395,000	*$30,000,000*	*+$21,605,000*
• Establish Energy Cyber Sense program including research, testing, analysis, and reporting to address cyber supply chain risks in the energy sector. Support government policies and orders to strengthen sector supply chain risk management capabilities and expand reach of supply chain risk management initiatives. This work includes demonstration of security practices for emerging technologies such as in Distributed Energy Resources or other key parts of the energy sector	• Expand scope of work with Energy Cyber Sense program including research, testing, analysis, and reporting to address cyber supply chain risks in the energy sector. Support government policies and orders to strengthen sector supply chain risk management capabilities and expand reach of supply chain risk management initiatives. This work includes demonstration of security practices for emerging technologies such as in Distributed Energy Resources or other key parts of the energy sector	• The increase will more broadly address supply chain risks to the energy sector as part of the Energy Cyber Sense program that was required as part of the Infrastructure Investment and Jobs Act (IIJA)

FY 2021 Enacted	FY 2023 Request	Explanation of Changes FY 2023 Request vs FY 2021 Enacted
Cyber Risk Assessments, Frameworks, and R&D Coordination $47,000,000	*$20,020,000*	*-$26,980,000*
• Continue the Advanced Threat Mitigation initiatives such as CYOTE supporting cybersecurity projects that use advanced and emerging technologies to protect and secure the energy delivery systems • Development and maintenance of the Cybersecurity Capability Maturity Model (C2M2) to improve transparency, cybersecurity preparedness and provide a better understanding of the cybersecurity capabilities, gaps and challenges facing utilities • Appropriation included congressionally required $10M for DarkNet, $5M for Consequence based Cyber Informed Engineering, and $2M for a pilot on electric vehicle charging facilities	• Develop, increase adoption, and measure adoption and impact of cybersecurity frameworks and methodologies in the energy sector. Work across applied energy and science offices to integrate cybersecurity into the R&D across DOE enterprise to ensure cybersecurity is designed in from ideation to execution. This work includes development of additional resources, profiles, and tools to support C2M2, CSF, and CYOTE user community	• DarkNet transitioned to the Office of Electricity • Initial research has been completed and methodology published, activities such as CyOTE will transition to implementation across the DOE enterprise

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's (CESER) Response and Restoration division leads efforts related to ESF-12, PPD-41, and other energy sector response-related functions for the Department.

As the lead for ESF #12, CESER works with partners to: assess the impacts of a disaster 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; provide technical expertise on energy damage assessment, restoration, and logistical assistance. During an incident requiring a coordinated federal response, the Response and Restoration program activates the Energy Response Organization to manage ESF #12 and SRMA 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. Within DOE, these responsibilities are managed by the Response and Restoration program in CESER, which supports preparedness, response, restoration, and recovery efforts in the energy sector, across federal, state, local, territorial, and tribal governments, private industry, trade associations, and non-governmental organizations.

To fulfill the Department's ESF #12 responsibilities, CESER trains and coordinates a cadre of volunteer responders from across DOE. Upon activation, DOE deploys responders to the FEMA National Response Coordination Center, FEMA Regional Response Coordination Centers, and/or FEMA Joint Field Offices and State Emergency Operations Centers. Each FEMA Region is represented by a Regional Coordinator, who maintains regular contact and supports planning efforts with regional and state counterparts. Additionally, a subset of responders is part of the ESF #12 Catastrophic Incident Response Team (CIRT) to respond to catastrophic incidents and remote locations.

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. The Department follows the National Cyber Incident Response Plan, representing the energy sector as the SRMA and supporting the Department of Homeland Security's (DHS) government-wide approach. DOE can support DHS Cyber Assessment Teams, Federal Bureau of Investigation (FBI) and industry with subject matter expertise when needed, leveraging the world-class capabilities of the DOE National Laboratories.

