OFFICE OF INSPECTOR GENERAL

CISA and FEMA Can Improve Coordination Efforts to Ensure Energy Sector Resilience

Homeland Security

September 2, 2022

OIG-22-63

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

September 2, 2022

MEMORANDUM FOR: The Honorable Deanne Criswell
Administrator
Federal Emergency Management Agency

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V CUFFARI Digitally signed by JOSEPH V CUFFARI Date: 2022.09.01 09:46:14 -04'00'

SUBJECT: *CISA and FEMA Can Improve Coordination Efforts to Ensure Energy Sector Resilience*

For your action is our final report, *CISA and FEMA Can Improve Coordination Efforts to Ensure Energy Sector Resilience*. We incorporated the formal comments provided by your office.

The report contains three recommendations aimed at improving coordination efforts to ensure Energy Sector resilience. Your offices concurred with all three recommendations. Based on information provided in your response to the draft report, we consider recommendations 1 and 3 open and resolved. We consider recommendation 2 open and unresolved until you provide additional information on efforts to update national guidance documents that contain conflicting terminology. As prescribed by the Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for the Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts. Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act of 1978, as amended,* we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Bruce B. Miller, Deputy Inspector General for Audits, at (202) 981-6000.

Attachment

DHS OIG HIGHLIGHTS

CISA and FEMA Can Improve Coordination Efforts to Ensure Energy Sector Resilience

September 2, 2022

Why We Did This Audit

The Energy Sector is critical for providing uninterrupted energy and services, such as oil, gas, and electricity. However, multiple disasters in recent years, including the 2021 winter storms in Texas, have exposed challenges and concerns the Energy Sector faces in preventing and responding to incidents. We conducted this audit to determine to what extent CISA's and FEMA's coordination efforts identify, monitor, and address Energy Sector concerns.

What We Recommend

We made three recommendations to improve CISA's and FEMA's coordination efforts to ensure Energy Sector resilience.

For Further Information:
Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

What We Found

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Emergency Management Agency (FEMA) can improve the effectiveness of their coordination efforts before, during, and after power outages. Specifically, they could improve their effectiveness by implementing the U.S. Government Accountability Office's leading practices and other key mechanisms for collaboration, such as:

- ensuring Energy Sector efforts are mutually reinforcing;
- establishing compatible Energy Sector policies, procedures, and other means to operate across agency boundaries; and
- updating and monitoring written Energy Sector agreements regularly.

CISA and FEMA have not focused on these areas because they have been working on other priorities for their respective missions. Nonetheless, it is imperative that CISA and FEMA coordinate efficiently and effectively to reduce the likelihood of power outages and, in the case of an incident, to restore and stabilize infrastructure-related services in affected areas.

Agencies' Response

The Department of Homeland Security concurred with all three of our recommendations. We included a copy of management comments in Appendix A.

Background

The Energy Sector is a critical infrastructure sector relied upon by all other sectors. It is one of 16 critical infrastructure sectors outlined in *Presidential Policy Directive-21* (PPD-21), which also designates a lead agency, or Sector Risk Management Agency, for each sector. The U.S. Department of Energy (DOE) is the lead agency for the Energy Sector and its two subsectors: 1) Electricity and 2) Oil and Natural Gas.

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Emergency Management Agency (FEMA) support DOE and other stakeholders before, during, and after incidents[1] involving power outages. CISA identifies and prioritizes critical infrastructure, provides technical assistance to critical infrastructure partners, conducts risk assessments of all 16 sectors, and coordinates the Federal response to security-related incidents. FEMA manages and oversees disaster response efforts and provides technical assistance and grant funding opportunities to improve preparedness, response, recovery, and mitigation efforts. CISA's and FEMA's efforts support the Department of Homeland Security's National Preparedness Goal to coordinate "the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk."[2] Figure 1 shows power crews staging equipment as they work to repair damaged power lines and restore electricity after a 2020 hurricane in Florida.

Figure 1. Crews respond to power outages in Florida in September 2020.
Source: FEMA.gov

[1] An "incident" is defined as any occurrence that necessitates a response to protect life or property, such as emergencies or disasters of all kinds and sizes. *National Response Framework,* p. 4.
[2] The *National Preparedness Goal, Second Edition* (September 2015).

Since 2013, the Federal Government has issued several guidance documents to outline its role in ensuring a secure and reliable Energy Sector. In 2013, a national policy, PPD-21, was established to strengthen the security and resilience of critical infrastructure. In conjunction with PPD-21, the *National Infrastructure Protection Plan 2013* (National Plan) and the *Energy Sector-Specific Plan* were issued to identify, prioritize, and provide technical assistance to the Federal agencies and stakeholders involved in critical infrastructure, including the Energy Sector and the Electricity Subsector. Meanwhile, the *National Response Framework* (NRF) and other Federal guidance provide additional roles and responsibilities for the response to and recovery from a power outage. Appendix B provides a more comprehensive list and description of the applicable Federal guidance.

In recent years, several incidents have highlighted the need for a resilient Energy Sector. For example, Hurricanes Irma and Maria in 2017 left the Commonwealth of Puerto Rico with power outages throughout the island, some of which lasted nearly a year. The Commonwealth and the Puerto Rico Electric Power Authority have received more than $12 billion related to the island's power grid. Additionally, powerlines that touched a tree triggered some of California's recent catastrophic wildfires, which caused millions of dollars in damage. Lastly, in February 2021, Texas experienced widespread power grid failures because frigid temperatures increased demand while straining the State's ability to produce electricity. These various incidents demonstrate some of the challenges the Energy Sector faces. Figures 2 and 3 show crews responding to recent disasters that impacted the Energy Sector.

