Strengthening the Resilience of Defense Critical Electric Infrastructure

Recommendations for the
U.S. Department of Energy

March 2022

EAC
ELECTRICITY ADVISORY COMMITTEE

Introduction

The U.S. Department of Energy (DOE) has significant opportunities to improve collaboration with the electric industry to bolster the resilience of the Defense Critical Electric Infrastructure (DCEI) that serves Critical Defense Facilities (CDFs).[1] Based on insights provided by responsible utilities (RUs) that own or operate DCEI,[2] this report offers specific proposals for progress. Some proposals can be implemented by DOE under its own authorities. Yet, given the inherently public-private and intergovernmental nature of many DCEI challenges, other recommendations would require DOE to partner with RUs, additional industry stakeholders, the U.S. Department of Defense (DoD), and state regulators. Principle recommendations include the following:

- *Create a team within Cybersecurity, Energy Security, and Emergency Response (CESER) that is responsible for sustained collaboration with industry on DCEI.* When DOE launched the DCEI program, the Department had not yet established a structured, systematic process for follow-up and coordination with the RUs that own/operate DCEI. In 2020–2021, DOE's Office of Electricity established more robust coordination mechanisms. Now that the DCEI program has transitioned to CESER, building on that progress will be of **foundational importance** for strengthening DCEI resilience, given the intensifying threats to DCEI and the significant coordination and policy issues surrounding the program, including those examined in this report.

- *Develop new funding options.* As threats to DCEI intensify, RUs will face a growing need to invest in DCEI and security. From an equity perspective, it makes no sense to require civilian utility customers to pay for investments that directly meet national defense needs versus ensuring reliable service to those customers themselves. This report proposes options to leverage federal funding for such investments rather than placing the burden entirely on ratepayers.

- *Accelerate the development of DCEI-specific resilience assessment tools.* The Electricity Advisory Committee (EAC) and other organizations have an array of valuable studies underway on resilience metrics. DOE should supplement these efforts by sponsoring the creation of metrics and assessment tools focused on the unique challenges of DCEI. Examples include the following:

---

[1] Critical Defense Facilities are those installations that are "critical to the defense of the United States," and "vulnerable to a disruption of the supply of electric energy provided to such a facility by an external provider." Defense Critical Electric Infrastructure is "any electric infrastructure that serves" a Critical Defense Facility, "but is not owned or operated by the owner or operator of such facility" within the continental United States. Excerpted from Section 215(a) of the Federal Power Act at https://www.law.cornell.edu/uscode/text/16/824o.

[2] DOE defines "responsible utility" as "an electric utility that owns or operates Defense Critical Electric Infrastructure." DOE. Revocation of Prohibition Order Securing Critical Defense Facilities. *Federal Register*, Vol. 86, No. 76 (April 22, 2021), 21309. https://www.govinfo.gov/content/pkg/FR-2021-04-22/html/2021-08483.htm

- Assessment tools should account for the likelihood that near-peer adversaries will seek out and target DCEI vulnerabilities and/or selectively disrupt the restoration of service to CDFs in ways that go far beyond the restoration challenges posed by natural hazards.

- New resilience metrics should also help DOE, regulators, and RUs determine "how much resilience is enough" against attacks designed to cripple CDF execution of Mission Essential Functions, where near-zero risk of failure will likely be the metric for adequacy.

- *Develop specialized mechanisms for DCEI-related information sharing*. RUs are prime targets for attack because of the CDFs they serve. To target investments in DCEI resilience, help utilities protect grid reliability when attacks begin and conduct restoration "under fire" (i.e., in the face of sustained cyber and/or physical attacks). RUs could benefit from specialized DOE information and intelligence sharing. This report proposes options for DOE to supplement the valuable information sharing initiatives that the Department already has underway by establishing a Critical Infrastructure Command Center (as proposed by the National Infrastructure Advisory Council [NIAC]) in addition to using state National Guard and local Federal Bureau of Investigation (FBI) facilities for two-way sharing of sensitive information when adversaries have disrupted normal communications systems.

- *Launch a dialogue on long-lead policy issues and opportunities for coordination.* In addition to the near-term initiatives summarized above, DOE and its federal partners should consider initiating discussions on emerging issues and opportunities for progress. Chief among them are the following:

  - *Coordination between DCEI and Grid Security Emergency (GSE)-related initiatives.* There is substantial overlap between the RUs and those utilities that, in a presidentially declared Grid Security Emergency, might receive GSE orders from DOE pursuant to Section 215(a) of the Federal Power Act. This report suggests promising opportunities for integration and mutual support between DCEI and GSE initiatives with industry.

  - *Account for possible expansions in designated CDFs.* Civilian seaports, air transportation companies, and many other non-Defense assets are absolutely vital for deploying and sustaining U.S. forces abroad. Other assets fall within the U.S. Department of Homeland Security's (DHS) definition of National Critical Functions. If DOE and its federal partners begin to expand the definition of CDFs to include these civilian assets and widen the scope of DCEI accordingly, RUs and their industry partners would want to consult with the Department on such issues.

Approach

This report is based on extensive interviews conducted with RUs, electricity subsector trade associations, and regional transmission organizations/independent system operators (RTOs/ISOs). All such interviews were conducted on a confidential, not-for-attribution basis, and anonymized quotes are taken directly from interviewees. The findings and recommendations in this report represent the views of the EAC and do not necessarily reflect the views of the parties and stakeholders who provided input for the development of this work product.

The report also draws on an October 14, 2020, briefing to the EAC on evolving DCEI programmatic initiatives, presented by Jennifer DeCesaro and Johanna Zetterberg, who were then on the staff of DOE's Office of Electricity.[3] In addition, the report benefits from significant contributions by EAC members.

Findings

Finding 1: Lack of formalized roles, defined program goals, broader industry engagement, and interagency coordination

Each RU interviewed for this study expressed strong support for strengthening DCEI resilience and, more broadly, helping to protect U.S. national security. The intent of this report is *not* to criticize the DCEI program or its initial rollout. *Every* equivalent initiative of such scale and criticality for national security experiences start-up difficulties. Furthermore, the entities interviewed for this report stressed that, in many respects (including the description of the program's importance in the emerging threat environment), the program's launch was exemplary. Most important, as noted in the Introduction, DOE has made significant progress since 2019 in strengthening coordination with industry.