To ensure that CESER can fulfill DOE's responsibilities, the Response and Restoration division maintains and develops capabilities to coordinate response operations, enhance situational awareness, and provide analysis of threats and incidents affecting the energy sector, including cyber during steady state and response operations. Overall, the Response and Restoration division works closely with the electricity and oil and natural gas industries; other Federal agencies; State, Local, Tribal, and Territorial communities; and DOE's National Laboratories to advance national energy security and to prepare for, respond to, and recover from evolving threats and incidents.

Highlights of the FY 2023 Budget Request

The FY 2023 Request will enable CESER to maintain existing capabilities, while continuing to improve operational response coordination and collaboration; situational awareness across the energy sector; and analysis of threats and incidents affecting the sector. Additionally, the FY 2023 Request supports further development of CESER's cyber incident analysis and response capabilities as the Nation's energy infrastructure continues to face evolving and increasing threats.

ALL-HAZARDS INCIDENT RESPONSE, REGIONAL SUPPORT, AND SITUATIONAL AWARENESS ($12M)

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 DOE. 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.

The FY 2023 Budget Request will enable the Response and Restoration division to maintain baseline activities while continuing to develop long term relationships at the regional level, a day-to-day regional presence to work side-by-side with regional FEMA, interagency, and states partners during steady state operations: enabling more efficient response capabilities. 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, and provide 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

The FY 2023 Budget Request will continue the expansion of the Office's Situational Awareness Team, and feasibility study to develop the concept of operations and physical build out of a 24/7 CESER Watch Office at Headquarters, which will provide continuous monitoring, initial incident reporting, and communication coordination with field elements, deployed personnel, and interagency partners. The CESER Watch will also serve as the primary point of contact to manage information, requests, and assist with response activations on behalf of the U.S. energy sector.

CYBER INCIDENT RESPONSE AND CYBER SITUATIONAL AWARENESS ($12M)

CESER is the lead for cybersecurity for the energy sector as the SRMA, pursuant to the FAST Act, Executive Order 13636, and Presidential Policy Directive-41 (PPD-41). PPD-41 and interagency cyber response documents that were developed in partnership with Department of Homeland Security (DHS)/Cybersecurity and Infrastructure Security Agency (CISA), FBI, and other agencies that outline the roles of sector specific agencies and the ability to provide subject matter expertise during cyber response efforts. To fulfill DOE's responsibilities, CESER will continue to develop and expand capabilities commensurate with the threat landscape, to support the energy sector, 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 and to support the DHS Joint Collaborative Environment to look at threats across other critical infrastructure sectors, such as water and communications. The FY 2023 budget will expand the current responder training program to focus on a deeper knowledge of energy management systems (e.g., distributed energy resources, grid supervisory control and data acquisition controls, etc.). Additionally, CESER will continue work to establish a mechanism to quickly leverage technical resources and capability of DOE's National Laboratories, Power Marketing Administrations, and other resources to be utilized during a cyber incident response that requires federal support.

Further, the FY 2023 Budget will continue enhancement of energy sector cyber threat situational awareness and build upon the results of a cybersecurity mission needs and capabilities study undertaken in FY 2021. Leveraging this enhanced cyber situational awareness, CESER will continue to support Analysis of Risks in the Energy Sector Reports for provide timely and actionable cybersecurity information to trusted industry partners. Additionally, CESER will strengthen its cyber situational awareness capabilities and processes so that it can pull in and share data streams from and to energy sector owners and operators, other departments, and agencies (e.g., DHS/CISA, FBI), the intelligence community, along with data from CESER's other tools such as CyTRICS, NAERM, CRISP, etc. In FY 2023, CESER will establish the Energy Threat Analysis Center (ETAC), in partnership with CISA Joint Cyber Defense Collaborative, to advance industry-government threat situational awareness, mitigation, and response. The ETAC goals will be: 1) establish a government and industry operational collaborative environment 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) enable 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) improve detailed understanding of national security risks associated with the energy sector which are or could be exploited by adversaries, including nation-states; 4)

achieve a deeper understanding of threat actor tactics, capabilities, and activities with potential to impact systemic risks to the energy sector; and 5) facilitate increased intelligence-sharing between industry and government of actual acute threat activity, including incidents, in a secure setting, both physical and virtual, to ensure U.S. energy security and resilience for all Americans.

