

# RESERVE COMPONENT SUPPORT FOR HOMELAND DEFENSE REPORT

*Advancing Homeland Defense (HD) policy initiatives, supplementing mobilization authorities, and other measures to strengthen the Department of Defense's (DoD) ability to use the Reserve Component (RC) to help achieve HD priorities in the 2022 National Defense Strategy (NDS)*

**Issued by the Reserve Forces Policy Board (RFPB) Subcommittee on the Reserve Component's Role in HD and Defense Support of Civil Authorities**

-----

**CLEARED  
For Open Publication**

Aug 27, 2024

5

Department of Defense  
OFFICE OF PREPUBLICATION AND SECURITY REVIEW



Table of Contents

- I. Executive Summary.....1-2
  - A. Activating, Mobilizing, Allocating, Deploying, and Employing RC forces for HD
  - B. RC Support for DCEI Resilience
  - C. Decision Criteria to help SecDef prioritize Activation and Allocation of RC Forces and Enhance Decision-Making
  - D. Strengthening HD Coordination with Federal Partners
  - E. Improving Unity of Effort Across the RC and with State and Local, Tribal, and territorial (SLTT) governments
  - F. RC Contributions to Deterrence by Resilience
- II. Background of the Report.....3-5
  - A. Section III: Defining HD
  - B. Section IV: Activating, Mobilizing, Allocating, Deploying, and Employing RC Forces for HD
  - C. Section V: RC Support for DCEI Resilience
  - D. Section VI: Decision criteria to help SecDef prioritize the allocation of RC forces and measures to enhance the value of the DoD’s Civilian Employment Information Registry to support decision-making
  - E. Section VII: Strengthening HD Coordination with Federal Partners
  - F. Section VIII: Improving Unity of Effort Across the RC, and with State, Local, Tribal, and Territorial (SLTT) Governments
  - G. Section IX: RC contributions to Deterrence by Resilience
  - H. Appendices
- III. Defining Homeland Defense.....6
  - A. HD Policy Guidance, Priority Initiatives, and Threats to DCI.....6
  - B. Contested Power Projection.....8
- IV. Activating, Mobilizing, Allocating, Deploying, and Employing RC Forces for HD.....9
  - A. Activation Authorities.....9
    - 1. *Title 10 U.S.C. §§ 12304, 12304a, and 12304b (Title 10)*.....9
    - 2. *Leveraging RC and USCG Capabilities for HD Cyber Incidents*.....10
    - 3. *Title 32 U.S.C. Ch 9*.....12
  - B. Deconflicting State and Federal priorities for the use of the NG.....13
  - C. Broader factors for strengthening RC contributions to HD.....14
- V. RC Support for DCEI Resilience.....16
  - A. DCEI, Critical Defense Facilities, and unique RC support opportunities.....16
    - 1. *Include Hawaii, Alaska, Guam, and other territories in Defense-related grid resilience initiatives*.....17
    - 2. *Support power resilience for ports and transportation infrastructure*.....18
    - 3. *Clarify DoD authorities to help utilities protect the broader electric grid and supporting infrastructure*.....18
  - B. Coordinating with industry for RC support to DCEI utilities.....19
  - C. Partnering with DOE and DHS to enable DoD RC support.....20
    - 1. *RC support for information sharing and other preparedness efforts*.....20
    - 2. *RC support for emergency operations*.....21

UNCLASSIFIED

- 3. *Additional RC support options*.....23
- VI. Decision criteria to help SECDEF prioritize the activation and allocation of RC Forces and measures to enhance the value of civilian employment information to support such decision-making.....24
- VII. Strengthening HD Coordination with Federal Partners.....27
  - A. Prioritizing HD in Interagency Planning.....27
  - B. Meeting DSCA Priorities in a Contested Homeland Environment.....29
  - C. Federal Partner Support for DCI Resilience.....29
  - D. HD Exercises.....30
- VIII. Improving Unity of Effort Across the RC, and with State, Local, Tribal, and Territorial (SLTT) Governments.....32
  - A. NGB, TAGs, and Sustained Partnerships for DCI Resilience.....32
  - B. Building on NG-utility Exercises and Other State Preparedness Initiatives.....32
  - C. Strengthening Unity of Effort Across the RC: Dual Status Commanders and Beyond.....34
- IX. RC Contributions to Deterrence by Resilience.....37
- Table of Appendices.....38
  - Appendix A: Report Findings and Recommendations.....38
  - Appendix B: Recommended Tasks to Organizations.....42
  - Appendix C: Subcommittee Members Biographies .....44
  - Appendix D: Acronym List.....50



July 12, 2024


**A Letter to Secretary Austin:**


We are pleased to provide you, “Reserve Component Support to Homeland Defense (HD): *Advancing HD policy initiatives, supplementing mobilization authorities, and other measure to strengthen the DoD’s ability to use the Reserve Components (RC) to help achieve HD priorities in the 2022 National Defense Strategy (NDS).*” This comprehensive report culminates two years of extensive research and analysis with DoD stakeholders, other federal departments and agencies, and the public and private electric sector.

The report is a first in a series and focuses on RC authorities and mobilization considerations in an HD environment against the pacing challenge posed by the People’s Republic of China (PRC) targeting US infrastructure and disrupting US military preparations and response in a conflict. It demonstrates that RC personnel are uniquely well positioned to strengthen resilience stated in the NDS to “withstand, fight through, and recover quickly from disruption.” Highlighting the defense critical electric infrastructure (DCEI), the report advocates for utilizing the expertise of RC personnel who work as civilians for DCEI operators and are trained to execute Title 10, US cyber missions, to help protect the grid-provided power essential for force projection and HD missions. Future subcommittee reports will discuss maritime ports, global supply chain, transportations, water, and other sectors.

For over a century, the homeland was viewed as a sanctuary from our adversaries and attacks to our independence and freedoms. The US has not faced a major conflict on the continental homeland since the War of 1812, or on American soil since the 1943 Battle of Attu on the Aleutian Islands. USNORTHCOM and USINDOPACOM – charged to conduct homeland defense and secure the United States and its interests – have not needed to request mobilization of the military in response to a large-scale threat in the homeland. In today’s complex, multi-domain environment, it’s particularly important to refine HD plans, and enhance the readiness of the Reserve Component in order to be fully prepared to execute all HD missions. To plan and respond to current and future adversarial threats, DoD will need to adequately plan to utilize the Total Force for HD.

We look forward to discussing this report with you and our continued collaboration on its findings and recommendations.

  
Hon. Dr. Paul N. Stockton  
Subcommittee Chair  
Homeland Defense and Support  
to Civil Authorities

  
Hon. Lisa S. Disbrow  
Chair  
Reserve Forces Policy Board

## I. EXECUTIVE SUMMARY

The Reserve Component (RC) is uniquely well-positioned to help achieve the top priority of the 2022 *National Defense Strategy* (NDS): “defend the homeland” against the pacing challenge posed by the People’s Republic of China (PRC).<sup>1</sup> The Strategy warns that the PRC could target our critical infrastructure to disrupt US military preparations in a conflict and undermine the will of the U.S. public. Russia, North Korea, Iran, and other potential adversaries pose significant threats to U.S. infrastructure as well. RC personnel who are trained to execute Title 10 US Code cyber missions, and who also work as civilians for critical infrastructure operators, can use their expertise to strengthen infrastructure resilience against adversary attacks – including electric systems crucial for deploying U.S. forces to regional contingency operations.

This report proposes specific ways the DoD may utilize the RC to better “defend the homeland.” It answers why the RC is an excellent HD option and examines changes the DoD can make now to better position for success. The report more specifically demonstrates how the DoD bolsters the resilience of Defense Critical Electric Infrastructure (DCEI) that serves Critical Defense Facilities and enables power projection in a contested homeland environment.<sup>2</sup> DCEI provides an excellent basis for review given the importance of critical infrastructure and that many members of the RC work in this sector. Future reports intend to review other sectors: ports and other transportations networks; the Defense Industrial Base and global supply risk management; and water and wastewater systems.

### **Report Findings:**<sup>3</sup>

#### **A. Activating, Mobilizing, Allocating, Deploying, and Employing RC forces for HD:**

1. Current RC activation authorities and processes are complex and inadequate for time-urgent HD response missions. DoD would benefit from a legislative amendment to Title 10, authorizing RC activation for HD and the use of the full RC to conduct HD activities in a timely manner, as directed by the Secretary of Defense and as a companion statute similar to Title 32, Chapter 9 for NG HD Activities.
2. While T32/Ch 9 provides a potentially useful authority for employing the National Guard for HD missions, it does not apply to the other elements of the RC. Additional measures are needed to bring the full range of RC capabilities to bear in support of HD. Furthermore, while this statute authorizes DoD to fund NG HD activities requested by Governors, other HD missions (directed by DoD in its capacity as the Lead Federal Agency (LFA) for HD), will be essential for the military protection of

---

<sup>1</sup> 2022 *National Defense Strategy* (NDS), Department of Defense (DOD), October 27, 2022, 1-2, <https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF>

<sup>2</sup> Defense Critical Electric Infrastructure (DCEI) is defined by Section 215A, “Critical Electric Infrastructure Security,” of the Federal Power Act (FPA), codified at Title 16 U.S.C. 824o-1; <https://www.govinfo.gov/content/pkg/USCODE-2022-title16/pdf/USCODE-2022-title16-chap12-subchapII-sec824o-1.pdf> .

<sup>3</sup> Report Findings and Recommendations are provided in Appendix A.

infrastructure critical to US security. New initiatives are required to address such challenges and help de-conflict competing priorities for the use of the NG and other RC elements.