Figures 2 and 3. Utility workers secure powerlines during 2018 wildfires in California (left). *Source*: DHS.gov (last accessed on May 4, 2022)
FEMA Urban Search and Rescue teams find a cut-off neighborhood after Hurricane Maria (right). *Source*: FEMA.gov (last accessed on May 4, 2022)

We conducted this review to determine to what extent CISA's and FEMA's coordination efforts identify, monitor, and address Energy Sector concerns. This audit focused on the Electricity subsector.

Results of Audit

CISA acts as the nationwide coordinator and facilitator of information related to critical infrastructure security and resilience. Meanwhile, FEMA acts as the nationwide coordinator of Federal disaster response and recovery. These two roles run parallel within the Energy Sector and during Federal disaster response operations. However, CISA and FEMA have not developed a comprehensive strategy to coordinate and prioritize their Energy Sector activities. CISA and FEMA can improve the effectiveness of their coordination efforts before, during, and after power outages by implementing the U.S. Government Accountability Office's (GAO) leading practices and other key mechanisms for collaboration, such as:

- ensuring Energy Sector efforts are mutually reinforcing;
- establishing compatible Energy Sector policies, procedures, and other means to operate across agency boundaries; and
- updating and monitoring written Energy Sector agreements regularly.

CISA and FEMA have not focused on these areas because they have been working on other priorities for their respective missions. Nonetheless, it is imperative that CISA and FEMA coordinate efficiently and effectively to reduce the likelihood of power outages, and in the case of an incident, to restore and stabilize infrastructure-related services in affected areas.

FEMA and CISA Could Implement Leading Practices and Other Key Mechanisms for Collaboration

Broadly defined, collaboration is any joint activity intended to produce more public value than could be produced when organizations act alone. In its 2005 report, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies* (GAO-06-15), the GAO identified eight leading practices that can help foster agency collaboration to effectively achieve national outcomes,[3] such as DHS' National Preparedness Goal. Leading or "best" practices are essential to make Government activities more efficient. In particular, three of GAO's leading practices could help CISA and FEMA better achieve their Energy Sector goals:

[3] *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies* (GAO-06-15), October 2005, https://www.gao.gov/assets/gao-06-15.pdf.

- Establish Mutually Reinforcing or Joint Strategies. Collaborating[4] agencies need to establish strategies that will help align activities and accomplish a common outcome.

- Establish Compatible Policies, Procedures, and Other Means to Operate across Agency Boundaries. Agencies need to ensure standards, policies, procedures, and data systems that will be used in the collaborative effort are compatible. When agencies work together, they can define and agree on their respective roles and responsibilities and common terminology. Frequent communication can improve agencies' collaboration and prevent misunderstandings.

- Define and Articulate the Common Outcome. Agencies can strengthen their commitment to work collaboratively by articulating their agreements in formal documents, such as memorandums of understanding (MOU). These written agreements are most effective when they are regularly updated and monitored.

GAO further expanded its effort by identifying mechanisms the Federal Government can use to lead and implement interagency collaboration.[5] GAO's report, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms* (GAO-12-1022), identified key considerations for implementing these mechanisms. Appendix C provides a complete summary of GAO's identified leading practices and mechanisms to consider when collaborating across entities.

FEMA and CISA Could Ensure Program Efforts Are Mutually Reinforcing

Individually, CISA and FEMA perform several activities that support the Energy Sector. However, they have not established a comprehensive and collaborative process to share information and coordinate with each other, DHS components, or Federal stakeholders. We identified several areas — the Regional Resiliency Assessment Program (RRAP), the Threat and Hazard Identification and Risk Assessment (THIRA), and mitigation grants — in which CISA and FEMA could enhance coordination to mutually reinforce Energy Sector activities.

[4] GAO-06-15 uses the term "collaboration" broadly to include interagency activities that others have variously defined as "cooperation," "coordination," "integration," or "networking."
[5] *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms* (GAO-12-1022), September 2012, https://www.gao.gov/assets/gao-12-1022.pdf.

CISA Could Include Key Partners in Its Regional Resiliency Assessment Program

CISA's RRAP is a voluntary, cooperative assessment of specific critical infrastructure; each assessment identifies a range of issues that could have regionally or nationally significant consequences. Specifically, RRAP resolves security and resilience knowledge gaps, informs risk management decisions, identifies opportunities and strategies to enhance resilience, and improves critical partnerships among the public and private sectors. CISA conducts RRAP assessments to identify challenges and funding opportunities to improve stakeholders' resilience, including Energy Sector stakeholders.

Energy Sector stakeholders could use the information from RRAP assessments to help guide investments, planning, and training, and to enhance Energy Sector resilience. However, CISA generally does not collaborate with DOE on these assessments, despite the assessments' potential to help DOE fulfill its lead agency responsibilities. According to CISA, it has invited DOE to participate in its RRAPs. However, DOE participated in only two of the five Energy Sector RRAPs we reviewed from the past 5 years. DOE officials said CISA's invitations have been inconsistent; as a result, DOE has not always participated.

Additionally, FEMA officials said RRAP assessments could help communities identify infrastructure that would benefit from its grant programs. FEMA and CISA have discussed partnering in RRAP efforts and in FEMA's Building Resilient Infrastructure in Communities grant program, but officials acknowledged they have not begun collaborating. Such a partnership would benefit both components and their stakeholders.