Nevertheless, when DOE issued the initial letters in 2019 informing these utilities of their status, many of them received limited or no follow-up on expected next steps or actions and implementation measures, including how the government may be able to assist any expected actions. Those that did get feedback received it in the form of verbal communications, which created confusion and posed challenges for coordination within RUs (versus written documentation that could have been more easily shared internally). DOE has since strengthened these coordination mechanisms. The findings and recommendations that follow are intended to

[3] DeCesaro, Jennifer, and Johanna Zetterberg. DOE, Office of Electricity. *Defense Critical Electric Infrastructure*. Presentation to the Electricity Advisory Committee, October 14, 2020. https://www.energy.gov/sites/prod/files/2020/10/f79/OE%20DCEI%20Strategy%20for%20EAC%2010.14.20%20FINAL.pdf

build on that progress and ensure that collaboration between industry and DOE can meet future threats to DCEI.

Finding 1a. Lack of an adequately structured DOE team for industry engagement

A number of RUs stressed that, going forward, industry would benefit from having a dedicated, centralized point of contact (POC) in DOE for sustained coordination, which could authoritatively represent DOE on emerging issues and consensus-building efforts. Others indicated that the program would benefit from having tighter "command and control" for when multiple DOE offices take an interest in DCEI-related issues and reach out to RUs. Entities suggested that DOE's dedicated DCEI team be responsible for coordinating with industry on developing "plans, checkpoints, milestones, and structure follow-up on identified shortfalls" in program implementation. Ideally, the DOE team also would be able to speak on behalf of DOE on broader issues raised by RU interviewees. The bottom line, as one RU respondent emphasized, is that "the most important thing that DOE could do is to create a sustained team in the Department to answer our questions, help us resolve problems, and provide for reachback to senior leaders."

Finding 1b. Need for additional DOE clarity and guidance on DCEI program goals

Confusion persists around DOE's objectives for the DCEI program and on criteria for determining and communicating which specific infrastructure is being categorized as DCEI within an RU's system. An interviewee emphasized that "no one is sure what exactly the goal is here. Fixing America's Surface Transportation Act (the FAST Act) says to identify CDFs/DCEI but says nothing beyond that. We aren't opposed to further steps, but what are DoD and DOE trying to achieve here? That needs to be clearly articulated so industry can provide recommendations on how best to achieve [those goals]." One highly experienced entity leader emphasized that despite DOE's past outreach, "I don't really know what DCEI is." Another stated that "we need more clarity on what is in and what is out."

Finding 1c. Lack of DOE engagement and information sharing with a broader array of industry stakeholders based on a "value added" approach

While limiting the availability of DCEI-related data is essential for national security and other imperatives, expanding industry engagement beyond the RUs (and beyond the informational briefings provided to the Electricity Subsector Coordinating Council) could create new opportunities to strengthen infrastructure resilience and build preparedness against potential attacks.

The RTOs and ISOs contacted for this report stated that they could provide valuable support for responsible entities and overall DCEI resilience, both for pre-event planning and during response operations. Reliability coordinators also could play a key role in protecting and restoring service to CDFs. However, these entities reported that despite repeated efforts, DOE had not yet included them in discussions on DCEI resilience.

Trade associations also are able to offer valuable expertise and support to their members who have been designated as "responsible entities." This is especially true for smaller rural cooperatives, public power, and investor-owned utilities that may serve vital CDFs but have limited cyber resources of their own (including experienced cyber personnel). Distribution-only entities that provide the "last mile" of service to defense installations (and may be under the regulatory purview of state or municipal authority) could deserve further consideration in this regard as part of a wholistic strategy that includes generation and transmission assets essential for serving CDFs.

The October 2020 DOE briefing on DCEI provides a useful foundation when considering broader industry engagement and information sharing. The briefing included a "program pillar" to "create and maintain key partnerships." The focus of this pillar is to "[r]efine the needs for partner and stakeholder information sharing, coordination, and collaboration." Key partners in that effort include CDF owners and operators; DCEI owners and operators; state, local, tribal, and territorial governments; power marketing administrations; security, intelligence, and law enforcement communities; grid reliability organizations; technical assistance providers; federal agencies; and others.[4]

Finding 1d. Inadequate unity of effort between DOE and DoD with respect to RUs

Every responsible entity surveyed for this report already had collaborative relationships with the major defense installations in their service areas before the DCEI program began. In some cases, that collaboration was extensive and included measures to assess and bolster the resilience of the military bases in question. Coordination typically occurred between utilities and the base commander of the installation. Increasingly, however, those discussions have included input from DoD "mission owners"—that is, representatives of the combatant commanders, service components, or other DoD organizations responsible for the missions (at home and abroad) that defense installations help execute.

A number of RU respondents noted that coordination between DOE and DoD on outreach to responsible entities is poor. These utilities report that they receive multiple requests for information, and sometimes requests for coordination on resilience initiatives, from both DoD and DOE. It is not clear "who has the ball," according to one entity. "We feel 'whipsawed'" said another.

Industry concerns over multiple (and potentially conflicting) sources of federal requirements regarding service to Defense installations are likely to grow, and are part of a larger, multilayered problem for RUs (e.g., DoD's efforts to expand the Cybersecurity Maturity Model Certification program beyond the Defense Industrial Base to utilities that have certain types of service

[4] DeCesaro and Zetterberg, op. cit., Slide 9.

contracts with defense installations, including CDFs).[5] Interviewees noted that the DHS definition of Defense Industrial Base explicitly excludes electric utilities.[6] Moreover, bulk power system entities are already subject to mandatory, enforceable critical infrastructure protection standards for cybersecurity. The costs and management burdens for responsible entities to comply with multiple and potentially redundant or conflicting security requirements would be significant.

Finding 2: Funding

In many cases, it would be unfair to expect ratepayers to fund improvements in DCEI resilience. Some resilience investments may provide benefits for both the CDF and other customers served by the same infrastructure. In other instances, however, DCEI upgrades to bolster service to CDFs will have little or no benefit to ratepayers in the region. In particular, equity problems will be significant for DCEI investments on behalf of remote CDFs that have few other customers in the area, or in dense urban areas where building additional substations could be expensive and difficult to get permitted.

Finding 2a. Existing DOE and DoD funding sources

A number of respondents argued that DoD- or DOE-appropriated funds are the appropriate way to pay for investments in DCEI resilience. One respondent stated that "If these upgrades are truly necessary for national security, DoD/DOE needs to find a pot of money to pay for them. *Full stop*." Another stated that "The Pentagon never imagines that it could get F-35s for free. Yet somehow DOE thinks that it can get additional substations for free." Still another cautioned that DOE was at risk of creating "unfunded mandates" for RUs. These concerns make it all the more important to pursue supplementary forms of funding for DCEI upgrades.