- B. RC Support for DCEI Resilience:** Substantial opportunities exist to strengthen RC support for the resilience of US utilities that operate DCEI and other infrastructure essential for HD.
- C. Decision Criteria to help SecDef prioritize Activation and Allocation of RC Forces and Enhance Decision-Making:** The existing *Civilian Employment Information Registry* does not systematically identify RC members employed as civilians in defense critical infrastructure companies and fails to specify whether they help protect infrastructure from cyberattacks or perform other essential functions in an HD environment. Such data will be crucial to help SecDef decide whether those personnel should continue to support HD in their civilian positions, versus being mobilized to execute T-10 missions.
- D. Strengthening HD Coordination with Federal Partners:** Federal D/As should have plans in place to assist DoD in HD missions related to their authorities, expertise, and industry relationships as Sector Risk Management Agencies for infrastructure critical to national security. DoD should collaborate with these partners to exercise their support plans and refine coordination mechanism to be effective “under fire” in a contested homeland environment.
- E. Improving Unity of Effort Across the RC and with State and Local, Tribal, and territorial (SLTT) governments:**
1. The National Guard Bureau (NGB) could be directed to help coordinate state NG initiatives to prepare for HD DCEI support activities.
    - o NGB should work with OUSD(P) to develop and implement sustained roles and responsibilities for the TAGs and State National Guards in supporting DCEI efforts, engagement with the states, and sustaining dialogue on Departmental priorities. In addition, TAGs should continue supporting multi-sector Defense Critical Infrastructure resilience efforts (both DoD and civilian-owned facilities) as appropriate, and closely monitor and support State level CI effort.
  2. Significant capabilities of the full RC, across all duty statuses (i.e., T10, T32, T14, SAD), will be necessary and crucial to support full mobilization (i.e., fort to port operations) and other DoD missions.
- F. RC Contributions to Deterrence by Resilience:** The NDS calls for measures to strengthen “deterrence by resilience” through coordination with the private sector and other partners to reduce the benefits that potential adversaries expect to achieve by aggressive action against the homeland.<sup>4</sup> Existing grid exercises provide the foundation on which to build such deterrence-oriented initiatives. However, such exercises are typically conducted without significant public visibility, and typically do not exploit opportunities to shape adversary perceptions.

---

<sup>4</sup> NDS, 8-9

## II. BACKGROUND OF THE REPORT

The RFPB is, by law, a federal advisory committee within the Office of the Secretary of Defense. As mandated by Congress, it “serves as an independent adviser to provide advice and recommendations directly to the Secretary of Defense on strategies, policies, and practices designed to improve and enhance the capabilities, efficiency, and effectiveness of the reserve components.”<sup>5</sup>

Over the past two years, the RFPB Subcommittee on the RCs’ Role in HD and Defense Support of Civil Authorities (DSCA) analyzed opportunities for the RC to conduct HD activities more capably, efficiently, and effectively. In particular, consistent with the priorities of the NDS and the *2023 Homeland Defense Policy Guidance*, the Subcommittee focused on strengthening RC contributions to enable force projection in a contested homeland environment and supporting the flow of forces from installations inside the US to and through US seaports of embarkation – i.e., “fort to port” operations.<sup>6</sup>

Subsequent studies by the RFPB will offer findings and recommendations for leveraging the RC in a contested homeland while projecting global power to: 1) help secure US port operations essential for power projection, in ways that leverage existing U.S. Coast Guard (USCG) security plans and capabilities and the specialized roles of the U.S. Coast Guard Reserves (USCGR); 2) more effectively manage HD-related supply chains; 3) enhance RC support for the resilience of water systems; and 4) help reduce vulnerabilities in other transportation systems sectors (aviation, highways, mass transit, pipelines, and rail) critical for Mission Assurance, homeland defense and power projection.

In conducting its research for this report, the Subcommittee received valuable insights and recommendations from senior leaders in the OSD, The Joint Staff (JS), Combatant Commands (CCMDs), The Adjutants General (TAG), Federal Departments and Agencies, and the owners and operators of DCEI and other electricity subsector organizations. The subcommittee thanks all these leaders for the time and care they took to offer their extraordinarily helpful perspectives. However, given the RFPB’s role as an independent source of advice to the Secretary of Defense, the findings and recommendations provided below are solely those of the Board.

The remainder of the report is structured as follows:

- **Section III: Defining HD.** This section identifies the statutory and policy characteristics of HD and distinguishes HD from DSCA. In order to help illuminate the key features of HD and the importance of defense critical infrastructure resilience, this section also examines a specific HD mission priority of the NDS: enabling force projection in contested homeland environment.

---

<sup>5</sup> Title 10 U.S.C. § 10301; DoD, Reserve Forces Policy Board, <https://rfpb.defense.gov/>

<sup>6</sup> The US Coast Guard (USCG) has specialized plans and capabilities to support such “military outloads” in US ports. US Coast Guard, *Office of Counterterrorism and Defense Operations Policy*, <https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Response-Policy-CG-5R/Office-of-Counterterrorism-Defense-Operations-Policy-CG-ODO/PWCS/>

- **Section IV: Activating, Mobilizing, Allocating, Deploying, and Employing RC Forces for HD.** This section offers findings and recommendations on authorities and DoD policies to mobilize and employ the RC for HD, including assistance to help non-DoD infrastructure owners and operators protect their DCI. In addition, this section examines the competition for RC resources likely to emerge in an HD environment characterized by large-scale disruptions of the electric grid and other infrastructure.
- **Section V: RC Support for DCEI Resilience.** This section analyzes opportunities for the RC to support DCEI resilience and proposes specific opportunities for collaborating with the Electricity Subsector Coordinating Council (ESCC), in close coordination with DOE and DHS.
- **Section VI: Decision Criteria to help SecDef Prioritize the Allocation of RC forces and Measures to Enhance the Value of the DoD's Civilian Employment Information Registry to Support such Decision-making.** In an HD environment, the Secretary of Defense will need to decide whether it is preferable to leave RC personnel in their civilian jobs to protect DCEI or mobilize them to perform Title 10 missions, to include National Guard personnel supporting DoD missions or operations in Title 32 status. This section recommends criteria to support the Secretary's decision-making and modifications to the Index to improve the data available to enable such decisions. The current Registry provides little data on the civilian-acquired skills and jobs that RC personnel may have in the private sector. The Registry is under-utilized and inadequate to support decision-making by the Secretary of Defense on how those personnel should best be employed in a contested homeland environment. This section recommends improvements to the Civilian Employment Information Registry to account for the data privacy and other concerns that utilities may have.
- **Section VII: Strengthening HD Coordination with Federal Partners.** Recent exercises and collaborative initiatives have helped DoD's Federal partners strengthen their awareness of their potential HD roles, including: 1) supporting DoD as the lead federal agency for HD operations, including the importance of DCI resilience; and 2) conducting their own Department-specific functions without DoD assistance when DoD is focused on a globally integrated campaign. This section offers findings and recommendations to build on this ongoing progress, including through operational planning with DoD partners and expanded HD exercises.
- **Section VIII: Improving Unity of Effort Across the RC, and with State, Local, Tribal, and Territorial (SLTT) Governments.** Many SLTT governments have little or no familiarity with HD (versus DSCA), or the impact that HD activities could have on the availability of state and territorial National Guard (NG) forces to execute high priority governor State active-duty (SAD) missions. By their very nature, TAGs provide SLTT awareness of and preparedness for crises, including HD. TAGs may also provide connectivity with DCI operators and SLTT governments in support of DoD resilience priorities. This section offers recommendations to authorize Dual Status Commanders (DSC) to coordinate HD activities across the Total Force, and with relevant CCMDs and SLTT governments.



## UNCLASSIFIED

- **Section IX: RC Contributions to Deterrence by Resilience.** To contribute to deterrence, RC initiatives must not only help utilities strengthen the survivability of their infrastructure, but also do so in ways that help shape adversary perceptions of US resilience. This section offers recommendations to help do so and thereby strengthen deterrence by resilience.
- **Appendix A: Report Findings and Recommendations.**
- **Appendix B: Recommended Tasks to Organizations.** Conducting HD operations, while also conducting global power projection, will tax the ability of DoD to sustain such operations in a protracted conflict. This section offers recommendations for DoD stakeholders on potential tasks to strengthen preparedness for executing HD missions.
- **Appendix C: Subcommittee Biographies**
- **Appendix D: Report Acronyms**
- **Appendix E: Subcommittee's Report Presentation for March 6, 2024 RFPB Meeting**

### III. DEFINING HOMELAND DEFENSE

Joint Publication (JP) 3-27, *Joint Homeland Defense*, defines HD as “the military protection of United States sovereignty and territory against external threats and aggression or, as directed by the President, other threats.” JP 3-27 also specifies that “DoD leads HD missions and may be supported by other USG departments and agencies while conducting such missions.”<sup>7</sup>

These characteristics sharply differentiate HD from DSCA. DoD is the lead Federal agency (LFA) for HD, as specified in JP 3-27. In contrast, DoD supports the Federal Emergency Management Agency (FEMA) or other civilian departments and agencies (D/As) for DSCA operations, as approved by the Secretary of Defense.<sup>8</sup> Whereas DSCA has evolved and matured with formal processes and guidance for habitual support to the LFA, DoD lacks guidance for civilian agency support for HD activities and other DoD missions. This reversal of traditional supported/supporting relationships between the military and civilian organizations has profound implications for government coordination and for prioritizing DoD operations, especially in the face of disruptive cyber and other attacks that create competing demands for DoD resources.

Another key difference lies in the level of experience of DoD, the RC, and their partners in conducting DSCA versus HD operations. For decades, DoD, with the use of RC assets, has repeatedly conducted DSCA activities, through a request for assistance (RFA) process that is well understood and frequently used by DoD, FEMA, and other Federal departments and agencies. DoD does not have equivalent experience in conducting HD activities, including those in which the RC would also support power projection or other Defense missions in a contested homeland environment. Additionally, DoD's partners do not have experience supporting DoD HD activities, contested power projection, or other defense missions. The absence of HD experience is primarily due to the successful global national security efforts that decreased the demand signal for HD activities. However, risks to the homeland have significantly changed in today's multi-domain environment, and adversaries are now preparing to conduct cyberattacks against defense critical infrastructure and other targets on US territory.

Furthermore, DoD must be able to “get it right” the *first time* the US conducts HD operations, especially during a crisis with the People's Republic of China or other potential adversaries. Employing the RC to support the defense of the homeland will require DoD and its partners to develop and exercise plans and coordination mechanisms far beyond those that exist today.