FEMA Could Consistently Share Threat and Hazard Identification and Risk Assessment Results with CISA

FEMA's National Risk and Capability Assessment is a suite of assessment products that include the National THIRA and the Community THIRA. These products measure risks, capabilities, and gaps using a standardized and coordinated process. The National THIRA assesses the most catastrophic threats and hazards to the Nation and establishes capability targets to manage those risks. The Community THIRA is a three-step risk assessment that helps communities understand and address risks.

According to FEMA officials, it can share THIRA results with Federal offices, including CISA, but it can only do so if there is a clear disaster or emergency

preparedness mission and a valid "need to know."[6] CISA has not obtained "need to know" status or requested the THIRA results. Additionally, FEMA officials confirmed that there is not a standardized process for regularly updating the list of which Federal offices need to know specific information or for ensuring that the information reaches the appropriate entities. As a result, FEMA does not consistently share THIRA results with CISA. CISA's input on the THIRA process and its subsequent review of results could help both components and their stakeholders identify risks.

FEMA Could Consistently Coordinate with CISA on Mitigation Grants

Hazard mitigation is any sustainable action that reduces or eliminates long-term risk to people and property from future disasters. FEMA provides various types of hazard mitigation funding, including the Public Assistance (PA) program's Section 406 hazard mitigation grants. This type of grant funding allows recipients to incorporate hazard mitigation when they repair and replace damaged facilities beyond their pre-disaster design. These improvements are considered part of the total eligible cost to repair, restore, or reconstruct facilities, including Energy Sector-related projects.

According to FEMA officials, CISA and some officials within FEMA's PA Division have discussed coordinating their hazard mitigation efforts but have not partnered on any Energy Sector-specific projects. FEMA has not developed a process for consistently requesting relevant data from CISA. This data could help FEMA better understand grant funding needs for communities affected by disasters. The DHS Office of Inspector General identified similar challenges in coordination between CISA and FEMA as part of our audit of the Dams Sector.[7]

FEMA and CISA Did Not Establish Compatible Policies, Procedures, and Other Means to Operate across Component Boundaries

FEMA and CISA have not ensured governing documents related to the Energy Sector and disaster response and recovery from power outages are accurate and updated. During our audit, we identified several policies and procedures that were outdated and contained conflicting terminology. This inaccuracy and inconsistency may limit the overall effectiveness of Federal efforts to ensure Energy Sector resilience.

[6] THIRA data includes jurisdiction-specific preparedness data that is considered "for official use only." The data cannot be distributed outside the Federal Government and is intended for recipients that have a clear disaster/emergency preparedness mission and a valid need to know.

[7] OIG-21-59, *CISA Can Improve Efforts to Ensure Dam Security and Resilience* (September 9, 2021), https://www.oig.dhs.gov/sites/default/files/assets/2021-09/OIG-21-59-Sep21.pdf.

The governing policies and procedures that guide the Federal Government's response to and recovery from incidents causing power disruption must be regularly updated. However, the Emergency Support Function-12 (ESF-12) Annex, the Response Federal Incident Operation Plan (FIOP), and the Recovery FIOP have not been updated since 2016, and the Power Outage Incident Annex (POIA) has not been updated since 2017. These documents still refer to the National Protection and Programs Directorate (NPPD), which was redesignated as CISA in 2018. Moreover, these do not reflect the significant change regarding CISA's current roles and responsibilities.

For example, the POIA requires NPPD's Infrastructure Protection Division to activate a Critical Infrastructure Crisis Action Team to provide incident support for situational awareness and planning when incidents have significant impacts on critical infrastructure. However, neither the Infrastructure Protection Division nor the Crisis Action Team are part of CISA's current structure. According to CISA, it still fulfills the required activities for incident support. Yet, if stakeholders relied on the POIA during significant power outage incidents, they would not receive clear guidance identifying current procedures and responsible agencies and divisions; this could lead to a delayed response.

Additionally, CISA's and FEMA's key guidance use different terminology to describe the same Energy Sector functions.[8] For example:

- CISA: CISA's National Plan lists four "lifeline functions:" Communications, Energy, Transportation, and Water. These lifeline functions are essential to the operation of most critical infrastructure sectors. If these lifeline functions were compromised or not properly restored, human health and safety would be at risk and the Nation could face serious economic consequences.

- FEMA: FEMA's 2019 NRF included a "community lifelines" concept in its disaster response framework. The NRF describes these essential community lifelines as those services that enable the continuous operation of critical government and business functions and are essential to human health and safety or economic security. Four of the seven community lifelines (Food/Water/Shelter, Energy, Communications, and Transportation) have near-identical definitions to the four lifeline functions listed in the National Plan. However, the terms are not interchangeable, and these strategic documents do not explain the similarities or differences in terminology. If stakeholders use these terms

[8] CISA and FEMA are responsible for updating the National Plan and the NRF, respectively. However, both documents are published by DHS.

when discussing the Energy Sector and emergency response efforts, it could lead to confusion.

CISA Did Not Regularly Update and Monitor Written Agreements

In February 2020, the U.S. Department of Defense, DOE, and DHS signed an MOU to partner on a new Energy Sector Pathfinder Initiative. This initiative was designed to promote information sharing and interagency collaboration, improve training and education about systemic risks, and develop joint operational preparedness and response activities to prevent and respond to cybersecurity threats. The initiative was scoped to address the technologies, challenges, and threats specifically facing the Energy Sector and was adapted to the regulatory environment, sector maturity, and existing sector relationships. For instance, the MOU details how DOE, DHS, and the U.S. Department of Defense should work with CISA to establish and maintain a reference library of past exercises and lessons learned to improve public and private response and resiliency activities.