Precedents exist for DoD funding of energy projects by utilities. Energy savings performance contracts (ESPCs) and utility energy service contracts (UESCs), for example, are two of many examples of such funding opportunities, which are often focused on "inside the fenceline" projects.[7] DoD notes that both ESPCs and UESCs can be used "to enhance energy resilience and cybersecurity at DoD installations in support of the National Defense Strategy."[8]

---

[5] Office of the Under Secretary of Defense for Acquisition and Sustainment. Cybersecurity Maturity Model Certification. https://www.acq.osd.mil/cmmc/

[6] According to the DHS definition of "Defense Industrial Base," "The Defense Industrial Base Sector does not include the commercial infrastructure of providers of services such as power, communications, transportation, or utilities that the Department of Defense uses to meet military operational requirements." https://www.cisa.gov/defense-industrial-base-sector

[7] DoD. Memo re: Policy on Energy Savings Performance Contracts and Utility Energy Service Contracts. November 2018. https://www.acq.osd.mil/eie/Downloads/IE/Signed%20ESPC%20and%20UESC%20Policy%20Nov%2020%202018.pdf

[8] DoD. Installation Energy Policy and Program Guidance. https://www.acq.osd.mil/eie/ie/FEP_Policy_Program_Guidance.html

However, one respondent cautioned against relying on existing DoD funding mechanisms that were designed for other purposes: "I have no idea how an ESPC concept would work for funding DCEI-related investments. DoD/DOE needs to just find a pot of money, not chase complicated funding schemes like this." Of course, at a time of intense pressure on federal budgets, gaining additional appropriated funds for DCEI improvements will be politically challenging.

Finding 2b. Broader funding issues

Interviewees also raised a variety of broader funding issues and concerns:

- Some respondents emphasized the importance of addressing cost recovery for investment in the distribution-level infrastructure that provides the last mile of service to CDFs.
- Respondents noted the importance of taking "the different business models (public power versus co-ops versus investor-owned utilities)" into account when developing alternative funding models and assessing funding support levels.
- Another respondent stated the following:

> "Funding for the dedicated part of the infrastructure will be critical to making the level of improvements needed. Most utilities have policies in place to collect reimbursement for special facilities to keep from overburdening the general ratepayers. These policies have probably limited the robustness of the existing services to DCEI as the DoD budgets have been limited for that type of expenditure. I think this is already covered, to some extent, in the document but wanted to point it out in this way."

One commentor noted the importance of considering "all ways DCEI could be strengthened that don't require money/investments. For example, just getting sites put at the bottom of load shedding lists, adding them to black start cranking paths, etc., could go a long way and avoid the (inevitably difficult) prospect of funding investment upgrades." DOE did advance a number of additional mitigation options in the December 2020, *Prohibition Order Securing Critical Defense Facilities.*[9] And while the order was subsequently revoked,[10] those initiatives demonstrate the Department's acknowledgment and commitment to examining innovative options to strengthen DCEI resilience.

---

[9] DOE. Prohibition Order Securing Critical Defense Facilities. December 2020. https://www.energy.gov/sites/prod/files/2020/12/f81/BPS%20EO%20Prohibition%20Order%20Securing%20Critical%20Defense%20Facilities%2012.17.20%20-%20SIGNED.pdf

[10] DOE. Revocation of Prohibition Order Securing Critical Defense Facilities. *Federal Register*, April 22, 2021. https://www.federalregister.gov/documents/2021/04/22/2021-08483/revocation-of-prohibition-order-securing-critical-defense-facilities

Another commentor noted that funding for redundancy projects is critically important and "can be at various levels like feeds from multiple substations and multiple circuits." Such projects might "include some 'obscure' circuits paths that are either hidden underground or able to be created through overhead switching that may not be obvious. Projects might also provide for the ability to create dedicated feeds during risky or abnormal times by switching non-critical laterals and loads to other circuits. This may help obscure the dedicated path during normal times."

Another commentor stated that if properly sited, certain types of infrastructure investments will almost certainly add resilience (e.g., stored/pumped hydropower, underground/submarine distribution lines, energy storage systems, localized small-scale cloud servers). As funds become available to support RU investments in resilience, these types of upgrades might be incentivized.

Finding 3: Sponsoring the development of DCEI-specific resilience assessment tools, standards, and metrics

Closely related to funding is the problem of establishing specific resilience needs for DCEI.[11] Thanks to DOE's April 20, 2021, *Request for Information on Ensuring the Continued Security of the United States Critical Electric Infrastructure*, industry had the opportunity to offer recommendations on establishing regulations, prohibitions, and other requirements to manage supply chain risks to DCEI and other infrastructure. However, threats to supply chains constitute only one of a growing number of potential attack vectors against DCEI. Moreover, against specific threats of greatest concern to DOE, "how much resilience will be enough?" What criteria should be established to assess progress toward achieving DCEI resilience goals? And are these goals appropriate to apply to DCEI and RUs, versus or in combination with applying them to CDFs for "inside the fenceline" resilience? These and other questions will take years to resolve and will need close coordination with initiatives on supply chain risk management, industrial control systems (ICS) security, and other DOE resilience initiatives to avoid overwhelming industry with multiple duplicative, and potentially conflicting, requirements.

One immediate opportunity for progress lies in developing an analytic framework and supporting metrics to assess the current status of DCEI resilience and identify critical gaps. The starting point for doing so is to specify the mission critical loads that must be served in a CDF, and the ability of the base's emergency power generators (current and programmed) to serve those loads for specified periods if grid service is interrupted. Assessments also should account for broader requirements for CDFs to perform their Mission Essential Functions and, above all, the ability of the surrounding communities that house their employees to maintain power, water, and other critical services for those employees and their families.

The EAC already has initiatives underway to develop recommendations on how to assess grid resilience, including the study being led by members of the Grid Resilience for National Security

[11] As will be subsequently discussed, a valuable mission assurance-focused resilience study is underway through the Grid Modernization Initiative.

Subcommittee. Other organizations also are focusing research on that topic. Especially significant is the Grid Modernization Initiative, which is conducting a study on *Energy Resilience for Mission Assurance*, which incorporates national security objectives into power system planning by theorizing, demonstrating, and vetting approaches to explicitly represent mission performance during long duration power system disruptions.[12] As those efforts go forward, they might account for DCEI-specific issues of concern to responsible entities.

Another source of valuable analysis and recommendations is the study published by the National Association of Regulatory Utility Commissioners on *Regulatory Considerations for Utility Investments in Defense Energy Resilience.* The study finds that regulatory proceedings that have taken DoD energy resilience into account can provide important lessons learned for consideration of DCEI-related issues by state regulators. The study also identifies new and complex questions for regulators raised by Defense energy resilience, including for DCEI. Key examples: "Should DoD, other federal agencies, ratepayers, or a combination of these be responsible for supporting defense energy resilience investments? How do we determine the share that each entity should contribute?"[13]

Finding 3a. Delineating relevant DCEI infrastructure for initial resilience assessments

Regardless of which tools and metrics are used, efficient and effective program management will require DOE, responsible entities, DHS, and DoD to agree on which components of DCEI should be the focus of initial assessments and potential risk management efforts. DCEI comprises electricity supply paths serving CDF missions, which may include generation assets, transmission and distributions lines, and substations and other grid interconnections. This definition comprises a potentially extensive array of infrastructure components and systems for many RUs. It may be helpful to develop and apply a risk-based approach to narrow the focus of initial resilience assessments.