Response and Restoration
Funding ($K)

	FY 2021 Enacted	FY 2022 Annualized CR[a]	FY 2023 Request	FY 2023 Request vs FY 2021 Enacted ($)	FY 2023 Request vs FY 2021 Enacted (%)
Response and Restoration					
All-Hazards Incident Response, Regional Support, and Situational Awareness	5,683	5,683	12,000	+6,317	+111.2%
Cyber Incident Response and Cyber Situational Awareness	300	300	12,000	+11,700	+3,900.0%
Total, Response and Restoration	**5,983**	5,983	**24,000**	**+18,017**	**+301.1%**

[a] FY 2022 amounts shown reflect the P.L. 117–95 continuing resolution (CR) level annualized to a full year. These amounts are shown only at the "congressional control" level and above; below that level, a dash (–) is shown.

Response and Restoration
Explanation of Major Changes ($K)

	FY 2023 Request vs FY 2021 Enacted
• All-Hazards Incident Response, Regional Support, and Situational Awareness	+12,000
- 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	
• Cyber Incident Response and Cyber Situational Awareness	+12,000
- Continue implementation of recommendations made in the 2021 CESER Cybersecurity Needs and Capabilities Assessment, a third-party study that identified 27 recommendations to improve CESER's cybersecurity and cyber incident response posture. Continue development of the ETAC operational concepts and begin feasibility studies for an ETAC facility. Identify and equip dedicated CESER classified space for cyber response operations	
Total, Response and Restoration	**+24,000**

Activities and Explanation of Changes

FY 2021 Enacted	FY 2023 Request	Explanation of Changes FY 2023 Request vs FY 2021 Enacted
Response and Restoration $5,983,000	**$24,000,000**	**+$18,017,000**
All-Hazards Incident Response, Regional Support, and Situational Awareness $5,683,000	*$12,000,000*	*+$6,317,000*
• *ESF 12 Responsibilities*: Maintain and expand cadre of trained volunteer emergency responders, focusing efforts on: ○ Conduct a strategic review of the Response and Restoration Program to guide programmatic improvements over a 3-5 year period ○ Expanding regionalization of emergency response cadre to ensure established regional relationships and understanding ○ Develop critical incident response responder team to provide initial support challenging incidents and incidents in remote locations ○ Educating responders to evolving adversarial threats and energy sector interdependencies ○ Maintain availability of DOE to provide subject matter expertise, from DOE's Power Marketing Administrations • *Situational Awareness and Emergency Response Tools*: Enhance EAGLE-I™ to expand near real-time situational awareness capabilities and make it platform for integration energy infrastructure situational awareness tools • Support development, operationalization, and integration of modeling and tools, such as predicted power outage restoration timelines and remote sensing to provide damage assessments to further improve response 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 capability 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. Expand access to available subject matter expertise across the DOE enterprise, to include the National Labs • Continued focus on and commitment to CESER's Regionalization model by expanding the Office's regional operations and Catastrophic Incident Response Team (CIRT). Expand steady-state operational capabilities to support regional and state day-to-day operations and preparedness efforts • Develop the operational concepts for a dedicated CESER Watch Office to provide daily energy sector monitoring, reporting, and support to emergency response operations • Fully understand and integrate CESER's emergency authorities (DPA, Jones Act, FPA 202c) into standard operational processes and procedures	• 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