The Pathfinder MOU included an initial coordination plan and outlined the roles, responsibilities, and desired outcomes. However, according to a CISA official, stakeholders have not met consistently since the MOU was formalized due to competing priorities at the agencies, and the initiative has not produced any significant results in more than 2 years.

Conclusion

The Energy Sector is a critical infrastructure sector relied upon by all other sectors. With increasing natural disasters and widespread power outages that follow, it is vital that CISA and FEMA effectively and efficiently coordinate with each other and with Energy Sector stakeholders to reduce the likelihood of power outages, restore electricity, and stabilize infrastructure-related services after an incident.

CISA and FEMA did not fully ensure their efforts were mutually reinforcing because they do not have the necessary processes and agreements to share information and coordinate activities. CISA did create an Energy Sector liaison position to monitor, coordinate, and report on its numerous ongoing efforts and responsibilities. However, CISA has not had a dedicated liaison for this role since December 2021. Additionally, according to CISA and FEMA officials, the components have not focused on improving collaboration because they have been working on other priorities for their respective missions. For instance, CISA cited other pressing COVID-19 and election-related priorities as reasons for why it has not monitored and made more progress on the Pathfinder Initiative. Similarly, FEMA noted that updating documents to show the

changes in DHS and CISA structure had not been a priority due to the COVID-19 pandemic and numerous other large-scale disasters. FEMA officials also said that plans are not updated in real time, but rather during the next scheduled revision.

Both CISA and FEMA could improve the outcomes of their efforts by increasing their coordination. Using GAO's leading practices, they could improve coordination, potentially improve agency outcomes, and achieve sector goals. Additionally, CISA and FEMA would benefit from preparing a comprehensive and adaptive framework for their Energy Sector activities and ensuring their goals are aligned with those set by DOE. Without such a plan, DHS risks losing important data that would strengthen Energy Sector relationships, programs, and outcomes.

Recommendations

Recommendation 1: We recommend the CISA Director and FEMA Administrator develop and document a comprehensive and adaptive framework ensuring collaboration between DHS components in support of Energy Sector activities, including procedures to:

a. periodically monitor and update DHS Energy Sector activities to ensure progress toward achieving common goals and outcomes, such as those in the *National Preparedness Goal* and the *Energy Sector-Specific Plan*; and
b. identify relevant participants and eliminate challenges to data sharing (e.g., developing a method for regularly updating the list of Federal offices with a "need to know" status and sharing risk assessment information with each other, DHS components, and key stakeholders, as permitted by law).

Recommendation 2: We recommend the CISA Director and FEMA Administrator each review and update key guidance in support of Energy Sector and disaster response activities to ensure it is current, relevant, and consistent. Additionally, we recommend CISA and FEMA work with the Sector Risk Management Agency to ensure DHS Energy Sector policies, procedures, and guidance are compatible and do not contain conflicting terminology.

Recommendation 3: We recommend the CISA Executive Assistant Director for Cybersecurity coordinate with the Department of Energy and the Department of Defense to review and update the Pathfinder Initiative memorandum of understanding, as needed, to ensure Pathfinder Initiative information is shared and interagency collaboration outcomes are met.

Management Comments and OIG Analysis

The Department provided written comments in response to a draft of this report. It expressed appreciation for the OIG's work planning and conducting our audit and issuing this report. We included a copy of DHS management's response in its entirety in Appendix A. CISA and FEMA also provided technical comments and suggested revisions to our report in a separate document. We reviewed the technical comments and made changes to the report when appropriate.

The Department concurred with all three of our recommendations. The following is a summary of the Department's response to our recommendations and OIG's analysis.

DHS Response to Recommendation 1: Concur. CISA's Stakeholder Engagement Division will formally document the Energy Sector Liaison's roles and responsibilities and associated Sector Risk Management Agency coordination mechanisms. The Energy Sector Liaison will work with DOE (the Sector Risk Management Agency) to identify relevant partners with a "need to know" for sharing risk information. The process will also specify coordination between the Energy Sector Liaison and FEMA's National Preparedness Directorate to ensure FEMA's input is coordinated. Estimated Completion Date: March 31, 2023

OIG Analysis of DHS Comments: CISA's and FEMA's actions are responsive to the recommendation. We consider the recommendation resolved and open. It will remain open until CISA and FEMA provide documentation showing all planned corrective actions have been implemented.

DHS Response to Recommendation 2: Concur. FEMA is updating the Response and Recovery Federal Interagency Operational Plans and will replace references to NPPD with references to CISA; these updates are undergoing final concurrence reviews. Additionally, FEMA and CISA are nearing completion of the ESF-14 Joint Plan, which will expand on concepts provided in the ESF-14 Annex to the NRF and clarify cross-sector coordination procedures across supporting agencies. Estimated Completion Date: December 30, 2022

OIG Analysis of DHS Comments: CISA's and FEMA's actions are partially responsive to the recommendation. We consider the recommendation unresolved and open. It will remain unresolved until FEMA and CISA provide additional information on actions they will take to ensure policies and procedures are consistent and to deconflict strategic concepts such as lifeline functions and community lifelines. The recommendation will remain open until FEMA and CISA update all relevant policy and operational documents.

DHS Response to Recommendation 3: Concur. CISA compared the Pathfinder MOU in July 2022 with recent achievements and determined additional updates were not needed. CISA's Cybersecurity Division found the Pathfinder Initiative was achieving intended outcomes in accordance with the objectives stated in the MOU despite the global pandemic. For example, CISA participated in multiple technical exchanges to identify effective ways to conduct cyber threat information sharing and an Interagency Analytics Exercise in 2022. The Department requested the recommendation be closed based on these actions.