Finding 3b. Holistic assessment of loads to be served and requirements for DCEI-provided power in emergencies

As noted in the introduction, it will be helpful to specify the mission critical loads that must be served in a DCF, and the ability of the base's emergency power generators (current and programmed) to serve those loads for specified periods if grid service is interrupted. Firm power resources and the vulnerability of their fuel supply chain back to sources, including refineries and pipelines and their cyber vulnerability, should be a focus, particularly in the context of expanding

[12] DOE. *Grid Modernization: Updated GMI Strategy 2020.* December 2020. p. 41. https://www.energy.gov/sites/prod/files/2021/02/f82/GMI_Strategy_FINAL%20as%20of%201.20.21.pdf

[13] National Association of Regulatory Utility Commissioners. *Regulatory Considerations for Utility Investments in Defense Energy Resilience.* November 2021. pp. 5–6.

distributed energy resources and intermittent renewable energy deployments. A growing number of military bases are bolstering their emergency power capabilities, including those based on renewable energy resources. They also are hardening their on-base distribution systems and supporting ICS against cyberattacks and improving their capabilities to black start their emergency energy systems. In addition, supported by the U.S. Army Corps of Engineers, installations are beginning to address the need for fuel resupply for longer duration power outages and replacement of generators as they break down due to extended use (or, in some cases, as one responded noted, "lack of proper maintenance by the base").

Assessments of DCEI resilience requirements must not be made in a vacuum but rather in a holistic manner. Under DoD's current leadership, "inside the fenceline" energy initiatives are likely to accelerate and encompass a widening array of CDFs. A holistic approach to assessing resilience requirements also will account for the grid-dependent infrastructure and critical functions on which surrounding communities rely. Employees of many military installations live off-base. Unless base employees know that their families will have the power, water, and other services necessary for their safety, those employees may feel compelled to take care of their families rather than report for duty. Moreover, many installations themselves (starting with the Pentagon) rely on water and wastewater services provided by their surrounding communities. Accounting for the requirements for resilient power in this broader context will be essential as well.

Finding 3c. Modeling tools for cyber and physical threats

Many current initiatives for developing resilience methodologies focus on natural hazards. Severe weather events and other such hazards can be assessed in terms of their likelihood of occurring and—based on these assessments—the costs that can be avoided by a given investment in resilience against such events. No equivalent approach will be useful for assessing investments in DCEI. For example, stochastic modeling of multiple scenarios is unlikely to be of significant value for resilience decision options against nation state attacks on absolutely vital CDFs. It would be more prudent to focus on events at the furthest "tail probabilities" that such models produce (e.g., catastrophic attacks wherein China and Russia carefully target attacks to maximize the disruption of U.S. national security). Localized threats, such as cyclical extreme storm events or seismic clusters, can be recognized and mapped (in the Pacific Northwest and Alaska, for example) into threat levels or resilience metrics for DCEI-affected sites. DOE's Grid Modernization Initiatives are tackling many of these issues, as is the EAC's own project on grid resilience and metrics. As these efforts evolve, a number of opportunities exist to address DCEI-specific issues.

Finding 3d. Restoration as a component of resilience metrics

Over the longer term, assessments of current levels of resilience should account for the ability of responsible entities to conduct "restoration under fire." Nation state attacks are not likely to be "one and done." As in the GridEx scenarios, they may continue for weeks, and be strategically targeted to disrupt restoration operations (including black start). The development of DCEI

resilience metrics should draw on lessons learned from GridEx V (November 2019) and the recent GridEx VI (November 2021).[14] The Defense Advanced Research Projects Agency's (DARPA) Rapid Attack Detection, Isolation and Characterization Systems (RADICS) program also enabled transmission operators and their partners to exercise black start restoration of the power grid under simulated attack conditions.[15]

RUs need to be able to operate DCEI manually "in the event of a cyber threat or disturbance. As the systems and operators become more dependent on automated, systems operations which require various communication infrastructure, it is important to retain enough basic manual operating/switching capability and operational expertise to continue operations during these events." Moreover, there needs to be a commitment on the part of the RU and military customers to periodically exercise manual operations in a degraded state while under "blue skies" in addition to and not a replacement for the "pull the plug" exercises. However, it is important to remember that exercises come at a cost, including additional labor, reduced revenue, and potentially service impact/degraded operations related to the exercise, which should not be passed on to the rest of the ratepayers.

Human capital also will be a key contributor to DCEI resilience if/when that infrastructure comes under attack. Experienced RU operators with detailed knowledge of their systems, and of attack mitigation and power restoration options, will be critical for sustaining or rapidly restoring power to CDFs. Sustained investment in workforce development should be prioritized accordingly.

Finally, over the longer term, restoration and resilience assessments should account for (1) the impact of "electrification of everything" on CDF power requirements involving DCEI, and (2) the risk that when earthquakes, hurricanes, or other events occur during an ongoing crisis with an adversary, that adversary may launch an "opportunistic" attack to disrupt restoration operations and exacerbate disruptions to DCEI and the CDFs they serve.

Finding 3e. Accounting for interdependencies: Natural gas and beyond

Electric service going into CDFs is only as resilient as the generation of power on which DCEI relies. Much of the nation's generation capacity, in turn, relies on the delivery of natural gas. DOE and its partners would benefit from examining the indirect risks posed to DCEI resilience by adversary threats to natural gas pipelines, rail lines for coal, and other delivered fuels, and assessing the implications of these findings for DCEI program strategy. Responsible entities can make critical contributions to such assessments. They have detailed understanding of their interdependencies with the infrastructure associated with their generation fuel types. They also can assist in examining the risk posed to CDFs from cascading failures between sectors. Collaboration with

[14] North American Electric Reliability Corporation (NERC). *GridEx V Lessons Learned Report*. March 2020. https://www.nerc.com/pa/CI/ESISAC/GridEx/GridEx%20V%20Public%20Report.pdf
[15] Defense Advanced Research Projects Agency (DARPA). *Rapid Attack Detection, Isolation and Characterization Systems (RADICS).* https://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems

DHS's National Risk Management Center and integration of DCEI resilience efforts with the North American Energy Resilience Model (NAERM) initiatives may be helpful in assessing DCEI resilience in this multi-sector context.