#### **A. HD Policy Guidance, Priority Initiatives, and Threats to DCI**

DoD's *2023 Homeland Defense Policy Guidance Fact Sheet* provides an essential starting point for prioritizing RC initiatives for HD. The Guidance “identifies initiatives that contribute to the Department's ability to project power, defend the homeland, and in the event of a conflict, maintain continuity of wartime operations.”<sup>9</sup> One priority initiative is: “focus on *defending defense critical infrastructure* against attacks in all domains and build resiliency and redundancy

<sup>7</sup> Joint Publication (JP) 3-27, *Joint Homeland Defense*, DoD, 12 December 2023, GL-5, A-1

<sup>8</sup> Details on DSCA operations, approval criteria, and related issues are provided in *Joint Publication (JP) 3-28, Defense Support of Civil Authorities*, October 29, 2018; [https://jdeis.js.mil/jdeis/new\\_pubs/jp3\\_28.pdf](https://jdeis.js.mil/jdeis/new_pubs/jp3_28.pdf)

<sup>9</sup> *Fact Sheet: 2023 Homeland Defense Policy Guidance*, DoD, February 21, 2024; <https://media.defense.gov/2024/Feb/21/2003397767/-1/-1/1/FACT-SHEET-2023-HOMELAND-DEFENSE-POLICY-GUIDANCE.PDF>

## UNCLASSIFIED

to fight through disruptions and maintain the ability to mobilize and respond to crisis or conflict. [emphasis added]”<sup>10</sup> This report is aligned with the Guidance’s focus on defense critical infrastructure, with a specific emphasis on strengthening RC support for the resilience of DCEI.

DCEI and other DCI will be vital for supporting multiple HD missions, including port to port operations. In future confrontations, adversaries are likely to target DCI to disrupt HD mission execution and DoD mission assurance. The 2024 Annual Threat Assessment issued by the ODNI highlights the challenges confronting the owners and operators of DCI and DCEI, and the imperative to bolster infrastructure resilience. A key finding of the Assessment:

If Beijing feared that a major conflict with the United States were imminent, it would consider undertaking aggressive cyber operations against U.S. critical infrastructure and military assets. Such a strike would be designed to deter U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces.<sup>11</sup>

To prepare for such disruptive attacks, the PRC is ramping up its campaign to embed compromises in US infrastructure and control system for exploitation in future crises. The Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) issued a series of alerts in 2023-2024 concerning such operations and the increasing severity of the threats they pose. Specifically, Brandon Wales, executive director of the CISA, stated:

“It is very clear that Chinese attempts to compromise critical infrastructure are in part to pre-position themselves to be able to disrupt or destroy that critical infrastructure in the event of a conflict, to either prevent the United States from being able to project power into Asia or to cause societal chaos inside the United States — to affect our decision-making around a crisis.”<sup>12</sup>

In addition, FBI Director Christopher Wray recently highlighted the severity of PRC threats to US infrastructure, and the imperative to strengthen the resilience against potential cyberattacks:

There has been far too little public focus on the fact that PRC [People’s Republic of China] hackers are targeting our critical infrastructure—our water treatment plants, our electrical grid, our oil and natural gas pipelines, our transportation systems—and the risk that poses to every American requires our attention now. China’s hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities. If or when China decides the time has come to strike, they’re not focused solely on political or military targets. We can see from where they position themselves,

---

<sup>10</sup> Id.

<sup>11</sup> *Annual Threat Assessment of the U.S. Intelligence Community*, Office of the Director of National Intelligence, February 5, 2024, 11; <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf>

<sup>12</sup> *China’s Cyber Army is Invading Critical US Services*, Ellen Nakashima and Joseph Menn, Washington Post, December 11, 2023; <https://www.washingtonpost.com/technology/2023/12/11/china-hacking-hawaii-pacific-taiwan-conflict/>

across civilian infrastructure, that low blows aren't just a possibility in the event of a conflict. Low blows against civilians are part of China's plan.<sup>13</sup>

## **B. Contested Power Projection**

For DoD Mission Assurance and HD, the threat to fort to port operations and supporting infrastructure poses an especially significant challenge. The former Commanders of U.S. Northern Command (USNORTHCOM) and U.S. Transportation Command (USTRANSCOM) noted that DoD heavily depends on domestic infrastructure to deploy and support forces for regional contingencies. These Commanders also cautioned “Over the past two decades, strategic competitors have observed our preferred way of conducting military operations — the away game through deliberate power projection from the homeland — and they have invested heavily in capabilities to hold our homeland at risk to delay or disrupt military force flow or to destroy the will of the people.”<sup>14</sup>

The U.S. electric utilities that help power DoD fort-to-port operations are aggressively strengthening the resilience of their networks, infrastructure, and operations, with the help of the Department of Energy (the Sector Risk Management Agency for Energy) and other partners. Nevertheless, significant opportunities exist to strengthen government-industry collaboration for DCEI resilience, including by leveraging the expertise and connectivity of personnel employed by DCEI utilities who are also part of the Ready Reserve. The remainder of this report offers specific recommendations to do so, together with broader initiatives to strengthen RC contributions to homeland defense.

Yet, all such RC support will depend on the adequacy and timeliness of DoD authorities to activate, mobilize, deploy, and employ the RC in future crises. The ability of the RC to help infrastructure owners and operators defend their assets also depends on new and broader DoD authorities to provide such assistance (which will be addressed later in this report). Both sets of authorities have gaps and ambiguities that DoD should become readily cognizant of and immediately move to remedy.

---

<sup>13</sup> *Director Wray's Opening Statement to the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party*, FBI, January 31, 2024; <https://www.fbi.gov/news/speeches/director-wrays-opening-statement-to-the-house-select-committee-on-the-chinese-communist-party>

<sup>14</sup> *Fighting to get to the Fight*, Glen D. VanHerck and Jacqueline D. Van Ovost, *Military Times*, May 31, 2022; <https://www.militarytimes.com/opinion/commentary/2022/05/31/fighting-to-get-to-the-fight/>

## IV. ACTIVATING, MOBILIZING, ALLOCATING, DEPLOYING, AND EMPLOYING RC FORCES FOR HD

### A. Activation Authorities

The statutes that authorize the utilization of the RC for HD missions are far reaching, but also inadequate for meeting current and emerging HD requirements. Two provisions of law are especially significant for the homeland: Title 10 U.S.C § 12304, and Title 32 U.S.C. Chapter 9.<sup>15</sup>

#### *1. Title 10 U.S.C §§ 12304, 12304a, and 12304b (Title 10)*

Under Title 10 U.S.C § 12304, DoD may access the RC:

... when the President determines that it is necessary to augment the active forces or that it is necessary to provide assistance referred to in subsection (b) [in responding to an emergency involving - (1) a use or threatened use of a weapon of mass destruction; or (2) a terrorist attack or threatened terrorist attack in the United States that results, or could result, in significant loss of life or property], he may authorize the Secretary of Defense and the Secretary of Homeland Security with respect to the Coast Guard when it is not operating as a service in the Navy, without the consent of the members concerned, to order any unit, and any member not assigned to a unit organized to serve as a unit of the Selected Reserve (as defined in section 10143(a) of this title), or any member in the Individual Ready Reserve mobilization category and designated as essential under regulations prescribed by the Secretary concerned, under their respective jurisdictions, to active duty for not more than 365 consecutive days.<sup>16</sup>

If properly utilized, the provision of 10 U.S.C. § 12304 can be a valuable tool in campaigning and enable timely RC timely access. DoD's access to the RC under 10 U.S.C. § 12304(a) or (b) requires approval by the President, as provided (generally) in a Presidentially-issued Executive Order (EO), or in response to certain emergencies, e.g., use of weapons of mass destruction (WMD), in circumstances other than war.

Nevertheless, 10 U.S.C. § 12304 is not fully adequate to meet potential RC mobilization needs in a contested homeland environment. One shortfall lies in ensuring rapid RC access for urgent, time-sensitive HD missions. RC units will require significant time to muster, train, and mobilize for HD operations. Indeed, mobilization of the RC under 12304 will take days - if not weeks or months - for integration and onward movement before reaching their final destinations.

---

<sup>15</sup> Other RC access authorities, include:

- Title 10 US Code § 12301(d) permits Service Secretaries to order RC members to active duty on a voluntary basis. However, it is utilized as a limited stopgap measure. It does not provide long-duration RC access nor sufficient number of personnel in a timely manner.
- Title 10 U.S.C. § 12302 provides for the "Partial Mobilization" of the RC. This authority applies in time of national emergency declared by the President, and only applies only to the Ready Reserve (comprised of the Selected Reserve, the IRR, and the ING), with a maximum of 1,000,000 Ready Reserve members able to be mobilized at any one time.

<sup>16</sup> Title 10 U.S.C. 12304, (amended P.L. 118-31, Dec. 22, 2023);

<https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section12304&num=0&edition=prelim>

## UNCLASSIFIED

An additional concern is the possibility that mobilization under 10 U.S.C. § 12304 could be perceived by senior U.S. officials as escalating a crisis, and therefore less attractive as a policy option. To address these potential perceptions, DoD could regularly and routinely mobilize RC units under 12304 for HD training and other activities during steady state operations, and thereby normalize such mobilizations.

Another shortfall of 12303 lies in the limited range of contingencies in which it can be employed, including specified types of emergencies and emergencies and WMD or terrorist attacks. According to statute and pursuant to DoDI 1235.12, *Accessing the Reserve Components*, RC forces may be accessed for actual or threatened WMD or terrorist attacks under 12304(b). The limitations of use or threatened use of WMD and to terrorist attacks (or threatened terrorist attacks) may not encompass Nation State attacks or gray-zone attacks which are neither WMD nor terrorist attacks to the Homeland, and which would likely coincide with global attacks elsewhere. Furthermore, RC mobilizations for HD operations may also cause downstream complications for the availability of forces for the Global Force Management (GFM) process.