OIG Analysis of DHS Comments: CISA's actions are responsive to the recommendation. We consider the recommendation resolved and open. It will remain open until CISA provides documentation showing the review of the MOU, multiple technical exchanges, interagency exercises and trainings, and various cybersecurity efforts described in its response.

Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107–296) by amendment to the *Inspector General Act of 1978*.

We conducted this audit to determine to what extent CISA's and FEMA's coordination efforts identify, monitor, and address Energy Sector concerns, with a focus on the Electricity subsector. The scope included a review of FEMA's and CISA's coordination with critical infrastructure partners before, during, and after disasters that occurred between 2017 and 2021 and involved power outages.

To accomplish our objective, we evaluated CISA's and FEMA's internal controls and obtained, reviewed, and analyzed documentation pertaining to the Energy Sector, including but not limited to: PPD-21, the *CISA Act of 2018*,[9] the National Plan, the Energy Sector-Specific Plan, the NRF, the National Disaster Recovery Framework (NDRF), the POIA, the ESF-12 and ESF-14 Annexes, and the Response and Recovery FIOPs.

We conducted interviews with officials from various divisions within CISA and FEMA to gain an understanding of roles and responsibilities in the Energy Sector, including policies and procedures followed, funding and technical assistance offered, and challenges and successes experienced. We also interviewed officials from DOE and the Federal Energy Regulatory Commission

[9] Public Law No. 115-278, November 16, 2018.

to better understand interactions and services provided by DHS components, including successes and challenges related to coordination efforts.

Additionally, we reviewed leading practices and key considerations identified by GAO. The team also met with GAO to ensure these leading practices and key considerations were being applied in the spirit GAO intended.

We conducted this performance audit between September 2021 and March 2022 pursuant to the *Inspector General Act of 1978*, *as amended*, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The Office of Audits major contributors to this report are Yesi Starinsky, Director; Doug Campbell, Audit Manager; Lauren Bullis, Auditor-in-Charge; Rebecca Hetzler, Auditor; John Schmidt, Program Analyst; Tanya Suggs, Program Analyst; Kirsten Teal, Program Analyst; Maria Romstedt, Communications Analyst; and Edward (Ted) Brann, Independent Reference Reviewer.

Appendix A
Management Comments to the Draft Report

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

August 12, 2022

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

JIM H CRUMPACKER
Digitally signed by JIM H CRUMPACKER
Date: 2022.08.12 09:07:53 -04'00'

SUBJECT: Management Response to Draft Report: "CISA and FEMA Can Improve Coordination Efforts to Ensure Energy Sector Resilience" (Project No. 21-049-AUD-FEMA)

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

DHS leadership is pleased to note OIG's recognition that the Cybersecurity and Infrastructure Security Agency's (CISA) Regional Resiliency Assessment Program (RRAP) resolves security and resilience knowledge gaps, informs risk management decisions, identifies opportunities and strategies to enhance resilience, and improves critical partnerships among the public and private sectors. RRAP also generates greater understanding and action among public and private sector partners to improve the resilience of a region's critical infrastructure and create strong partnerships with federal, state, local, and territorial government officials and private sector organizations across multiple disciplines, which are essential to the RRAP process.

In addition, the OIG noted that the Federal Emergency Management Agency's (FEMA) National Risk and Capability Assessment is a suite of assessment products that include the National Threat and Hazard Identification and Risk Assessment (THIRA), and the Community THIRA, and that these products measure risks, capabilities, and gaps using a standardized and coordinated process which help communities understand and address risks.

As the Sector Risk Management Agency (SRMA) for the Energy Sector, it is also important to note that the Department of Energy (DOE) leads, facilitates, and supports programs and associated activities within the sector, and that CISA and FEMA support

DOE as it carries out its work within the sector to advance critical infrastructure security. Accordingly, CISA and FEMA support DOE and follow SRMA guidance in executing emergency preparedness and information sharing efforts within the Energy Sector. As part of this, CISA and FEMA are committed to providing products and services that enhance our collective understanding of risk and guide national preparedness and resilience efforts, and to coordinate in developing and delivering these products and services, when appropriate.

The draft report contained three recommendations with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual and other issues under a separate cover for OIG's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Enclosure

Enclosure: Management Response to Recommendations Contained in 21-049-AUD-FEMA

OIG recommended the CISA Director and FEMA Administrator:

Recommendation 1: Develop and document a comprehensive and adaptive framework ensuring collaboration between DHS components in support of Energy Sector activities, including procedures to:

a. Periodically monitor and update DHS Energy Sector activities to ensure progress toward achieving common goals and outcomes, such as those in the National Preparedness Goal and the Energy Sector-Specific Plan; and

b. Identify relevant participants and eliminate challenges to data sharing (e.g., developing a method for regularly updating the list of Federal offices with a "need to know" status and sharing risk assessment information with each other, DHS components, and key stakeholders, as permitted by law).