The need to account for gas-electric interdependencies further exemplifies the value of including RTOs/ISOs and reliability coordinators in DCEI resilience assessments. One responsible entity noted that they are uncertain as to whether they have an adequate understanding of the indirect risks to DCEI posed by disruptive threats to natural gas transmission systems, and that a number of RTOs/ISOs are seeking to clarify such issues. Of course, NAERM also can make analytic contributions in this regard. Quantifying the risks to DCEI posed by gas-electric interdependencies would need to focus on the following:

- Physical and cyber threats to pipelines and estimates of service interruptions associated with them
- Potential effects of attacks interrupting gas flows to specific generators in RTO/ISO service areas
- Pipeline system networking, redundancies, and capabilities for emergency operations that may mitigate the consequences of adversary attacks on power generation
- Increasing the reliance of gas pipeline compressors on electric power versus offtake gas, and the attendant risks of mutually reinforcing gas-electric system disruptions during adversary attacks
- Issues involving firm versus interruptible service for DCEI
- Other factors that could affect the generation of power on which DCEI relies

One respondent noted that a number of RTOs/ISOs have performed analysis of the potential effects of gas supply disruptions on grid reliability (although not specifically the impacts on DCEI) and suggested that industry-government initiatives on resilience assessments leverage this analysis, if possible. In particular, the risks of gas supply interruptions are magnified by "the inability for natural gas pipeline companies to obtain regulatory approval to build new pipelines to improve resilience and supply alternatives. How is the electric side factoring that into their planning when building gas-powered plants?"

Finally, while the analysis above has focused on gas-electric interdependencies, interviewees noted that the electricity subsector also has other dependencies. The availability of diesel or other secondary fuels can mitigate the loss of gas supplies for dual-fuel generators, but only if that diesel fuel can be resupplied in long-duration outages. The communications sector, including both wired and wireless services and other critical service providers (including cloud storage and other data and software services), offers potential points of electric system vulnerability as well. The water sector also provides essential cooling functions and other services.

Finding 3f. A strategic "bridge" is needed between resilience metrics and improved reliability metrics and assessment tools.

The Interruption Cost Estimate (ICE) Calculator has long served as a vital tool to help assess the cost-effectiveness and prudency of investments to strengthen the reliability of service against short-duration outages. Efforts are now underway to update the ICE Calculator with fresh data, more advanced methodologies for estimating the economic costs of outages (including on a regional basis), and other much-needed improvements. Lawrence Berkeley National Laboratory's study on *A Hybrid Approach to Estimating the Economic Value of Enhanced Power System Resilience* is especially useful in this regard.[16]

The development of assessment tools for investments in DCEI resilience would benefit from developing along a separate but coordinated path. In particular, DOE and industry can explore opportunities to "crosswalk" resilience and reliability assessment tools and help ensure that partners ultimately have the tools they need for investing against the full spectrum of hazards and outage lengths—from traditional reliability events to extended, full-scale cyberattacks by nation states.

Such an integrated approach also could help address broader DCEI interdependency issues and resilience assessment challenges. In addition to interdependencies with the natural gas system, DCEI has interdependencies with surrounding electric systems, which utilities can assess using metrics/tools focused on ensuring broader grid reliability. By employing updated versions of the ICE Calculator, utilities may be able to more effectively design their systems to meet specified standards and criteria. However, for responsible entities, such design efforts also would need to include DCEI-related guidance and criteria that DOE and partner entities jointly develop. These partners would need to avoid creating gaps and seams between broader system reliability and DCEI resilience metrics, and strategically bridge them instead.

Of course, because past metrics development efforts have primary focused on reliability, new approaches will be necessary for resilience. Reliability metrics analyze the historical performance of the system and utility operations. Instead of relying on such historical data, resilience metrics might be based on the resilience capabilities of CDF power systems, the local distribution systems serving those installations, and the regional subtransmission/transmission systems that provide power for distribution utilities. Such assessments might employ a system that gives points for resiliency elements. Examples include local generation, fuel type and hours/days of back-up, circuit back-ups within the site, redundant feeds from the RU, the obscurity of the redundant feeds, the number of redundant substations, the number of redundant subtransmission lines, and so forth. A point system also could include operational processes in the DCEI and at the RU. The assessments could be used to evaluate the strengths, weaknesses, and improvement

[16] Lawrence Berkeley National Laboratory. *A Hybrid Approach to Estimating the Economic Value of Enhanced Power System Resilience*. February 2021. https://emp.lbl.gov/publications/hybrid-approach-estimating-economic

opportunities in the various sets of assets, resources, and operational processes that provide resilience for DCEI.

Finding 4: Developing specialized mechanisms for information sharing for DCEI-related threats

DOE continues to improve its sharing of threat-related data with industry. Nevertheless, a number of RUs suggested that they might benefit from expanded information sharing that reflects a harsh reality: Because they serve CDFs, they could be prime targets for attack. Calls for additional data sharing are hardly new (or limited to responsible entities). Most notably, in a 2019 study on *Transforming the U.S. Cyber Threat Partnership*, NIAC found that despite sustained efforts to improve the sharing of threat data with the private sector, existing information sharing and partnership structures are neither agile enough nor tactical enough to respond to a cyber-attack with the necessary speed.[17]

Since the publication of that report, DOE and its partners have strongly advocated for the advancement of information sharing, both for Enterprise IT through programs such as the Cybersecurity Risk Information Sharing Program (CRISP) and for the operational technology ICS realm enhanced with the announcement of a 100-day ICS Action Plan for increased industry-government visibility, detection, and response capabilities.[18] Leaders of the energy and financial sectors also have partnered to establish the Analysis and Resilience Center for Systemic Risk, a nonprofit, Section 9-specific cross-sector organization designed to mitigate systemic risk to the nation's most critical infrastructure from existing and emerging threats.[19]

Gaps remain, however. The Cyberspace Solarium Commission called for additional partnership initiatives "with the owners and operators of the most critical infrastructure and improved intelligence sharing between government and industry."[20] NIAC's follow-up study in 2021 frames the need for deeper and more timely sharing in starker terms:

> "The absence of direct collaboration and innovation with the private sector creates intelligence gaps: government cyber threat data often lacks the context and transparency to determine how an attack could manifest in infrastructure systems or the potential magnitude of damage or disruption. This delays the federal government's ability to translate aggressive cyber threats into actionable mitigation measures and distinguish those threats that pose the greatest risks to national security. This gap creates the