Other authorities to access the RC for Active Duty, 12304a and 12304b, do not fully remedy these problems, and entail further impediments to the rapid mobilization of the RC. Title 10 U.S.C. § 12304a provides DoD access to the RC in response to a major disaster or emergency defined by the Robert T. Stafford Disaster Relief and Emergency Assistance Act.<sup>17</sup> Under 12304a, access to the Army Reserve, Navy Reserve, Marine Corps Reserve, and Air Force Reserves is limited for DSCA activities-only, which is not HD. This authority is also limited to a continuous period of not more than 120 days, and, most importantly, does not provide access to the NG or USCGR, both of which will be crucial for supporting fort to port operations.<sup>18</sup>

Title 10 U.S.C. § 12304b provides secretaries of the MILDEPs with access to RC units. However, their access to the RC is limited to support of *preplanned missions* in support of CCMDs. Similar to the prior constraint with “*named operations*” that existed under 12304, RC support under 12304b for preplanned missions will not be available for emergent HD missions. As such 12304b does not adequately address RC access for HD operations especially within CONUS, and where RC will be needed in response to an emergent operation to support force projection in a contested homeland environment.

### ***2. Leveraging RC and USCG Capabilities for HD Cyber Incidents***

The National Defense Authorization Act for Fiscal Year 2024, Sec 1532, amended Title 10 U.S.C § 12304 and added authority for DoD to order reserves to active duty to respond to a significant cyber incident.<sup>19</sup>

Subsection 12304(c) is especially pertinent for enabling the RC and USCG to support such cyber-related operations particularly for HD. That Subsection, titled “AUTHORITY RELATING TO SIGNIFICANT CYBER INCIDENTS,” provides that:

---

<sup>17</sup> Title 42 U.S.C. § 5122

<sup>18</sup> Title 14 U.S.C. § 3713 provides access to USCGR units and personnel to augment the Regular USCG to aid in prevention of and response to an imminent, serious natural or manmade disaster, accident, catastrophe, act of terrorism, or transportation security incident.

<sup>19</sup> National Defense Authorization Act for Fiscal Year 2024, PL 118-31, December 22, 2023.

## UNCLASSIFIED

When the Secretary of Defense or the Secretary of the department in which the Coast Guard is operating determines that it is necessary to augment the active armed forces for the response of the Department of Defense or other department under which the Coast Guard is operating, respectively, to a covered incident, such Secretary may, without the consent of the member affected, order any unit, and any member not assigned to a unit organized to serve as a unit of the Selected Reserve (as defined in section 10143(a) of this title), under the respective jurisdiction of such Secretary, to active duty for not more than 365 consecutive days.

This provision, however, limits the number of Selected Reserve and Individual Ready Reserve (IRR) called upon to 200,000 members at any one time, of whom no more than 30,000 may be members of the IRR. Importantly, while this provision opens availability to access the RC for HD operations, it is limited to cyber incidents involving DoD or DHS information systems or a breach of said systems involving personally identifiable information, unless determined by the President that - the cyber incident, or series of incidents, is likely to result in demonstrable harm to national security interests, foreign relations, or the economy of the US, or to public confidence civil liberties, or public health and safety of the people of the US.<sup>20</sup>

DoD has yet to develop policies to implement this authority. Notwithstanding, one potential gap with this new authority involves the parameter for the Secretary of Defense to access DoD RC and the Secretary of Homeland Security to access the U.S. Coast Guard Reserve to defend against or respond to significant cyber incidents that may result in demonstrable harm to national security for incidents other than those involving their respective information systems.

The “triggers” for SecDef use of this activation authority are:

1. SecDef determines a cyber incident involving a DoD information system, or a breach of a DoD system that involves PII, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the people of the United States;
2. The President determines that a cyber incident, or collection of related cyber incidents, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States;
3. The Secretary of Homeland Security determines a cyber incident involving a DHS information system, or a breach of a DHS system that involves personally identifiable information, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States; or

---

<sup>20</sup> Title 10 U.S.C. 12304(k) defines a “covered incident” as a cyber incident involving DoD or DHS information system, or a breach of said system that involving personally identifiable information, that the Secretaries involved determine is likely to result in demonstrable harm to national security interests, foreign relations, or the economy of the US, or to public confidence civil liberties, or public health and safety of the people of the US.

4. The Secretary of Homeland Security declares a "significant incident" IAW the Cyber Response and Recovery Act (section 2233 of the Homeland Security Act of 2002 (6 U.S.C. § 677b)).

Accordingly, while SecDef clearly has the authority to active the RC for a significant cyber incident affecting DoD, SecDef's discretion to use this authority in other scenarios depends on determinations by the President or the Secretary of Homeland Security. Therefore, this authority may not be available to support DoD cyber-related HD missions not involving DoD systems, including HD missions involving non-DoD-owned DCI.

In addition to DSCA, this authority may be beneficial in supporting HD and Defend Forward missions. Moreover, this provision could be enormously helpful for the "port" component of fort to port operations. Subsequent reports to be issued by the HD Subcommittee will offer detailed findings and recommendations on such USCG contributions to HD.

### 3. Title 32 U.S.C. Ch 9

One specific authority under Title 32 of the US Code - Title 32 U.S.C. Chapter 9 (T32/Ch 9) - provides access to the NG for HD activities. While T32/Ch 9 provides valuable provisions for DoD to fund and employ the NG for HD activities, gaps remain within the whole of DoD HD missions at the national strategic level. Under T32/Ch 9, the Secretary of Defense may provide funds to a Governor to employ NG units or members [as full-time NG duty under section 502(f)] to conduct HD activities that the Secretary determines to be necessary and appropriate for participation by the NG units or members, as the case may be. As defined by this statute, an HD activity is:

an activity undertaken for the military protection of the territory or domestic population of the United States, or of infrastructure or other assets of the United States determined by the Secretary of Defense as being critical to national security, from a threat or aggression against the United States.”<sup>21</sup>

Under T32/Ch 9, DoD may fund the HD activities of the of the NG at the direction of a Governor. Activation of the NG for HD would occur under T32 USC 502(f).<sup>22</sup> However, to date, DoD has not approved a request for DoD funding of NG HD activities under T32/Ch 9, and multiple significant attacks may spur multiple Governor requests for DoD funding of National Guard HD activities. Moreover, the Secretary of Defense can also request that the Governor employ the National Guard for HD activities, thereby, further increasing the demand for the NG.

---

<sup>21</sup> Title 32 U.S.C. § 901

<sup>22</sup> DoD policy provides some principal-level guidance for NG HD activities. DoDD 3160.01, *Homeland Defense Activities Conducted by the National Guard*, implements sections 901-908 of T32/Ch9 to include assigning responsibilities for requesting funding and employment of the National Guard to conduct HD activities.<sup>22</sup> This directive proscribes responsibilities such as developing, coordinating, and issuing policy guidance, and overseeing policy implementation for NG HD activities. It also provides review processes for HD requests to include determining if an actual or credible threat exists to the US and whether the HD activity is for the protection of infrastructure or assets critical to national security; or whether the performance of the HD activity adversely impacts training or readiness or degrades military skills. Additionally, the directive requires COCOMS CCMDs, CNGB, and Governors to ensure the NG HD funded activity does not conflict with ongoing Federal missions.



The President or the Secretary of Defense may also request under 32 U.S.C. § 502(f)(2)(A) and per regulations prescribed by the Secretary of the Army or Secretary of the Air Force, for NG units to support of DoD “operations or missions,” which may include HD.

However, fort to port operations provide a case in point where large-scale HD operations may require the entire RC, not limited primarily to the NG. To mobilize, gather, and deploy forces from the interior of the US to and through ports of embarkation, and mitigate the effects of infrastructure attacks targeted to delay and disrupt such operations, the entire RC, including multiple state NGs, and their infrastructure partners will likely play crucial roles in facilitating force movements.

In theory, multiple Governors and TAGs could, and will likely, employ their own NG under SAD to protect DCEI, and other State assets, in their state that are essential for the moving forces from installations in the interior of the U.S. to (and through) U.S. ports of embarkation. In practice, however, state-to-state HD funding requests for NG employment under T 32/Ch 9 would be cumbersome and untimely to provide immediate response to HD attacks. It would be far more efficient and effective for HD missions to be centrally coordinated by appropriate CCMDs, the JS, NGB, and OSD. The Report’s Appendix offers recommendations on how to structure DoD-led coordination of state NGs and other reserve components to execute HD activities, including utilization of Dual Status Commanders (DSCs).<sup>23</sup>

## **B. Deconflicting State and Federal priorities for the use of the NG**

When threats or aggression against the United States require the military protection of the population of the United States, or of infrastructure determined by the Secretary of Defense as being critical to national security, the Secretary may decide to use NG personnel for HD missions, including by providing funding for NG HD activities under T32/Ch 9, to meet those challenges. At the same time, however, the large-scale disruption of the U.S. grid, water systems, and other US infrastructure will also pose urgent threats to public health and safety – all of which will be of intense concern to Federal leaders, Governors, and other SLTT leaders.

The net effect: multiple, simultaneous demands will emerge for utilizing the RC in a contested environment. These missions include:

- DoD-directed Federal overseas T-10 contingency operations;
- DoD-directed Federal T-10 HD operations;
- State-directed, DoD-authorized and funded T-32 NG HD activities; and
- DoD-directed T-10 DSCA missions in response to requests for assistance from FEMA, or other Federal civilian authorities to help save and sustain lives, including measures to

---

<sup>23</sup> A Dual Status Commander (DSC) is an officer of the Army National Guard (ARNG), Air National Guard (ANG), commissioned officer of the Regular Army or Regular Air Force who has completed specialized training and certification. DSCs are jointly managed by the commander of U.S. Northern Command and the chief of the National Guard Bureau and may, by law, serve in two statuses (federal and state) simultaneously. *Dual Status Commander Fact Sheet*, National Guard Bureau; [https://www.nationalguard.mil/Portals/31/Resources/Fact%20Sheets/DSC%20Fact%20Sheet%20\(Nov.%202020\).pdf](https://www.nationalguard.mil/Portals/31/Resources/Fact%20Sheets/DSC%20Fact%20Sheet%20(Nov.%202020).pdf)

mitigate the effects of cyber-induced disruptions of electric service to hospitals, water systems, or other critical civilian facilities.