FY 2021 Enacted	FY 2023 Request	Explanation of Changes FY 2023 Request vs FY 2021 Enacted
Cyber Incident Response and Cyber Situational Awareness $300,000	*$12,000,000*	*+$11,700,000*
• Conduct a third party assessment of CESER's cybersecurity mission needs and capabilities focused on current capacity to conduct energy sector cyber incident response, CESER roles and responsibilities, and capability needs to support the cyber response mission	• 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 • Deploying a feasibility study for a physical ETAC capabilities	• The change included implementing corrections to the findings and recommendations in the 2021 CESER Cybersecurity Needs and Capabilities Study, which focused on identifying and clarifying cyber roles and responsibilities, and leveraging capability across CESER and the DOE enterprise to support cyber response operations • In 2021, a study was commissioned, focusing on identifying and clarifying cyber roles and responsibilities, and leveraging capability across CESER and the DOE enterprise to support cyber response operations. In 2023, focus will change to implementing the suggested changes • In 2021, initial operational concepts for the ETAC were developed, and in 2023, the concept will be expanded to include a feasibility study • A reorganization is included in FY 2023, including the addition of ETAC

Information Sharing, Partnerships, and Exercises

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 disaster events, cyber and physical security threats, aging/failing infrastructure, and the potential shortage of a skilled workforce, this budget is aimed at assessing security risk, securing critical infrastructure, enhancing infrastructure resilience, sharing information, and promoting learning and adaptation through strategic partnerships with the energy sector. The hazards to the energy system, including cyber, can only be effectively addressed through partnerships across all levels of government, private industry, and academia. The Office of Cybersecurity, Energy Security, and Emergency Response's (CESER) Preparedness, Policy, and Risk Analysis division at CESER is focused on cultivating these trusted partnerships to share information, manage risk, and increase the security and resilience of critical infrastructure in the energy sector.

CESER's partnerships—with energy owners and operators, manufacturers, and trade associations; with other Federal agencies; across States, local governments, tribes, territories (SLTT); with academia and the National Labs; and with the energy information sharing and analysis centers—help to advance collective preparedness and resilience to the growing landscape of threats, technology developments, and energy system trends. This budget is directed at: 1) continuing to build capacity and guidance for energy sector and SLTT partners to advance critical energy infrastructure security and resilience from all-hazards; and 2) managing key DOE authorities and responsibilities, including serving as the Sector Risk Management Agency (SRMA) for the energy sector and fulfilling DOE responsibilities under the Fixing America's Surface Transportation Act and the National Defense Authorization Act. True public-private partnership is integral to meeting CESER's cybersecurity, energy security, and emergency response objectives. As the SRMA for energy, the Department is currently assessing the following risks that are a priority for the energy sector, including, but not limited to, hurricanes/severe weather, wildfires, earthquakes, cyber-attacks and electromagnetic interference.

This program is the point of entry for SLTT and energy private sector partners when collaborating with DOE and the Federal Government on critical infrastructure protection and resilience, energy security, and emergency response and recovery. The Department is placing emphasis on supporting Section 9 companies[a], Defense Critical Electric Infrastructure companies, investor owned, municipal, and cooperative utilities in addition to SLTT energy entities.

Highlights of the FY 2023 Budget Request

The budget request supports a continued expansion of energy sector security and resilience 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. The budget request is focused on the President's priorities for combating climate change, creating clean energy jobs, and promoting energy justice. Activities will include studies of economically disadvantaged and underserved communities for emergency preparedness, response and recovery, the vulnerability of energy assets, and training, exercise, and workforce development opportunities.

Training the next generation workforce on energy sector risks and developing a cyber-educated workforce will be an overall emphasis in both Planning, Preparedness, and Resilience and Exercises and Training activities.

[a] 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."

Planning, Preparedness, and Resilience ($19M)

- **Manage Energy Sector Risk ($10M):** Establish new and build on existing mechanisms to work with energy companies to identify systemically important entities and perform intelligence-informed risk analysis, in close coordination with other DOE offices and through the National Labs, as well as in coordination with other Federal agencies and critical infrastructure sectors. As the SRMA energy sector lead, CESER will develop a robust capacity to better support the energy sector (e.g., owners and operators, trade organizations, subsector coordinating councils, SLTT, Section 9) need for a cohesive and coordinated set of resources and provide for more collaborative engagement opportunities to inform risk analysis. CESER will prepare and provide action-oriented, intelligence-informed threat briefings to support energy system investment and decision-making. CESER will also establish new coordination and relationship-building opportunities to identify and eliminate barriers to energy security information sharing across governments and industry.