[17] The President's National Infrastructure Advisory Council. *Transforming the U.S. Cyber Threat Partnership.* December 12, 2019. pp. 5–6. https://www.cisa.gov/sites/default/files/publications/NIAC-Transforming-US-Cyber-Threat-PartnershipReport-FINAL-508.pdf
[18] DOE. *Energy Sector Cybersecurity Preparedness*. https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity
[19] https://www.businesswire.com/news/home/20201030005462/en/Announcing-the-Formation-of-the-Analysis-Resilience-Center-ARC-for-Systemic-Risk
[20] Cyberspace Solarium Commission. Final Report. 2020. p. 144. https://www.solarium.gov/

potential to over- or under-estimate a cyber threat and hinders appropriate federal and industry response."[21]

The proposed DOE DCEI team and its industry partners would benefit from considering the following options, in addition to providing the necessary clearance to industry if implemented, to help meet the specialized needs of RUs (as well as reliability coordinators and other entities essential for cyber preparedness and response):

- Critical Infrastructure Command Center (CICC): Proposed by the President's National Infrastructure Advisory Council (NIAC), a fully operational CICC will provide a classified space for senior executives and cyber experts from the energy, financial services, and communications sectors to work collaboratively with intelligence analysts and other government staff to operationalize intelligence, provide tactical and innovative solutions, and mitigate the most pressing cyber threats in real time.

  Interviewees for this report noted some considerations if the CICC initiative goes forward. First, NIAC developed the proposal without explicit attention to whether RUs should be included and how their specialized needs might be met. Second, it would be crucial to ensure that "the CICC will help the DCEI entities without putting them in a new bucket to be subject to additional regulations."

- Joint Collaborative Environment (JCE): Proposed by the Cyberspace Solarium Commission, the JCE would share cyber threat data among federal entities and between the U.S. government and the private sector. The Commission also proposed that the "most critical of the critical"—meaning systemically important critical infrastructure—would be identified and subjected to specific benefits and requirements to support U.S. security priorities.[22]

  As with the CICC, interviewees expressed concern that not all RUs will "make the cut" for inclusion in the JCE. In addition, it would be essential to provide for that inclusion within the system for broader government-industry information sharing and the cyber incident response that is emerging under the Administration, with both DOE and DHS playing crucial roles in that system. As DOE and industry discussions go forward on this broader coordination system, useful options for consideration are provided in a recent study,

[21] The President's National Infrastructure Advisory Council. *Actionable Cyber Intelligence: An Executive-Led Collaborative Model*. January 21, 2021. pp. 5–6.
https://www.cisa.gov/sites/default/files/publications/NIAC%20Actionable%20Cyber%20Intelligence_FINAL_508_0.pdf

[22] Cyberspace Solarium Commission. March 2020.
https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view

National Cyber Defense Center: A Key Next Step Toward a Whole-of-Nation Approach to Cybersecurity.[23]

- Existing mechanisms for specialized information sharing with DOE and other federal partners: A growing number of RUs and other utilities have close collaborative relationships with their respective state National Guard (NG) organizations, especially for providing NG support for power restoration following natural hazards and, increasingly, in anticipation of cyberattacks. Some of these NG installations also provide for access to their Sensitive Compartmented Information Facilities (SCIFs) for utility personnel with the necessary clearances. FBI field offices also can provide on-site facilities for specialized information sharing.
- RU access to CDF facilities: Every CDF has an SCIF. One respondent suggested that DOE partner with DoD to "create a path for the DCEI entities to have read-ins, briefings, and access to classified space via the bases themselves." In doing so, they could "build upon the relationship DCEIs and CDFs *should* have and encourage regular engagement and a shared space. One idea for consideration is to host a quarterly virtual classified DOE briefing for CDFs and DCEIs (with the trade association personnel who have clearances) that DCEI's can participate in at the CDF's SCIF." This would allow for sharing during blue sky days and provide a place for coordination and sharing on black sky days.
- Funding for installation of SCIFs at RUs (*not recommended*): In theory, it might be possible to have DOE or other agencies fund and authorize RUs to have their own SCIFs and associated secure communications systems to DOE. In practice, most respondents rejected this option as neither necessary nor desirable. One noted that "some DCEI utilities are extremely small; suggesting that they have SCIFs is wild." Another noted that while some utilities may consider SCIFs worth the trouble, many others might find them too costly and difficult to maintain and a source of still more regulatory requirements. The other options recommended above are more viable.

Finding 5: Initiating discussions on long-lead DCEI policy issues

All findings provided above constitute urgent priorities for building on DCEI progress to date. However, for the longer term, the EAC would like to present two additional topics that could offer significant benefits.

Finding 5a. Opportunities for mutual support between the DCEI program and Grid Security Emergency (GSE)-related initiatives

Section 215A of the Federal Power Act provides a foundation for discussions about opportunities for mutual support between the DCEI program and GSE-related initiatives. The Act grants the

[23] Miller, James, and Robert Butler. *National Cyber Defense Center: A Key Next Step Toward a Whole-of-Nation Approach to Cybersecurity*. Johns Hopkins University, Applied Physics Laboratory. July 2021. https://www.jhuapl.edu/Content/documents/NationalCyberDefenseCenter.pdf

Secretary of Energy the authority to issue orders to power companies to protect and restore grid reliability in GSEs.[24] In recent industry-led exercises, including GridEx V and a June 1, 2021, tabletop exercise conducted by the Electricity Subsector Coordinating Council's GSE Working Group, a number of opportunities emerged for mutual support between GSE and DCEI.

In both exercises, the scenario involved the issuance of GSE orders to an RU to prioritize the protection and restoration of power to a notional CDF. Participants in the 2021 exercise found that during industry-government consultations to draft an order, it would be enormously helpful if the CDF installation commander could have already shared with their RU (and other key partners) data on their power requirements. Such data could include the following:

- What voltages, power quality levels,[25] and other power requirements will the base have during those service periods?
- How might external power requirements for a given utility be adjusted to account for the contribution of emergency generators to serving installation loads?
- What are the technical characteristics of the transmission/distribution power feeds and other electric infrastructure at the CDF that would interface with a given utility's systems?
- What are the time horizons for achieving the goals of the order? One participant noted that "it makes a big difference if we only have a 12-hour window to accomplish the goal of the order" versus a longer period. "Some orders might even need immediate implementation." Time-sensitive orders should include such information, and initial consultations may need to be scheduled accordingly.

Of course, such data also could be valuable to RUs in the context of initiatives to strengthen DCEI resilience (especially in terms of addressing the "how much is enough" issues raised in Finding 3 of this report). Going forward, DOE's DCEI program might make the collection and secure sharing of such CDF power requirements a priority.