Consistent with first priority that the NDS assigns to defending the homeland, this report assumes that T-10 and HD missions will take precedence over the use of the NG for DSCA operations, even if wide-area attacks are underway against critical infrastructure. DoD may need to collaborate with FEMA and SLTT leaders to develop planning factors for HD missions as well as prioritize and determine the potential availability of the NG for DSCA missions in such an environment. This describes a “simultaneity challenge” between: (1) DoD’s overseas contingency operations and HD operations versus DSCA; and (2) DoD’s operational missions versus State operational missions. Accordingly, DoD and its partners should also develop an HD decision support framework to assist DoD and the President’s decisions to allocate scarce RC resources, in ways that account for increasingly severe threats to the homeland and to defense critical infrastructure.

Nevertheless, while HD will take priority over other DSCA in a contested homeland environment, the President ultimately determines the priority for employing DoD forces. Under extraordinary circumstances, the President could direct that a DSCA mission will take precedence over other DoD missions, as occurred in 2012 during Superstorm Sandy. DoD should account for that possibility in its HD plans, including the potential need to source personnel from other RC or the AC to help perform HD missions when the AC and RC are executing Presidentially directed DSCA operations or other missions. OSD should also consult with Governors via the Council of Governors to discuss challenges of simultaneity and implications for NG and RC force allocation.

In addition, DoD faces the risk that RC assets might be double, or triple counted - creating a “simultaneity gap” - in conflicts that involve simultaneous overseas contingency and homeland defense operations (e.g., support for global campaigns, OPLAN, SD-approved DSCA and utility support operations). DoD should assess these risks and develop plans for mobilizing and allocating RC personnel that realistically account for force availability in a multi-mission environment.

### **C. Broader factors for strengthening RC contributions to HD**

T32/Ch 9 applies only to the NG. Yet, other components of the RC can make immensely valuable contributions to HD. Currently, Title 10 does not include direct authority for the utilizing the Army Reserve, Air Force Reserve, Navy Reserve, the Marine Corps Reserve, or the Coast Guard Reserves for *specific* HD missions. DoD should assess whether gaps exist in activation authorities and plans for utilizing the specialized HD capabilities of these RC elements, including for support for fort to port operations and DCI resilience.

To align with the 2022 NDS, DoD should also update its Total Force Policies to ensure that the Department can adequately plan, program, and budget DoD’s mission assurance in a contested homeland and ensure the Joint Force gets to the fight. DoD needs to recognize the challenges of mobilizing RC personnel to defend the homeland and critical infrastructure. With the re-emergence of the RC’s importance as strategic reserve with continued operational function, updated DoD guidance and policy will be necessary to define DoD roles in defense of the

## UNCLASSIFIED

homeland's critical infrastructure, assess anticipated DoD HD and DSCA missions in a contested homeland, evaluate potential RC contributions to such roles and missions, and recommend appropriate allocation and of RC personnel.

### *FINDINGS:*

- Current activation authorities and processes to access the RC are complex and inadequate for performing time-urgent HD response missions. For immediate and more efficient mobilization of the RC for emergent HD, DoD would benefit by seeking a legislative amendment to Title 10, authorizing RC activation for HD and the use of the entire RC to conduct HD activities in a timely manner, as directed by the Secretary of Defense as a companion statute similar to Title 32, Chapter 9 for NG HD Activities.
- While T32/Ch 9 provides a potentially useful authority for employing the NG for HD missions, it does not apply to the other elements of the RC. Additional measures will be needed to bring the full range of RC capabilities to bear in support of HD. Furthermore, while this statute authorizes DoD to fund NG HD activities requested by Governors, other HD missions (directed by the DoD in its capacity as the Lead Federal Agency (LFA) for HD), will be essential for the military protection of infrastructure critical to US security. New initiatives will be required to address such challenges and help de-conflict competing priorities for utilizing the NG and other RC elements.

### *RECOMMENDATIONS:*

- Review HD policy and statutes for HD sufficiency to include Title 10 U.S. Code 12304. Develop policy and legislative proposals for Congress to supplement DoD Title 10 mobilization authorities for the RC, including 1) immediate mobilization for HD missions for the whole of the RC, and 2) standing mobilization orders for preplanned HD missions.
- Propose an amendment to Title 10 U.S.C. to authorize the use of the full RC to conduct HD activities, as directed by the Secretary of Defense.
- Use the Council of Governors to build consensus with States on criteria, processes, and consultative mechanisms to de-conflict competing Federal and State priorities for using the NG and, as applicable, other RC elements to conduct homeland defense activities.

## V. RC SUPPORT FOR DCEI RESILIENCE

For many decades, the RC has helped utilities restore power following hurricanes and other natural disasters at the direction of DoD as part of a DSCA mission or, in the case of the NG, at the direction of a State Governor. DoD support missions may include debris removal, security and transportation assistance, and other tasks. State NG organizations are also increasingly developing partnerships with utilities to support post-cyberattack power restoration when NG personnel serve in a SAD status. As one example, the Virginia NG participated in Cyber Fortress (2022) with participants from Dominion Energy, the Virginia Department of Emergency Management, the Virginia Department of Information Technology, the Virginia State Police and other local, state, and federal organizations.<sup>24</sup> Moreover, under the leadership of the DOE, DoD is partnering with DOE and DCI pilot programs in a growing number of states focused on strengthening cyber defenses for utility infrastructure and planning for the prioritized restoration of power to critical defense facilities.

However, no database adequately quantifies the number of state NG partnerships with utilities. The NGB should develop such a database with ongoing and proposed partnerships with states and utilities. NGB should also develop an assessment of emerging best practices to develop future initiatives, in coordination with TAGs.

The RC has unique capabilities to support such efforts across a broad range of resilience activities. The NDS defines resilience as “the ability to withstand, fight through, and recover quickly from disruption.”<sup>25</sup> The RC can significantly assist utilities that own and operate DCEI in each of these categories “left, during, and right of boom.” However, specialized plans and coordination mechanisms will be required to enable such support and help electricity utilities sustain the flow of power essential for to support power projection in a contested homeland environment.

### **A. DCEI, Critical Defense Facilities, and unique RC support opportunities**

Ensuring the flow of grid-provided power to Critical Defense Facilities (CDFs) constitutes a core requirement for power projection. As defined by Sec 215A of the Federal Power Act, CDFs are 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.”<sup>26</sup> In turn, DCEI constitutes “any electric infrastructure that serves” CDFs.<sup>27</sup> The Responsible Utilities (RUs) that operate DCEI will be especially important partners for DoD in strengthening mission assurance.

RC personnel who are employed in their civilian roles by RUs are well-positioned to help strengthen such mission-critical grid resilience and can contribute to properly developed requests for assistance for RUs in a number of ways.

---

<sup>24</sup> *Virginia Guard, Partners Conduct Cyber Exercise*, October 24, 2022;

<https://www.nationalguard.mil/News/Article/3196964/virginia-guard-partners-conduct-cyber-exercise/>

<sup>25</sup> NDS, 8

<sup>26</sup> Title 16 U.S.C. §824o-1. Critical electric infrastructure security,

<https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title16-section824o-1&num=0&edition=prelim>

<sup>27</sup> *Id.*

- In their civilian jobs as RU employees, RC personnel may be trusted agents of their utilities. These employees acquire an in-depth knowledge of their utilities' networks, operations, cyber protections, and/or power restoration plans. Their RU-specific expertise makes these RC personnel especially useful for planning, exercising, and (if attacks are underway) identifying potential support options to help protect or restore the flow of power to Critical Defense Facilities and to other customers essential for HD.
- Provide opportunities to assign properly-trained RC employees of an RU, who are familiar with RC support capabilities that can be brought to bear, to assist in response to a civil authority's RFAs. Specifically, an RC employee of the RU may be able to translate the RU's support requirements into the RC unit's military-business processes, and align support requests with the DSCA RFA system (modified as necessary for HD support). Emerging threats to the electricity sector increase new vulnerabilities to the RUs that previously were not known or did not exist. The RUs now require assistance and support that were not previously needed. RC efforts can ultimately expedite the delivery of urgent-needed resources down to the tactical level, as approved by the Secretary of Defense.
- RC personnel who are employees of RU responsible for cybersecurity may also (when mobilized for T-10 duty) serve in the Cyber National Mission Force (CNMF) or other DoD components. The training and skills they acquire to perform their T-10 missions could be of significant value in strengthening the resilience of DCEI networks, operations, and infrastructure against cyberattacks, and vice versa.

In addition to RUs employing individual RC personnel, a growing number of State NG, U.S. Army, Navy, Air Force, and Marine Corps Reserve units are developing close collaborative relationships with utilities in their states and conduct resilience exercises with them, together with SLTT government officials. As in the 2022 Cyber Yankee, such exercises increasingly involve multistate coordination of cyber response operations.<sup>28</sup> A number of initiatives could help DoD and its partners build on these foundations.

### ***1. Include Hawaii, Alaska, Guam, and other territories in Defense-related grid resilience initiatives***

The term DCEI, as defined by the Federal Power Act, applies only to "electric infrastructure located in any of the 48 contiguous States or the District of Columbia."<sup>29</sup> That definition excludes the infrastructure that serves defense facilities in Hawaii, Alaska, and Guam, all of which may be vital for executing USINDOPACOM plans. DoD should remain cognizant of this gap and, distinct from DCEI-specific initiatives, partner with DOE to help strengthen the resilience of utilities in those states and territories essential for INDOPACOM power projection.

---

<sup>28</sup> John Randall, "Cyber Yankee 2022 Underway," *Defense Visual Information Distribution System*, June 10, 2022; <https://www.dvidshub.net/news/422723/cyber-yankee-2022-underway>

<sup>29</sup> Federal Power Act, section 215(A)(a)(4); [https://www.ferc.gov/sites/default/files/2021-04/federal\\_power\\_act.pdf](https://www.ferc.gov/sites/default/files/2021-04/federal_power_act.pdf)

## ***2. Support power resilience for ports and transportation infrastructure***

The nature of port to port operations will also require expanded outreach to non-Defense power customers. Civilian-operated ports that serve as seaports of embarkation may not necessarily be classified as CDFs. The same is true of the multimodal transportation systems and supporting infrastructure necessary to move forces and other assets from Defense installations to those SPODs. To identify priorities for grid support in a contested homeland environment, DoD will need to “disaggregate” missions and account for the flow of forces ISO OPLANS. That disaggregation process is already underway. Under DoD’s *Mission Assurance Construct Implementation* initiative, Defense Components are identifying MA requirements for CCMD campaign plans, OPLANS, concept plans (CONPLANS), and core joint mission essential tasks (JMETs).<sup>30</sup> These efforts will support broader work to strengthen the resilience of Defense Critical Infrastructure essential to mission assurance and OPLAN execution. However, as applied to DCEI, DoD and its partners (especially DOE) will need to address two key issues as discussed below.