- **Post Disaster Recovery and Resilience ($2M):** When a major disaster strikes, the restoration of energy systems depends on the planning and coordinated response effectiveness of local, State, multi-State, tribal, territorial, and national responses. In FY 2023, the SLTT Energy Assurance and Resilience program will continue to support technical assistance engagement for coordinated risk analysis and energy security and resilience planning with States and territories to improve preparedness to all hazards, including hurricanes, wildfires, fuel emergencies, and cyber events, and impacts from the growing threat of climate change. CESER will expand, aggregate, and deliver analyzed data to SLTT energy and emergency officials via dynamic risk analyses that build on lessons learned from exercises and real-world energy disruptions and informs SLTT policy and investment decisions. CESER will support communities during the recovery phase following major disasters by facilitating access to resources that will help to build resilience, protect critical energy infrastructure, and reduce or avoid impacts from future incidents.

- **Provide State Energy Security Planning Technical Assistance ($5M)**: Mitigating the impacts of climate change and cyber-attacks on critical energy infrastructure is a priority for state governments. Cybersecurity is also top of mind for many states who are aggressively pursuing new renewable distributed energy resources deployments. Enabling states to analyze and manage risk, coordinate across state agencies and with industry, and providing guidance and training to support these activities will bolster the states' energy security capabilities and national security overall. CESER will support state energy security and assurance planning through technical assistance and guidance on planning, designing and implementing robust energy security programs, and by continuously updating security planning training. CESER will also incorporate inclusion and energy justice as a key component in resources developed. These methods, approaches will enable SLTT governments to enhance and exercise their energy assurance plans and regulatory models, incorporating cybersecurity, hardening, and other resilience measures and incentives at the local level.

- **Defense Critical Electric Infrastructure (DCEI) ($2M)**: 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 Defense Critical Infrastructure. The DCEI program's objective is to strengthen energy infrastructure systems for national security purposes. In FY 2023, CESER will continue to implement DOE's DCEI strategic plan by applying successful methods validated in FY 2021 to a larger group of critical defense facilities, increasing national defense and security readiness against power supply interruptions.

Training and Exercises ($9M)

Exercises are critical to planning and evaluating a coordinated response to emergencies. CESER prepares for all hazards that could affect energy delivery alongside federal, state, and local government entities, partners from the oil and natural gas and the electricity subsectors, and representatives from other critical infrastructure sectors. By conducting senior-level policy discussions and operationally focused tactical preparedness exercises, CESER is preparing the nation to effectively mitigate any threat to reliable energy. After each exercise, CESER undergoes improvement planning based on a thorough after-action review of the actions or discussions from the exercise. The lessons learned from the improvement planning are integrated into CESER's emergency response plans and procedures as well as into future exercises for training and validation. Exercise results are shared with participants through after-action reports, providing participants with ways in

which they can augment their own preparedness plans. These recommendations often include ways in which participants can better utilize mutual assistance networks and government resources, should an incident affect the energy infrastructure.