Response: Concur. CISA's Stakeholder Engagement Division (SED) supports all external SRMAs through Sector Liaisons, who serve as coordinators for those critical infrastructure sectors for which CISA is not the SRMA. Through this relationship, CISA works in concert with SRMAs to build capacity, strengthen partnerships, and enhance resilience within, and across, sectors. Specifically, CISA's Sector Liaisons use formal mechanisms such as Sector and Government Coordinating Councils, topic-specific working groups, and SRMA-led project teams, as well as less formal routine communications to collaborate within DHS, and between the DHS and non-CISA SRMAs to ensure appropriate coordination, situational awareness, and communications with the SRMAs and with partners and stakeholders. Accordingly, although DOE develops the meeting cadence of the sector council meetings (typically quarterly) and identifies relevant participants and data sharing challenges as the SRMA for the Energy Sector, CISA's Sector Liaisons also maintain regular contact and engagement with non-CISA SRMAs, including DOE, to conduct regular, ongoing, and *ad hoc* consultation and collaboration in accordance with the 2013 National Infrastructure Protection Plan.[1]

With these roles and responsibilities in mind, CISA's SED will formally document Energy Sector Liaison roles and responsibilities and associated SRMA coordination mechanisms to ensure progress toward achieving common goals and outcomes. SED will also specify the need for the Energy Sector Liaisons to work with DOE, in its capacity as SRMA, to identify relevant partners with a "need to know" for sharing risk information. This formal documentation will specify that CISA's Sector Liaison will coordinate with

[1] https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

FEMA National Preparedness Directorate (NPD) to ensure that FEMA's input is coordinated, as appropriate. FEMA's NPD will collaborate through formal SRMA-led mechanisms and less formal routine communications to provide input, insights, and recommendations to the SRMA regarding achievement of common goals and objectives, and to support SRMA-led efforts to identify Energy Sector data sharing partners and challenges, and to collaboratively address those challenges.

Estimated Completion Date (ECD): March 31, 2023.

Recommendation 2: Review and update key guidance in support of Energy Sector and disaster response activities to ensure it is current, relevant, and consistent. Additionally, we recommend CISA and FEMA work with the Sector Risk Management Agency to ensure DHS Energy Sector policies, procedures, and guidance are compatible and do not contain conflicting terminology.

Response: Concur. Since February 2019, FEMA's Office of Response and Recovery (ORR) has been leading a multi-year planning effort to revise the Response and Recovery Federal Interagency Operational Plans (FIOPs). Updates to the joint Response and Recovery FIOP is undergoing final concurrence and includes changes to replace "National Protection and Plans Directorate" with CISA. In addition, FEMA's ORR currently conducts full updates to its operational plans on a five-year planning cycle, and reviews published plans to determine the need for administrative or interim updates, as appropriate, with out-of-cycle prioritization given to critical corrections rather than administrative updates. Accordingly, as FEMA maintains a wide range of operational plans with equities across the entire Federal government, FEMA typically includes updates to operational plans addressing a rebranding or reorganization within an agency on the scheduled cycle.

CISA's Integrated Operations Division and FEMA's ORR are also nearing completion of the initial Emergency Support Function (ESF) #14, "Cross-Sector Business and Infrastructure, Joint Plan," which should be finished by August 31, 2022. Once complete, the ESF #14 Joint Plan will expand on concepts provided in the ESF #14 Annex to the National Response Framework, thus supporting the activation of ESF #14 at the federal level. While the scope of this plan is limited to procedural guidance for CISA and FEMA personnel who staff the National Response Coordination Center during activation, it will help clarify cross-sector coordination procedures across the supporting agencies.

ECD: December 30, 2022.

OIG recommended that the CISA Executive Assistant Director for Cybersecurity:

Recommendation 3: Coordinate with the Department of Energy and the Department of Defense [DOD] to review and update the Pathfinder Initiative memorandum of understanding, as needed, to ensure Pathfinder Initiative information is shared and interagency collaboration outcomes are met.

Response: Concur. The "Memorandum of Understanding Between the U.S. Department of Energy, the U.S. Department of Homeland Security, and the U.S. Department of Defense for the Energy Sector Pathfinder," which became effective on January 14, 2020, stipulates a yearly review by signatories and sets forth a process for updates. In July 2022, CISA's Cybersecurity Division reviewed the memorandum against the recent achievements of the Pathfinder Initiative, and does not believe that further updates are needed at this time, especially with regard to ensuring information is shared and interagency collaboration outcomes are met. Moreover, CISA's Cybersecurity Division found that the Pathfinder Initiative was achieving intended outcomes in accordance with objectives stated in the MOU. Specifically, although joint progress in implementing the objectives of the MOU was limited in 2020 and 2021 by workforce restrictions brought about by the global COVID-19 pandemic, such as the diversion of personnel and other resources to meet the demand to secure the COVID-19 vaccine supply chain, the signatories to the MOU continued to meet, plan, and make progress in all three of the core objectives outlined in the MOU.

For example, federal Pathfinder partners participated in multiple technical exchanges to identify effective ways to conduct cyber threat information sharing. From November 8, 2021, to January 13, 2022, CISA's Cybersecurity Division participated in a Pathfinder Interagency Analytics Exercise, in which five federal partner Pathfinder agencies participated, including Cyber National Mission Force from the Department of Defense, the Federal Bureau of Investigation, the National Security Agency, CISA, and the Office of Cybersecurity, Energy Security, and Emergency Response from the Department of Energy. Further, nine industry participants that are both Energy Sector entities and participants in the Cybersecurity Risk Information Sharing Program also participated. Ultimately, this Interagency Analytics Exercise enabled federal and industry participants to collaborate and explore the value to be gained from a joint approach to analyzing data for cyber indicators of compromise. Further, CISA's Cybersecurity Division is currently participating in a second iteration of the Pathfinder Interagency Analytics Exercise series, which is taking place from July 26, 2022 to October 25, 2022.