## ***3. Clarify DoD authorities to help utilities protect the broader electric grid and supporting infrastructure***

Broader challenges exist for ensuring the availability of electricity for HD missions. DoD provides support to DOE pilot programs to strengthen DCEI resilience, and – as suggested above – should expand that support to utilities that serve ports and other facilities vital for power projection that may not constitute CDF. DCEI resilience significantly depends on the resilience of multiple components of the electricity subsector, including electric power generation, transmission, and distribution owners and operators. For example, without adequate power generation, the grid will lack the capacity necessary to serve CDFs. It is prudent to assume that adversaries understand these gaps in the vital national security role of bulk power system generators and will target them for cyberattack accordingly.<sup>31</sup>

Of course, not every grid infrastructure is equally vital to successful HD mission execution, and DoD resources, including the RC, available to support utility resilience are limited. DoD should continue to partner with DOE, its National Laboratories, and other research institutions to identify the electric infrastructure most vital for executing HD and OPLANS, and prioritize DoD support to subsector entities accordingly.<sup>32</sup> Over time, such efforts should also address the grid’s dependencies on the flow of natural gas for power generation and other supporting infrastructure. In addition, DoD should clarify its authorities to assist asset owners and operators with protecting their infrastructure that is mutually beneficial to DoD, beyond the narrow definition of DCEI in the Federal Power Act, and – if necessary – propose legislation to fill gaps that exist.

---

<sup>30</sup> Joint Staff, *Mission Assurance Construct Implementation*, August 23, 2023; [https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%203209.01A%20\(JS-221219-T8WP\)%20VDJS%20Signed.pdf](https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%203209.01A%20(JS-221219-T8WP)%20VDJS%20Signed.pdf)

<sup>31</sup> The bulk power is comprised of: (A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (B) electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy. North American Electric Reliability Corporation, *Glossary of Terms*, December 1, 2023, 9; [https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary\\_of\\_Terms.pdf](https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf)

<sup>32</sup> The Critical Infrastructure Defense Analysis Center (CIDAC), discussed in Section VII, will also play a valuable role in assessing these interdependencies.

## **B. Coordinating with industry for RC support to DCEI utilities**

The best way for the designated DoD HD lead to engage with the electricity subsector is via the ESCC, in close coordination with DOE and DHS. The ESCC is the principal liaison between the electric sector and the federal government, coordinating efforts to prepare for and respond to national-level disasters or threats to critical infrastructure. As the primary stewards of the energy grid, ESCC members are at the forefront of national security and resilience. The ESCC coordinates emergency response efforts following natural disasters and malicious attacks, facilitates critical conversations on detecting and mitigating of threats to the energy grid, and supports initiatives that improve the sector's overall security and resilience posture. The ESCC membership consists of CEOs and senior executives from investor-owned electric companies, municipal and public power utilities, electric cooperatives, and their respective trade associations to represent all industry segments and reflect the diverse voices of energy grid asset owners and operators.<sup>33</sup>

The ESCC's Cyber Mutual Assistance (CMA) program offers an especially promising opportunity for RC-industry collaboration.<sup>34</sup> This program offers a framework for electric companies to assist each other in preparing for or responding to outages or disruptions to operations caused by cyber means. This framework has been expanded to include owners and operators of natural utilities, including those that serve Defense installations. The designated DoD HD lead should coordinate with CMA representatives to explore how the RC might help DoD (e.g., USNORTHCOM or USINDOPACOM) requests for forces within this framework and identify specific priorities for RC assistance.

Collaborating with the ESCC will also help DoD achieve systematic, integrated outreach to the diverse components of the electricity sector that DoD depends on and is essential to HD operations. A range of components of the electricity subsector play vital roles in supporting DoD mission execution, including municipal/public power utilities, rural electric cooperatives, and investor-owned utilities (IOUs). Representatives of each of these components currently participate in the CMA program.

In addition, independent power producers generate much of the electricity that these utilities deliver to CDFs. Reliability Coordinators, Regional Transmission Operators (RTOs), Independent System Operators (ISOs) and other Bulk Power System entities also play critical roles in maintaining reliable service to CDFs and in responding to cyber-induced disruptions. Coordination with representatives of these subsector components is essential to ensure that industry priorities, operational considerations, and coordination mechanisms inform DoD and its energy sector partners.

---

<sup>33</sup> Brochure - *Protecting the Energy Grid from National-level Disasters and Threats is a Responsibility the Government and the Electric Power Industry Share*, Electricity Subsector Coordinating Council, January 2024; [https://www.electricitysubsector.org/-/media/Files/ESCC/Documents/ESCC\\_Brochure.pdf](https://www.electricitysubsector.org/-/media/Files/ESCC/Documents/ESCC_Brochure.pdf)

<sup>34</sup> *The ESCC's Cyber Mutual Assistance Program*, Cyber Mutual Assistance, May 2023; <https://www.electricitysubsector.org/-/media/Files/ESCC/Documents/CMA/Cyber-Mutual-Assistance-Program-One-Pager.pdf>

### **C. Partnering with DOE and DHS to enable DoD RC support**

As noted above, DoD should closely coordinate with DOE in all such industry engagements and leverage existing DOE emergency plans for DoD-led HD activities involving DCEI. DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) serves an especially important role in coordinating with DoD on support options. DOE's Office of Electricity (OE) can also make significant contributions to help DoD anticipate longer term grid resilience challenges and mitigation measures for HD.

DoD is supporting CESER in conducting DCEI resilience pilot programs in multiple states. However, minimal funding is available to ramp up such activities. DoD should help DOE identify national defense requirements for DCEI resilience improvements, and thereby justify increased appropriations for such efforts. As OPLAN disaggregation goes forward, DoD can assist DOE in clarifying the need for (and benefits of) the execution of specific programs to help ensure that DCEI utilities can sustain or rapidly restore power essential for DoD mission execution.

DoD can also support DOE to identify new funding options to help DCEI utilities recover the costs incurred for defense-oriented spending. As threats to DCEI intensify, they will face a growing need to invest in DCEI and security. DOE and DHS should consider ways to provide federal funding for such investments rather than placing the burden entirely on ratepayers.<sup>35</sup>

In addition to supporting the requirements definition process, three other initiatives could enable RC support and take advantage of unique RC capabilities across the spectrum of resilience activities before, during, and after adversary cyberattacks on DCEI.

#### ***1. RC support for information sharing and other preparedness efforts***

DOE currently provides information on cyber threats and mitigation options to DCEI owners and other utilities through an array of programs, including the Energy Threat Analysis Center (ETAC) and Cybersecurity Risk Information Sharing Program (CRISP).<sup>36</sup> The Electricity Information Sharing and Analysis Center (E-ISAC) also provides valuable, industry-led information sharing, curated analysis and security expertise on cyber threats and other security challenges.<sup>37</sup> In addition, DHS's Cybersecurity & Infrastructure Security Agency (CISA) provides cyber threat advisories and related information to infrastructure owners and operators.<sup>38</sup> DoD's interagency partners also conduct utility-specific analysis and consultations on exploitable vulnerabilities and mitigation options.

---

<sup>35</sup> *Strengthening the Resilience of Defense Critical Electric Infrastructure*, Electricity Advisory Committee to the Department of Energy, March 2022, 7-9; [https://www.energy.gov/sites/default/files/2022-03/EAC%20Recommendations%20-%20Strengthening%20DCEI%20Resilience%20-%20Final\\_508.pdf](https://www.energy.gov/sites/default/files/2022-03/EAC%20Recommendations%20-%20Strengthening%20DCEI%20Resilience%20-%20Final_508.pdf)

<sup>36</sup> Energy Threat Analysis Center (ETAC), <https://www.energy.gov/ceser/energy-threat-analysis-center-0>; Cybersecurity Risk Information Sharing Program (CRISP); [https://www.energy.gov/sites/default/files/2021-12/CRISP%20Fact%20Sheet\\_508.pdf](https://www.energy.gov/sites/default/files/2021-12/CRISP%20Fact%20Sheet_508.pdf), Office of Cybersecurity, Energy Security, and Emergency Response, DOE,

<sup>37</sup> Electricity Information Sharing and Analysis Center (E-ISAC), North American Electric Reliability Corporation, <https://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx>

<sup>38</sup> Cybersecurity & Infrastructure Security Agency (CISA), Information Sharing, <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing>



DoD is now sharing actionable threat information as well. Most notable is USCYBERCOM's Under Advisement program. That initiative allows partners across all industry sectors to collaborate and share unclassified technical information on foreign threats, supported by the insights that USCYBERCOM gains in supporting U.S. allies abroad. U.S. Army Lieutenant General William J. Hartman, Deputy Commander of USCYBERCOM, noted "Under Advisement, and the relationships we have built with our industry partners, is game-changing." That program enables the Command "to enrich industry data with our expertise and unique insights and share that back with trusted private sector partners—who then can better defend their networks at home, while we pursue malicious cyber actors abroad."<sup>39</sup>

RC employees of DCEI utilities can supplement these activities in important ways. These employees who train to perform CNMF roles, when mobilized, have security clearances and specialized cyber expertise. They are also likely familiar with utility-specific networks, operations, and incident response protocols. That is a *unique* combination that no other component of the Total Force can offer. With carefully drafted policy, several specific RC support options may leverage the singular characteristics of such personnel.