There is substantial overlap between the RUs and those utilities which, in a presidentially declared Grid Security Emergency, might receive GSE orders from DOE pursuant to Section 215(a) of the Federal Power Act. This report suggests promising opportunities for integration and mutual support between DCEI and GSE initiatives with industry. Does the CDF need power 24/7, or only during certain periods to execute its Mission Essential Functions? Would intermittent service be acceptable? As installations continue to make progress in their on-base distribution to prioritize

---

[24] The Federal Power Act notes that "Before issuing an order for emergency measures under paragraph (1), the Secretary shall, *to the extent practicable in light of the nature of the grid security emergency and the urgency of the need for action*, consult with appropriate governmental authorities in Canada and Mexico, entities described in paragraph (4), the Electricity Sub-Sector Coordinating Council, the Commission, and other appropriate federal agencies regarding implementation of such emergency measures." [Emphasis added] See 16 U.S.C. § 824o–1, *Critical electric infrastructure security*, Section (b)(3).

[25] Open Power Quality. A Beginner's Guide to Power Quality. https://openpowerquality.org/docs/intro-power-quality.html

service to mission critical loads versus dining halls and other non-essential functions, it may be possible to significantly downsize power requirements and structure GSE orders for DCEIs accordingly.

Finding 5b. Accounting for possible expansions in designated CDFs

While the Federal Power Act provides a definition of CDFs, and DOE already has a close working relationship with DoD to support the Secretary of Energy's responsibilities for designating such facilities, the entities interviewed for this report suggested that consultation would be necessary regarding how the set of CDFs might evolve in the future, and how the possible increased costs of DCEI investments for an expanded set of facilities would be paid for (versus becoming additional "unfunded requirements").

Such consultations might include DoD input on how the Department is reassessing its own requirements for mission assurance. DoD Directive 3020.40, *Mission Assurance* (November 29, 2016), established an important policy shift by directing components to prioritize the combatant commander's execution of operation plans (OPLANs).[26] Focusing on OPLAN execution offers a range of potential benefits. By disaggregating OPLANs and identifying specific dependencies on installations, support functions, and the infrastructure that they rely on, DoD will be able to prioritize and target resilience initiatives in ways that produce the greatest value for deterrence and warfighting. Initiatives to prioritize investments in DCEI would benefit from accounting for this broader process. Consultations with responsible entities on whether additional CDFs are likely to be designated in their service areas also would benefit from accounting for this broader process, given the long lead times required to make resilience investments and ensure funding for them.

Some entities also said that they had received indications that infrastructure serving ports and other civilian assets might be designated as DCEI. Given the importance of such assets to national defense, including the deployment and sustainment of U.S. forces to regional contingences, such "mission creep" is understandable. However, DOE would benefit from hearing from responsible entities on the challenges, risks, and cost of expanding the scope of DCEI. DoD's continuing efforts to disaggregate its missions to better clarify facility support requirements (and associated electric infrastructure implications) also would be helpful to undergird such consultations.

The need for such dialogue also will extend to any possible expansion of DCEI to include DHS-designated National Critical Functions—that is, "functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a

[26] DoD Directive 3020.40: Mission Assurance (MA). https://fas.org/irp/doddir/dod/d3020_40.pdf

debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[27]

Of course, DHS and electric utilities also can continue to advance separate initiatives to strengthen the resilience of electric service to National Critical Functions unrelated to the DCEI program. But doing so would magnify the problems that RUs already face with regard to "double tapping" by DOE and other federal entities and could create confusion over which priorities should prevail in investing scarce resilience resources.

Efforts to achieve unity of effort across the federal government would be beneficial in this realm, as well as for the development of new funding mechanisms so that ratepayers are not required to pay for investments that meet national defense and homeland security needs.

Recommendations

The recommendations below are ordered in accordance with the overall priority assigned to them by the RUs and other entities interviewed for this report. As noted in the Introduction, many of these interviewees emphasized that it was of *foundational importance* for DOE to establish a structured, formalized team for industry engagement on DCEI issues. Their rationale is that doing so is a prerequisite for moving forward on all the other proposals identified in this study and to institutionalize the progress made in DOE-industry coordination over the past year. Progress on funding issues was the other top priority for respondents. The additional recommendations that follow are less urgent, but could offer significant value over the longer term.

Recommendation 1

Recommendation 1a. Formalize a DOE team for industry engagement.

Based on the responses described in Finding 1, the EAC recommends that DOE create a dedicated, centralized POC and team within DOE for sustained coordination, which could authoritatively represent DOE on emerging issues and consensus-building efforts. DOE is best positioned to determine how such a team could be structured within CESER. Clearly defined roles and responsibilities for this POC and their team would help prevent redundancy and confusion when multiple DOE offices take an interest in DCEI-related issues and reach out to RUs. As noted in Finding 1, whenever practical, DOE guidance to entities on DCEI issues should be in written form versus verbal communications that are more difficult to accurately share with chief security officers and other key personnel below the chief executive officer level.

[27] Cybersecurity & Infrastructure Security Agency. National Critical Functions. https://www.cisa.gov/national-critical-functions#:~:text=National%20Critical%20Functions%20(NCFs)%20are,safety%2C%20or%20any%20combination%20thereof

Recommendation 1b. Clarify criteria, terms, and program goals.

DOE's POC and team should clarify relevant criteria, terms, and program goals, and have the expertise and reachback capability to other DOE components to do so. As indicated in Finding 1, several respondents were not clear on the goals related to DCEI, or even the definition of the term itself. DOE's team should coordinate with industry on developing "plans, checkpoints, milestones, and structure follow-up on identified shortfalls" in program implementation. DOE might propose the criteria, and industry would then help refine them and use those criteria to identify the DCEI components of their own systems. Such consultations also should include DoD as appropriate.

Recommendation 1c. Engage and share information with a broader array of industry stakeholders.

The Department should consider what limited types of information would be most useful to provide to RTOs/ISOs, reliability coordinators, trade associations, distribution utilities, and others, given the roles they play in grid reliability and resilience, and how they could support initiatives related to those areas of responsibility.

Engagement could include the following possible areas of support, which would likely be of value to a broad range of entities across all industry components:

- Education and technical assistance on DCEI-related issues
- Insights on policy-related issues
- Clarification of federal requirements and resilience options

To determine which data sets and actions are relevant for different types of DCEI stakeholders and to establish priorities for partnerships and information sharing, DOE should consider mapping threat vectors (focused on disrupting service to CDFs) against infrastructure ownership and system operations beyond just the last mile service providers.

Recommendation 1d. Improve coordination with the U.S. Department of Defense.

The DOE team responsible for DCEI, in coordination with other DOE offices, should consider serving as the lead federal POC for industry DCEI engagement to help deconflict efforts and guidance across federal entities and with the DoD in particular.