- **Cyber Exercises, Training, and Cyber Workforce Development ($7M):** In support of CESER's energy disruption and emergency response efforts from a cyber incident, this program will conduct cyber exercises with interagency stakeholders, SLTT partners, and industry through leading events such as Liberty Eclipse, as well as by providing technical training such as CyberStrike. CESER will expand other training opportunities to offer middle and senior-level OT security managers in the U.S. energy sector an opportunity to more fully understand the cyber strategies and tactics that adversaries use in targeting U.S. energy infrastructure. CESER will design training, exercises and experimentation focused on cyber grid incident recognition, cyber mitigation and electric restoration, and resilience, leveraging a testbed of power and industrial control system assets in conjunction with the energy sector asset owners and the National Labs. CESER will also continue to expand the CyberForce Competition to include at least three events throughout the year and enhance the ability for CyberForce participants to network and look at potential internship and job opportunities. The CyberForce Competition works with U.S. universities, colleges, and technical schools across the country to advance cybersecurity in the OT/industrial controls systems environment to train the next generation of energy sector cybersecurity experts in the U.S. The program includes an annual cyber defense competition and "Conquer the Hill" skill-based cybersecurity competitions.

- **Non-cyber Exercises and Training ($2M)**: In support of the response to natural disasters and other non-cyber physical incidents, CESER will host exercises with interagency stakeholders, SLTT partners and industry that focus on the impacts to energy infrastructure from terrorism, hurricanes, wildfires, earthquakes, etc. 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 work together in response to catastrophic incidents. 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 from a diverse array of challenging exercise scenarios, allowing them to build upon and validate improvements made in response to lessons learned from previous exercises and real-world incidents. CESER strives to ensure that each iteration of Clear Path presents an increasingly realistic and challenging experience for all participants. The continued success of Clear Path is predicated on the resolute support and involvement from federal, state, and local municipality government partners, cross-sector entities, and private sector organizations. To date, CESER has engaged over 1200 energy sector and cross-infrastructure sector partners.

Information Sharing, Partnerships and Exercises
Funding ($K)

	FY 2021 Enacted	FY 2022 Annualized CR	FY 2023 Request	FY 2023 Request vs FY 2021 Enacted ($)	FY 2023 Request vs FY 2021 Enacted (%)
Information Sharing, Partnerships and Exercises					
Planning, Preparedness, and Resilience	7,322	0	19,000	+11,678	+159.0%
Training and Exercises	4,080	0	9,000	+4,920	+120.6%
Total, Information Sharing, Partnerships and Exercises	**11,402**	**0**	**28,000**	**+16,598**	**+145.6%**

SBIR/STTR:
FY 2021 Enacted: SBIR/STTR: $0
FY 2023 Request: SBIR/STTR: $0

Information Sharing, Partnerships and Exercises
Explanation of Major Changes ($K)

	FY 2023 Request vs FY 2021 Enacted
• Planning, Preparedness, and Resilience - 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.	+19,000
• Training and Exercises - Conduct internal and external exercises with the interagency, SLTT governments, and industry on cyber and natural hazards, provide cybersecurity training for operational technology and industrial control systems, and expand the scope of the CyberForce Competition.	+9,000
Total, Information Sharing, Partnerships and Exercises	**+28,000**

Activities and Explanation of Changes

FY 2021 Enacted	FY 2023 Request	Explanation of Changes FY 2023 Request vs FY 2021 Enacted
Information Sharing, Partnerships and Exercises **$11,402,000**	**$28,000,000**	**+$16,598,000**
Planning, Preparedness, and Resilience $7,322,000	*$19,000,000*	*+$11,678,000*
• Develop grid resilience tools and analyses to help State electricity officials promote prudent, strategic decision-making • Provide technical assistance to Federal, SLTT and regional entities to address key challenges in the energy system • Continue to implement regulatory responsibilities and evaluate regulatory reform to reduce federal burden • Support for technical assistance work to provide stakeholders an in-depth understanding of the resilience of the electric grid and related infrastructure • Provide institutional support to potential critical electric infrastructure investments that address the vulnerabilities of the North American energy system	• 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 FY22 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 inclusion and energy justice in methods, approaches and tools that will enable SLTT governments to enhance and exercise energy assurance plans and regulatory models, incorporating cybersecurity, hardening, and other resilience measures and incentives • Expand CyberForce competition and scale CyberStrike workshops through virtual and in person opportunities. Support the President's Cup Cybersecurity Competition. Expand cyber exercises and training by enhancing and leveraging existing testbed environments which can provide realistic simulation capabilities, allowing for advanced training and efficiencies
Training and Exercises $4,080,000	*$9,000,000*	*+$4,920,000*