Authority for the access of RC utility employees to classified threat information and Defense facilities, consistent with policies governing such access, enables sustained opportunities to strengthen DCEI resilience that would not otherwise be possible. Very few utilities have the Sensitive Compartmented Information Facilities (SCIFs) and supporting communications necessary to receive, store and process classified information. However, every major Defense installation has a SCIF. State Fusion Centers and Multi-State Information and Analysis Centers may also be able to provide facilities for secure information sharing. In addition to supplement existing unclassified information-sharing mechanisms in significant ways, authorities enabling RC employees of utilities to gain access to classified information through such facilities and apply insights they gain to strengthen utility networks that are mutually benefit DoD can bolster DoD's HD and mission assurance. RC employees' access could also enable them to strengthen and sustain collaboration between DCEI utilities with the CDFs they serve and provide opportunities with their civilian-acquired skills to develop mechanisms for operational coordination when adversaries attack the grid. To facilitate such coordination, DoD should also consider aligning RC personnel employed by RUs with appropriate RC positions that have the authority and appropriate clearances to assist DoD in HD-related operations, as liaisons.

## ***2. RC Support for emergency operations***

CESER is responsible for leading DOE's plans and operations in response to disruptions of electric systems and other energy infrastructure, including the coordination of power restoration efforts under Emergency Support Function (ESF) #12 - Energy Annex.<sup>40</sup> The NG frequently assists with ESF #12 response to natural hazards. However, in a significant cyberattack on the DCEI by China or other potential nation-state adversaries, DOE would almost certainly exercise

---

<sup>39</sup> *CYBERCOM's 'Under Advisement' to increase private sector partnerships, industry data-sharing in 2023*, USCYBERCOM, June 29, 2023; <https://www.cybercom.mil/Media/News/Article/3444464/cybercoms-under-advisement-to-increase-private-sector-partnerships-industry-dat/#:~:text=Under%20Advisement%2C%20or%20UNAD%2C%20is,cyber%20threats%20to%20the%20Nation.>

<sup>40</sup> Federal Emergency Management Agency (FEMA), *Emergency Support Function #12 – Energy Annex*, June 2026; [https://www.fema.gov/sites/default/files/2020-07/fema\\_ESF\\_12\\_Energy-Annex.pdf](https://www.fema.gov/sites/default/files/2020-07/fema_ESF_12_Energy-Annex.pdf)

## UNCLASSIFIED

an additional set of authorities and functions for Grid Security Emergencies (GSEs). The RC is exceptionally well positioned to support GSE operations designed to protect or rapidly restore power to Critical Defense Facilities, ports of embarkation, and other assets vital for OPLAN execution.

The Section 215(A) of the Federal Power Act defines GSEs as:

the occurrence or imminent danger of— (A)(i) a malicious act using electronic communication or an electromagnetic pulse, or a geomagnetic storm event, that could disrupt the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of critical electric infrastructure or of defense critical electric infrastructure; and (ii) disruption of the operation of such devices or networks, with significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure, as a result of such act or event; or (B)(i) a direct physical attack on critical electric infrastructure or on defense critical electric infrastructure; and (ii) significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure as a result of such physical attack.<sup>41</sup>

If the President declares a GSE, the Federal Power Act authorizes the Secretary of Energy to issue orders for emergency measures as are necessary, in the Secretary's judgment, to “protect or restore the reliability of critical electric infrastructure or defense critical electric infrastructure during the emergency.” The Secretary can issue such orders to the Electric Reliability Organization (i.e., NERC), a regional entity or entities, or any owner, user, or operator of critical electric infrastructure or of defense critical electric infrastructure within the United States.<sup>42</sup>

RC personnel may support DOE-DoD pre-planning for issuing and implementing orders to the specific entities for whom they work for and with, and leverage their collaboration between utilities, CDFs, and DoD (including identifying mission-critical loads pertinent to DoD). RC personnel can also leverage their familiarity with exercise design to build real-world preparedness to execute emergency orders. Thus far, however, DOE has conducted few such activities with DCEI utilities. Previous GridEx exercises have highlighted the electric industry’s strong interest in deepening collaboration with DOE on the consultative process that would precede the issuance of an order, what those orders should encompass, and the threat scenarios for which utilities should prepare.<sup>43</sup> DoD should collaborate with DOE to move forward on such preparedness initiatives and include the RC as appropriate.

---

<sup>41</sup> Federal Power Act, section 215(A)(a)(4), August 13, 2019; [https://www.ferc.gov/sites/default/files/2021-04/federal\\_power\\_act.pdf](https://www.ferc.gov/sites/default/files/2021-04/federal_power_act.pdf)

<sup>42</sup> Office of Electricity Delivery and Energy Reliability, DOE, *Grid Security Emergency Orders: Procedures for Issuance*, Federal Registry, January 10, 2018; <https://www.federalregister.gov/documents/2018/01/10/2018-00259/grid-security-emergency-orders-procedures-for-issuance>

<sup>43</sup> *GridEx VI Lessons Learned Report*, NERC, April 2022, pgs 10-11; <https://www.nerc.com/pa/CI/ESISAC/GridEx/GridEx%20VI%20Public%20Report.pdf>

### *3. Additional RC support options*

One priority for exploring options for RC assistance lies in survivable communications. Industry-wide GridEx exercises demonstrated that severe adversary attacks could compromise the ability of utilities to share critical operational data and support power restoration operations.<sup>44</sup> With proper authorities and agreements, RC communications systems may be able to help supplement these communications systems in contested homeland environments. The DoD lead should collaborate with RC components and other DoD organizations to identify candidate systems, including survivable mobile communications networks that could be deployed to RU operations centers, and assess their potential value for utility support for HD operations.

An additional opportunity for assistance lies in establishing a template Memorandum of Understanding (MOU) between utilities and appropriate DoD components, including state NGs . While several utilities are strengthening their relationships with such organizations, they typically need to develop MOUs on a case-by-case basis, rather than having a model to use as a starting point and modify for their own circumstances and priorities. Moreover, existing coordination mechanisms focus on NG support for cyber incident response in SAD. The DoD lead should collaborate with the ESCC and appropriate DoD components to develop and template MOU for DoD support to RUs and other utilities essential for supporting HD operations.

ESCC members are likely to identify additional support options as discussions with DoD go forward. In addition, industry input will be essential to help meet two other preparedness challenges: the de-confliction of civilian and military roles for RC employees of utilities, and the refinement of the CEI in ways that meet both industry and DoD priorities.

#### *FINDING:*

- Substantial opportunities exist to strengthen RC support for the resilience of utilities that operate DCEI and other infrastructure essential for homeland defense.

#### *RECOMMENDATION:*

- In coordination with DoD components, the Department of Energy, and the Department of Homeland Security should collaborate with the ESCC to assess priorities for RC support to DCEI and other grid infrastructure critical for HD. Building on the *2023 Homeland Defense Policy Guidance*, OSD will also refine its processes and criteria for requesting, approving, and coordinating such support.

---

<sup>44</sup> Id., pgs v and 8

## **VI. DECISION CRITERIA TO HELP SECDEF PRIORITIZE THE ACTIVATION AND ALLOCATION OF RC FORCES AND MEASURES TO ENHANCE THE VALUE OF CIVILIAN EMPLOYMENT INFORMATION TO SUPPORT SUCH DECISION-MAKING**

Potential conflicts between the military and civilian roles of RC personnel have occurred in the past and reflect long-standing mobilization issues facing DoD post 9-11, and more recently during COVID operations.<sup>45</sup> Operating in a contested homeland environment will make these conflicts pale by comparison. Given the assessment of the NDS that the PRC or Russia could use a wide array of tools to “hinder US military preparations and response in a conflict,” and to “target our critical infrastructure and other systems,” the United States will face multiple, potentially competing demands to help counter these threats.

Section IV noted that Governors might require employment of their NG forces while DoD may require their use for HD missions, including support for fort to port operations. In a confrontation with the PRC or other potential adversaries, awareness of ongoing or forecasted conflicts between DoD and State “demand signals” is required, as well as many other simultaneous requirements for the employment of the RC, including execution of foreign contingency OPLANs and DSCA operations.

However, within this broader competition for scarce RC resources, measures to strengthen the resilience of DCEI poses an especially significant problems for “double counting.” Indications are many such RC personnel wear two hats: one as civilian employees (e.g., of electric utilities), and the other as uniformed military personnel subject to mobilization for T-10 missions. During a crisis, these personnel could be mobilized to execute such missions precisely when their utilities most need them to protect power flow to CDFs.

At the RFPB’s Quarterly Meeting on December 7, 2022, senior Defense leaders stated that it would be inappropriate to develop detailed Directives or other policies that would lock the Department into a fixed policy to resolve conflicts over RC utilization. Instead, these leaders emphasized that the Department needed flexibility to meet unforeseen circumstances and rapidly changing mission priorities.

One proposed suggestion involved the development of decision criteria for DoD leaders to determine the allocation of scarce DoD resources (including the RC), guided by the principles of “do no harm” and maximizing overall value for HD and other DoD missions and priorities. That suggestion has great merit. However, given the scarcity of RC resources relative to their demand in a contested homeland environment, it is likely that any allocation the RC between T-10, HD, or DSCA missions is likely to cause harm to lower priority missions. A better approach: develop criteria based on how the RC can most efficiently and effectively help DoD and the Total Force achieve key Presidential goals in a specific conflict (including both foreign and domestic priorities).