Additional progress has been made in identifying Industrial Control System training from government and industry sources, including CISA. For example, DOD and DOE led the development of a training curriculum document, with input from CISA, that establishes a baseline for education necessary for energy sector-relevant cyber operations. Further, federal Pathfinder participants reviewed, and began editing, a draft joint cyber incident

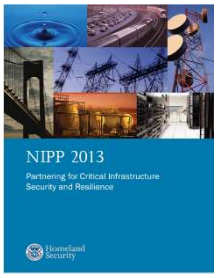
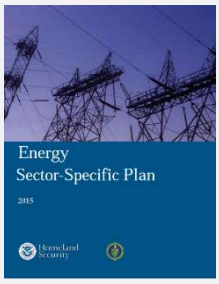
response playbook that was initially generated by a critical private sector partner from within the energy sector. CISA, DOD, and DOE have also collaborated on "joint threat hunt" and "collaborative threat hunt" operations in order to develop policies, procedures, and technologies that facilitate rapid transfer of information between agency teams in the case of a cyber incident. As background, threat hunting is a search for evidence of an attacker in the network, even in the absence of an alert or indicator that an attacker has breached the network. The ability of the government to jointly conduct these operations and/or rapidly share findings from threat hunt operations is critical to promoting a whole-of-nation response to a catastrophic cyber incident in order to reduce operational friction and promote unity of response.

We request that OIG consider this recommendation resolved and closed, as implemented.

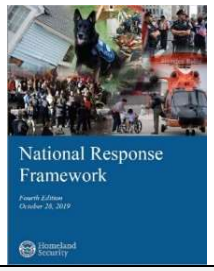
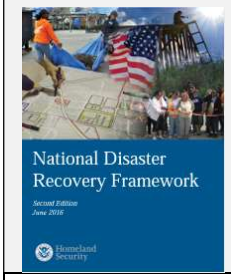
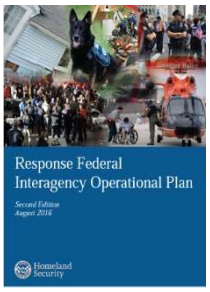
6

Appendix B
Federal Energy Sector Guidance Documents

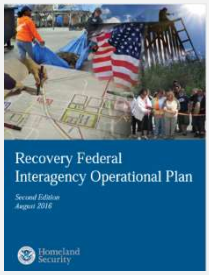
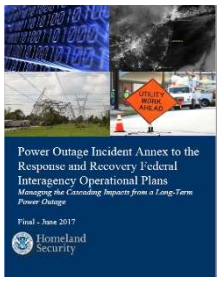
Table 1. Summary of Energy Sector Guidance

Federal Guidance	Purpose
Presidential Policy Directive-21 (PPD-21) (published by the White House in February 2013)	PPD-21 promotes a unified effort to strengthen and maintain secure, functioning, and resilient critical infrastructure by: • establishing a national policy on critical infrastructure security and resilience; • promoting shared responsibility among Federal, state, local, tribal, and territorial (SLTT) entities, including public and private critical infrastructure owners and operators; • clarifying critical infrastructure-related functions, roles, and responsibilities across the Federal Government, and enhancing overall coordination and collaboration; and • identifying uniquely critical energy and communications systems that provide enabling functions across all critical infrastructure sectors.
 *National Infrastructure Protection Plan* (National Plan) (published by DHS in 2013)[10]	The National Plan guides the critical infrastructure community's collaborative efforts to advance security and resilience under three broad categories: • building on partnership efforts; • innovating in managing risk; and • focusing on outcomes.
 *Energy Sector-Specific Plan* (published by DHS and DOE in 2015)	The Energy Sector-Specific Plan guides and integrates the sector's continuous efforts to improve the security and resilience of its critical infrastructure and describes how the Energy Sector contributes to national infrastructure security and resilience goals.

[10] The *CISA Act of 2018* requires CISA to develop a comprehensive national plan for securing the key resources and critical infrastructure. Public Law No. 115-278, November 16, 2018.

Federal Guidance	Purpose
 *National Response Framework* (NRF) (published by DHS in October 2019)[11]	The NRF provides a foundation for the Nation's emergency management efforts and how to respond to all types of incidents.
Emergency Support Function 12 Annex to the NRF (ESF-12 Annex) (published by FEMA in June 2016)	The ESF-12 Annex describes the roles and responsibilities of ESF-12/Energy Sector stakeholders such as SLTT entities, nongovernmental organizations, and the Federal Government. Additionally, it provides core capabilities and agency functions for response to and recovery from a power outage.
Emergency Support Function 14 Annex to the NRF (ESF-14 Annex) (published by FEMA in October 2019)	The ESF-14 Annex provides guidance to align and support cross-sector operations among infrastructure owners and operators, businesses, and government partners to stabilize community lifelines, as well as any impacted National Critical Functions, including those with equity in the Energy Sector.
 *National Disaster Recovery Framework* (NDRF) (published by DHS in June 2016)[12]	The NDRF establishes a common platform and forum for how the whole community (the Federal Government, SLTT governments, the private sector, and individuals) builds, sustains, and coordinates delivery of recovery capabilities. The NDRF emphasizes preparing for recovery before a disaster.
 *Response Federal Incident Operational Plan* (Response FIOP) (published by DHS in August 2016)[13]	The Response FIOP builds on the NRF by describing the concept of operations for integrating and synchronizing existing national-level Federal capabilities to support SLTT and insular area governments. It is a plan that addresses probable threats and hazards while describing the Federal Government's coordination efforts to save lives, protect property and the environment, and meet basic human needs after an emergency or disaster.

[11] DHS delegated updates and maintenance of the NRF to FEMA.
[12] FEMA is responsible for the review and maintenance of the NDRF.
[13] FEMA is responsible for the management and maintenance of the Response FIOP.