FY 2021 Enacted	FY 2023 Request	Explanation of Changes FY 2023 Request vs FY 2021 Enacted
• Exercises, Competitions and Workshops: Conduct Clear Path and Liberty Eclipse exercises with a focus on the connection between emergency response of a cyber nature and consequence management ▪ Continue to host the CyberForce energy sector cyber defense and "Conquer the Hill" competitions and CyberStrike workshops ▪ Support the President's Cup Cybersecurity Competition	• Training and Exercises: Conduct internal and external exercises with the interagency, SLTT governments, and industry on cyber and natural hazards, provide cybersecurity training for operational technology and industrial control systems, and expand the scope of the CyberForce Competition	Through exercise efforts such as Clear Path and Liberty Eclipse, examine improvement items from past preparedness events and real world responses. Continue leveraging simulated cyber environments (at National Labs) to enhance SESER and industry partner's collective response capabilities to cyber-attack scenarios. Develop cyber training opportunities for energy sector partners to increase awareness on current activities, techniques, and procedures. Expands the CyberForce Competition to include a multi-day event, mini competitions, virtual career fair, and lead-up activities in support of energy sector workforce development.

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.

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, cyber, 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. Increased need is seen in the area of cyber preparedness and incident response. CESER is working closely with the Office of the Chief Information Officer, the Office of the Chief Human Capital officer (OCHO) and other program offices across DOE to provide cyber pay incentives, similar to those already implemented at the Cybersecurity and Infrastructure Security Agency (CISA) to retain and recruit highly-skilled cyber talent at the Department. The cybersecurity field is in high demand across both public and private sectors. The Federal government salary in this filed 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 in coordination with the OCHO has developed a detailed staffing plan to identify staffing requirements across the organization. CESER's staffing efforts will continue to focus on building core capabilities of partnerships with industry as the energy sector SRMA, capability building in the energy sector, risk analysis of cyber, 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 equipment purchases, upgrades, and replacements, office furniture, commercial credit card purchases using simplified acquisition procedures when possible, and miscellaneous expenditures.

Highlights of the FY 2023 Budget Request

This budget request provides additional FTEs for support mission critical work.

Program Direction
Funding ($K)

	FY 2021 Enacted	FY 2022 Annualized CR	FY 2023 Request	FY 2023 Request vs FY 2021 Enacted ($)	FY 2023 Request vs FY 2021 Enacted (%)
Program Direction Summary					
Washington Headquarters					
Salaries and Benefits	6,459	6,459	15,195	+8,736	+135.3%
Travel	347	347	295	-52	-15.0%
Support Services	1,430	1,430	4,211	+2781	+194.5%
Other Related Expenses	876	876	1,763	+887	+101.3%
Total, Washington Headquarters	9,112	9,112	21,464	+12,352	+135.6%
National Energy Technology Laboratory					
Salaries and Benefits	1,282	1,282	1,754	+472	+36.8%
Travel	120	120	116	-4	-3.3%
Support Services	438	438	333	-105	-24.0%
Other Related Expenses	1,048	1,048	1,456	+408	+38.9%
Total, National Energy Technology Laboratory	2,888	2,888	3,659	771	+26.7%
Total Program Direction					
Salaries and Benefits	7,741	7,741	16,949	+9,208	+119.0%
Travel	467	467	411	-56	-12.0%
Support Services	1,868	1,868	4,544	+2,676	+143.3%
Other Related Expenses	1,924	1,924	3,219	+1,295	+67.3%
Total, Program Direction	12,000	12,000	25,123	+13,123	+109.4%
Federal FTEs	21	44	93	+72	+342.9%
Additional FE FTEs at NETL supporting CESER[a]	9	9	11	+2	+22.2%
Total CESER-funded FTEs	**30**	**53**	**104**	**+74**	**+246.7%**

[a] CESER funds FTEs at FE's National Energy Technology Laboratory who support CESER activities. These 10.4 FTEs are in FE's FTE totals and are not included in the CESER FTE totals shown on the "Federal FTEs" line.