Recommendation 2

Recommendation 2a. Consult with DoD to identify options for federal funding of DCEI investments.

Discussions of funding issues and options to resolve them should be a prime focus for future DOE-industry engagement. To avoid asking RU ratepayers to unfairly shoulder the burden of paying

for DCEI infrastructure costs, DOE should identify (in consultation with DoD) options for federal funding of DCEI investments. DOE should consider engaging with DoD on whether existing funding mechanisms might be modified to help responsible entities make targeted, CDF-specific investments in DCEI resilience outside the fenceline, especially against cyber and physical threats.

Recommendation 2b. Address broader industry funding concerns.

Dialogue on developing new sources of funding should also address broader industry concerns:

- DOE should consider cost recovery for investments in distribution-level infrastructure that provides the last mile of service to CDFs.
- When assessing funding opportunities and uses, the different business models (public power versus co-ops versus investor-owned utilities) should be taken into account.
- DOE should consider that limited DoD funding for policies and programs that reimburse utilities for dedicated infrastructure serving CDFs has limited the provision of such infrastructure.
- DOE and industry should conduct focused research on low-cost options to bolster resilience.
- Funding for redundancy projects should be a priority.

Recommendation 3

Recommendation 3a. Determine which infrastructure should be the focus of resilience assessments.

DOE will need to take a targeted approach to risk management within the vast electricity grid and work with its partners to determine the specific energy system infrastructure and equipment deemed to be of the highest priority from a risk management perspective using appropriate risk-based methods in drawing DCEI boundaries on the grid. Partnering with responsible entities to develop such a targeted approach will be essential.

Recommendation 3b. Develop a holistic assessment of loads to be served and requirements for DCEI-provided power in emergencies.

DOE should coordinate with DoD to develop a systematic outreach process to installation commanders and mission owners, and—factoring in their assessment of emergency power capabilities versus operational requirements (including a maximum assumed length of outages)—use that as a starting point to help assess resilience requirements for DCEI-provided power.

Recommendation 3c. Recognize the limits of existing modeling tools for cyber threats.

To assess the prudency of resilience-oriented investments, DOE and its partners should focus on specific threat vectors, vulnerabilities to them, and attack consequences, and largely ignore efforts to measure event probability or stochastic modeling. These partners also should develop options to measure the value of DCEI resilience investments in terms of national security. Typical "avoided cost" approaches are unlikely to be adequate. Moreover, traditional avoided cost models fail to account for mission critical operations and capabilities that must generally be available and are absolutely essential during times of conflict.

Recommendation 3d. Assess potential gaps and investment requirements for contested restoration of service scenarios.

DOE and responsible entities should partner to assess potential gaps and the investment requirements for *contested restoration* of service to CDFs in ways that go far beyond the assessment tools under development for natural hazards. DOE and industry should leverage the insights provided by the GridEx exercises and DARPA RADICS program to develop tools and practices to assess the resilience of DCEI under exercises that test what could be presented by a foreign adversary in the future.

Recommendation 3e. Account for sector, supply chain, and infrastructure interdependencies.

DOE and its partners would benefit from examining the indirect risks posed to DCEI resilience by adversary threats to natural gas pipelines, rail lines for coal, and other delivered fuels, and assessing the implications of these findings for DCEI program strategy. Quantifying the risks to DCEI posed by gas-electric interdependencies should become a primary area of focus for the DCEI program. DOE also should consider sponsoring the development of holistic reliability assessments and metrics to account for other interdependencies, such as with diesel fuel supply chains and the communications sector.

Recommendation 3f. Develop appropriate assessment tools.

The development of assessment tools for investment in DCEI resilience should go forward along a separate but coordinated path to that of the ICE Calculator. In particular, DOE and industry should explore opportunities to "crosswalk" resilience and reliability assessment tools and help ensure that partners ultimately have the tools they need for investing against the full spectrum of hazards and outage lengths, from traditional reliability events to extended, full-scale cyberattacks by nation states.

Recommendation 4: Develop specialized mechanisms for information sharing for DCEI-related threats.

The proposed DOE DCEI team and its industry partners should consider the following options, in addition to ensuring that RUs have the clearance to utilize them, to help meet the specialized needs of RUs (as well as reliability coordinators and other entities essential for cyber preparedness and response):

- Critical Infrastructure Command Center: DOE and responsible entities should explore whether and how a command center of this sort could meet the specialized requirements for defending DCEI.
- Joint Collaborative Environment: As DOE and industry discussions go forward on this broader coordination system, useful options for consideration are provided in a recent study, *National Cyber Defense Center: A Key Next Step Toward a Whole-of-Nation Approach to Cybersecurity*.[28]
- Build on existing mechanisms for specialized information sharing with DOE and other federal partners: DOE and RUs should consider policy initiatives with the National Guard, the FBI, state fusion centers, and other potential partners to expand and institutionalize access to such facilities.
- Provide for RU access to CDF facilities: DOE should consider hosting a quarterly virtual classified briefing for CDFs and DCEIs (with the trade association personnel who have clearances) that DCEIs can participate in at the CDF's SCIF.

Recommendation 5

Recommendation 5a. Pursue opportunities for mutual support between the DCEI program and Grid Security Emergency (GSE)-related initiatives.

DOE should pursue opportunities for mutual support between the DCEI program and GSE-related initiatives. For example, going forward, DOE's DCEI program should make the collection and secure sharing of relevant CDF power requirements with RUs a priority.

Recommendation 5b. Account for the possible expansions in designated CDFs.

DOE should consult with RUs on how the set of CDFs might evolve in the future, and how the possible increased costs of DCEI investments for an expanded set of facilities would be paid for (versus becoming additional "unfunded requirements").

---

[28] Miller, James, and Robert Butler. *National Cyber Defense Center: A Key Next Step Toward a Whole-of-Nation Approach to Cybersecurity*. Johns Hopkins University, Applied Physics Laboratory. July 2021. https://www.jhuapl.edu/Content/documents/NationalCyberDefenseCenter.pdf

Conclusion

DCEI resilience is of critical importance for our nation's security. DOE has a significant opportunity to build on the work it has already done in this area, and the recommendations contained in this report derive directly from insights provided by the RUs and other electric industry stakeholders with whom DOE seeks to improve its collaboration. Key to the success of improving DCEI resilience is establishing a structured, formalized team within DOE for industry engagement on DCEI issues. This would build upon the accomplishments made by DOE to date and serve as a prerequisite for moving forward on all the other proposals identified in this study. Together with the recommendations on the use of appropriated funds to support DCEI investments, and initiatives on resilience metrics and information sharing to help target such spending, the EAC believes the proposals and insights presented here offer significant opportunities for DOE and its partners to strengthen DCEI resilience.