Federal Guidance	Purpose
 *Recovery Federal Incident Operational Plan (Recovery FIOP)* (published by DHS in August 2016)[14]	The Recovery FIOP describes how Federal departments and agencies will partner with SLTT and insular governments, nongovernmental organizations, and private sector partners to deliver recovery core capabilities within the range of their authorities, skills, and resources.
 *Power Outage Incident Annex* (POIA) (published by DHS in June 2017)[15]	The POIA offers guidance for providing Federal-level response and recovery assistance to SLTT and insular areas while protecting privacy, civil rights, and civil liberties. It outlines the types of Federal support available to critical infrastructure stakeholders for restoration activities, the responsibilities of industry stakeholders, potential critical information requirements, and unique considerations that could hinder federally provided mission-essential services.

Source: Federal guidance documents

[14] Interagency partners, including FEMA, are responsible for reviewing and maintaining the Recovery FIOP.
[15] FEMA is responsible for managing and maintaining the POIA.

Appendix C
GAO's Leading Practices and Mechanisms for Collaborating Across Entities

Table 2. Leading Practices to Enhance Agency Collaboration

Leading Practice	Description
Define and articulate a common outcome	Collaborative effort requires agency staff working across agency lines to define and articulate the common Federal outcome or purpose they are seeking to achieve that is consistent with their respective agency goals and mission.
Establish mutually reinforcing or joint strategies	Collaborating agencies need to establish strategies that work in concert with those of their partners or are joint in nature. Such strategies help in aligning the partner agencies' activities, core processes, and resources to accomplish the common outcome.
Identify and address needs by leveraging resources	Collaborating agencies can look for opportunities to address resource needs by leveraging resources, thus obtaining additional benefits that would not be available if they were working separately.
Agree on roles and responsibilities	Collaborating agencies should work together to define and agree on their respective roles and responsibilities, including how the collaborative effort will be led.
Establish compatible policies, procedures, and other means to operate across agency boundaries	Agencies need to address the compatibility of standards, policies, procedures, and data systems that will be used in the collaborative effort.
Develop mechanisms to monitor, evaluate, and report on results	Agencies need to create the means to monitor and evaluate their efforts to identify areas for improvement.
Reinforce agency accountability for collaborative efforts through agency plans and reports	A focus on results implies that Federal programs contributing to the same or similar goals should collaborate to ensure the goals are consistent and program efforts are mutually reinforcing.
Reinforce individual accountability for collaborative efforts through performance management systems	Agencies are to hold executives accountable for, among other things, collaboration and teamwork across organization boundaries to help achieve goals by requiring the executives to identify programmatic crosscutting, and partnership-oriented goals through the performance expectations in their individual performance plans.

Source: GAO-06-15

Table 3. Mechanisms to Lead and Implement Interagency Collaboration

Mechanism	Description
Outcomes and Accountability	Agencies may not have the same overall interests or may even have conflicting interests. However, by establishing a goal based on what the group has in common, a collaborative group can shape its own vision and define its own purpose.
Bridging Organizational Cultures	Establish ways to operate across agency boundaries such as developing common terminology, creating compatible policies and procedures, and fostering open lines of communication.
Leadership	Leadership models range from identifying one agency or person to lead to assigning shared leadership over a collaborative mechanism. Additionally, influence of leadership can be strengthened by a direct relationship with high-level officials. Last, transitions and inconsistent leadership can weaken the effectiveness of any collaborative mechanism.
Clarity of Roles and Responsibilities	Clarity can come from agencies working together to define and agree on their respective roles and responsibilities, as well as steps for decision making, and can be codified through laws, policies, MOUs, or other requirements.
Participants	It is important to ensure that the relevant participants have been included in the collaborative effort. These participants should have full knowledge of the relevant resources in their agency; the ability to commit these resources and make decisions on behalf of the agency; the ability to regularly attend all activities of the collaborative mechanism; and the knowledge, skills, and abilities to contribute to the outcomes of the collaborative effort.
Resources	Collaborating agencies should identify the human, information technology, physical, and financial resources needed to initiate or sustain their collaborative effort.
Written Guidance and Agreements	Not all collaborative arrangements need to be documented through written guidance and agreements; however, it can be helpful to document key agreements related to the collaboration. Additionally, written agreements are most effective when they are regularly updated and monitored.

Source: GAO-12-1022

Table 4. Areas Where GAO-06-15 and GAO-12-1022 Align

Leading Practices Identified in GAO-06-15	Mechanisms Identified in GAO-12-1022						
	Outcomes and Accountability	Bridging Organizational Cultures	Leadership	Clarity of Roles and Responsibilities	Participants	Resources	Written Guidance and Agreements
Define and articulate a common outcome.	X	–	–	X	–	–	X
Establish mutually reinforcing or joint strategies.	–	–	–	X	–	–	X
Identify and address needs by leveraging resources.	–	–	–	–	–	X	X
Agree on roles and responsibilities.	–	–	–	X	–	–	X
Establish compatible policies, procedures, and other means to operate across agency boundaries.	–	X	–	–	–	X	X
Develop mechanisms to monitor, evaluate, and report on results.	X	–	–	–	–	–	X
Reinforce agency accountability for collaborative efforts through agency plans and reports.	X	–	–	–	–	–	X
Reinforce individual accountability through performance management systems.	X	–	–	–	–	–	X

X = Practices and mechanisms align.
– = No data.
Source: Table created by DHS OIG based on GAO analysis within GAO-12-1022

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
CISA Component Liaison
FEMA Component Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.

OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305