	FY 2021 Enacted	FY 2022 Annualized CR	FY 2023 Request	FY 2023 Request vs FY 2021 Enacted ($)	FY 2023 Request vs FY 2021 Enacted (%)
Support Services and Other Related Expenses					
Support Services					
Technical Support	1,180	1,180	3,906	+2,726	+231.0%
Management Support	688	688	638	-50	-7.3%
Total, Support Services	1,868	1,868	4,544	+2,676	+143.3%
Other Related Expenses					
Other Services	701	701	1,580	+879	+125.4%
EITS Desktop Services	223	223	639	+416	+186.5%
WCF	1,000	1,000	1,000	0	0.0%
Total, Other Related Expenses	1,924	1,924	3,219	+1,295	+67.3%

Program Direction

Activities and Explanation of Changes

FY 2021 Enacted (Comparable)	FY 2023 Request	Explanation of Changes FY 2023 Request vs FY 2021 Enacted
Program Direction $12,000,000	**$25,122,000**	**+$13,123,000**
Salaries and Benefits $7,741,000	*$16,949,000*	*+$9,208,000*
• Salaries and benefits for executive management, programmatic oversight, and analysis for the effective implementation of the CESER program	• Salaries and benefits for executive management, programmatic oversight, and analysis for the effective implementation of the CESER program	• The increase is due to requesting additional FTEs
Travel $467,000	*$411,000*	*-$56,000*
• Travel includes transportation, subsistence, and incidental expenses that allow CESER to effectively facilitate its mission	• Travel includes transportation, subsistence, and incidental expenses that allow CESER to effectively facilitate its mission	• The decrease is due to an increased use of virtual meeting options and virtual training

FY 2021 Enacted (Comparable)	FY 2023 Request	Explanation of Changes FY 2023 Request vs FY 2021 Enacted
Support Services $1,868,000	*$4,544,000*	*+$2,676,000*
• Support Services includes contractor support directed by the federal staff to provide analysis to management	• Support Services includes contractor support directed by the federal staff to provide analysis to management	• The increase is due to an increase in contractual costs
Other Related Expenses $1,924,000	*$3,219,000*	*+$1,295,000*
Other Related Expenses includes equipment upgrades and replacements, office furniture, minor construction, commercial credit card purchases using simplified acquisition procedures when possible, and miscellaneous expenditures	• Includes equipment upgrades and replacements, office furniture, minor construction, commercial credit card purchases using simplified acquisition procedures when possible, and miscellaneous expenditures	• The increase is for additional support for staff, including increased telework and transition from desktop computers to laptops and mobile devices

Cybersecurity, Energy Security, and Emergency Response

Research and Development ($K)[ab]

	FY 2021 Enacted	FY 2022 Annualized CR	FY 2023 Request	FY 2023 Request vs FY 2021 Enacted ($)	FY 2023 Request vs FY 2021 Enacted (%)
Basic	5,139	5,139	0	-$5,139	-100.0%
Applied	48,120	48,120	105,000	+$56,880	+118.2%
Development	11,664	11,664	20,000	+$8,336	+71.5%
Total, R&D	64,923	64,923	125,000	+$60,077	+92.5%

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

	FY 2021 Enacted	FY 2022 Annualized CR	FY 2023 Request	FY 2023 Request vs FY 2021 Enacted ($)	FY 2023 Request vs FY 2021 Enacted (%)
Risk Management Tools	1,077	1,077	912	-165	-15.3%

[a] Development reporting includes a proportional share of program direction funding in addition to direct Development funding.

[b] The Basic and Applied R&D conducted by CESER in FY 2021 will be performed by the Office of Electricity in FY 2023.