---

<sup>45</sup> *Revised Mobilization/Demobilization Personnel and Pay Policy for Reserve Component Members Ordered to Active Duty in Response to the World Trade Center and Pentagon Attacks - Section I*, OSD P&R Memorandum to Service Secretaries, May 15, 2007; and *Reservists Deemed Essential Employees May Be Exempted from Mobilization*, December 20, 2020; <https://www.military.com/benefits/reserve-and-guard-benefits/2020/12/29/reservists-deemed-essential-employees-may-be-exempted-mobilization.html>

DoD can take additional steps to facilitate such decision-making on RC force allocation. One such step is to improve DoD's database concerning RC civilian employment skills. As required by Title 10 U.S.C. § 10204, Personnel Records, the Secretary shall maintain adequate and current personnel records of each member of the reserve components to include civilian occupational skills.<sup>46</sup> DoD Instruction (DoDI) 7730.68 establishes policy, assigns responsibilities, and provides guidance for establishing the Uniformed Services Human Resources Information System (USHRIS).<sup>47</sup> This system comprises authoritative human resource data as reported by the uniformed services from their systems of records, including the Civilian Employment Information Transaction File.<sup>48</sup> As defined by DoDI 7730.68, the civilian employment information transaction file is a reporting requirement of the skill and employer information of the Reserve Component Service Members in the Ready Reserve of the Military Services.<sup>49</sup> Additionally, DoDM 7730.69, Volume 1, states that DoD will use Civilian Employment Information program data to skills data for information reports, strategic planning, policy planning and development, and for research and analysis with DoD.<sup>50</sup>

However, DoD's utilization of Civilian Employment Information data, while administratively systematic, remains threadbare for identifying RC personnel with critical civilian skills for the defense of the homeland, specifically within the critical infrastructure sector to include utilities. Notwithstanding, the requirement to maintain a Cyber Registry, Civilian Employment Information data of RC personnel certain critical skills within the civilian critical infrastructure sector are also of significant necessity for strategic planning for HD.<sup>51</sup>

DoD policy states that the Civilian Employment Information program data and skills data may be used for information reports, strategic planning, policy planning and development, and for research and analysis within the DoD or DoD-sponsored research.<sup>52</sup> Transforming the Civilian Employment Information Registry to meet emerging HD demands and developing a robust Civilian Employment Information database to include identifiers critical to maintaining the resilience of central CI utilities, will be essential to assist DoD and commanders in mobilization decision making in addition to strategic planning for homeland defense mission sets.

However, DoD must also understand utility priorities and requirements in Civilian Employment Information Registry data, including those associated with privacy protections. Engaging with the ESCC to identify and collaborate in resolving such issues will be essential. The same is true of developing voluntary procedures for gathering data on RC employees of DCEI utilities.

---

<sup>46</sup> Title 10 U.S.C. 10204, Personnel Records; <https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section10204&num=0&edition=prelim>

<sup>47</sup> DoD Instruction 7730.68, *Uniformed Services Human Resources Information System*, effective September 1, 2023; <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/773068p.PDF>

<sup>48</sup> Id.

<sup>49</sup> Id.

<sup>50</sup> DoD Manual 7730.69, Volume 1, *Uniformed Services Human Resources Information System, Main Reporting Requirements*, effective September 1, 2023;

[https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/773069\\_vol1.pdf](https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/773069_vol1.pdf)

<sup>51</sup> DoD Directive 8140.01 and DoDI 8140.02 requires tracking the cyber requirements of positions of DoD Regular Component and Selected Reserve of the Reserve Components as well as the cyber qualifications of Service members. See DoDM 7730.69, Volume 2, September 1, 2023

<sup>52</sup> DoD Manual 7730.69, Volume 1, Section 7

*FINDING:*

- The existing *Civilian Employment Information Registry* does not systematically identify RC members employed as civilians in defense critical infrastructure companies and fails to specify whether they help protect infrastructure from cyberattacks or perform other essential functions in an HD environment. Such data will be crucial to help SecDef decide whether those personnel should continue to support HD in their civilian positions, versus being mobilized to execute T-10 missions.

*RECOMMENDATIONS:*

- Develop “do no harm”- based policy guidance and decision support criteria to help OSD determine whether RC personnel should remain in their civilian jobs to defend DCEI, or be mobilized to perform T-10 missions.
- Reinvigorate and ensure the effective participation of OSD and the Military Departments to update and maintain RC Civilian Employment Information Registry, and add the data to the Index necessary to support DCEI collaboration.
- Partner with the ESCC to account for utility perspectives on the data that the CEI should include, provide necessary privacy protections, and determine how data can be most effectively and efficiently gathered regarding RC employees.

## VII. STRENGTHENING HD COORDINATION WITH FEDERAL PARTNERS

Indications are awareness of homeland defense missions is rapidly growing among DoD's Federal partners. Nevertheless, deeper collaboration is crucial to develop the operational plans, capabilities, and coordination mechanisms for these Departments and Agencies (D/As) to effectively support DoD as the lead Federal Agency when HD activities are underway.

Building on existing interagency exercises and planning frameworks to incorporate HD offers the most efficient and effective way to advance such progress, with DoD providing strategic support on specific mission priorities to help partners shape and prioritize their efforts. DoD can also assist interagency planning by identifying the types of DSCA assistance that may *not* be available to FEMA and other partners in a contested homeland environment, so that D/As, can plan to execute their own responsibilities without such support. These planning investments will assist DoD and civilian agencies in developing formal processes and potential requests for civilian agency support to DoD for HD.

### **A. Prioritizing HD in Interagency Planning**

FEMA exemplifies the progress underway across the interagency in reshaping traditional Agency priorities to account for the shifting threat environment. FEMA Administrator Deanne Criswell recently stated: “what keeps me up at night is the looming danger presented by nation-state threats to our homeland.” Citing *Volt Typhoon* and other Chinese cyber campaigns, she noted that these “stealth attacks have the capability to seriously compromise critical infrastructure, and that the PRC is developing the ability to use the ‘cyberverse’ to aggressively disrupt and even destroy our critical infrastructure.”<sup>53</sup>

FEMA is collaborating with emergency managers nationwide to build preparedness against these threats. Administrator Criswell empathizes that we should “treat them just like an impending natural disaster ...” and that “[w]e must prepare at all levels to mitigate and develop easily executed solutions[]” by establishing “...public/private/military relationships and frameworks for collaboration before an event.”<sup>54</sup>

The work that FEMA and its SLTT partners have underway to strengthen these relationships and planning efforts exemplify the progress that other D/As will need to make. Such progress will be especially important for the Environmental Protection Agency (SRMA for the water sector), the Department of Transportation, and other DoD partners that help ensure the resilience of other infrastructure vital to support HD mission execution.

However, given the multi-sector nature of Chinese threats to the homeland and their implications for all such agencies, plans will also be needed to coordinate interagency support for DoD in a homeland defense environment. Three opportunities to advance such planning offer particular promise:

---

<sup>53</sup> *FEMA Administrator Deanne Criswell's Remarks to the National Emergency Management Association*, FEMA, October 4, 2023; <https://www.fema.gov/fact-sheet/fema-administrator-deanne-criswells-remarks-national-emergency-management-association>

<sup>54</sup> *Id.*, 4-5

- *Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience.* The Biden Administration is currently revising PPD 21 to account for emerging threats to the homeland. As the Administration notes, “Updated policy would strengthen the public-private partnership and provide clear guidance to executive departments and agencies (agencies) on designating certain critical infrastructure as systemically important.” In addition, the revised version “will clarify the roles, responsibilities, and services of the Sector Risk Management Agencies and the Cybersecurity and Infrastructure Security Agency (CISA) to coordinate a national effort to secure and protect against critical infrastructure risks.”<sup>55</sup>

Both sets of changes can help strengthen interagency preparedness to support DoD HD missions. DoD should collaborate with the National Security Council (NSC) to designate critical infrastructure that is not only systemically important, but also (as in the case of DCEI) vital to the execution of HD missions. DoD can also assist the PPD 21 update by helping in clarify supporting roles that CISA and SRMAs may play in DoD homeland defense missions. To enable such progress, DoD should be as specific as possible in terms of the OPLAN in which it will need support and the capabilities and support functions that its interagency partners should be prepared to provide, and the prerequisites for doing so in a contested (and potentially highly disrupted) homeland environment.

- *The National Cyber Incident Response Plan (NCIRP).* The NCIRP lays out the key roles that the Department of Homeland Security and its federal partners will play in incident response.<sup>56</sup> DHS is now leading the effort to update the NCIRP.<sup>57</sup> DoD should help revise the plan to account for HD activities and the role DoD in leading them, including those in which the RC would help DCEI utilities protect and restore power to CDFs.
- *National Response Framework (NRF).* The NRF guides the nation’s response to all types of disasters and emergencies. It is built on scalable, flexible, and adaptable concepts identified in the National Incident Management System (NIMS) to align key roles and responsibilities. It includes Emergency Support Functions that describe federal coordinating structures that group resources and capabilities into functional areas most frequently needed in a national response. The NG most frequently deploys in SAD to conduct incident response operations in accordance with the frameworks established by NIMS and the NRF.

The NRF promotes engaged partnerships amongst all levels of government and Federal and SLTT partners. Federal planning is integrated to align, link, and synchronize response actions to enable federal departments and agencies and other national-level partners to provide the right resources at the right time to support local, state, tribal, territorial, and insular area government

---

<sup>55</sup> *A Presidential Critical Infrastructure Protection Order Is Getting A Badly Needed Update, Officials Say*, Tim Starks, Washington Post, May 11, 2023; <https://www.washingtonpost.com/politics/2023/05/11/presidential-critical-infrastructure-protection-order-is-getting-badly-needed-update-officials-say/>

<sup>56</sup> *National Cyber Incident Response Plan (NCIRP)*, Department of Homeland Security, December 2016; [https://www.cisa.gov/sites/default/files/ncirp/National\\_Cyber\\_Incident\\_Response\\_Plan.pdf](https://www.cisa.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf)

<sup>57</sup> *CISA Releases Fact Sheet on Effort to Revise the National Cyber Incident Response Plan (NCIRP)*, CISA, October 20, 2023; <https://www.cisa.gov/news-events/alerts/2023/10/20/cisa-releases-fact-sheet-effort-revise-national-cyber-incident-response-plan-ncirp>



response operations.<sup>58</sup> Under FEMA’s coordination, DoD should collaborate with its Federal and SLTT (FSLTT) partners to examine whether and how these frameworks might be supplemented to coordinate support for DoD-led HD operations.

### **B. Meeting DSCA Priorities in a Contested Homeland Environment**

FEMA Administrator Criswell has called on the emergency management community to “imagine that happening in a geopolitical conflict with multiple attacks on our critical infrastructure and the possibility that DoD support might not be available,” and build incident response capabilities that can successfully go forward in the absence of DSCA support.<sup>59</sup> Sections IV and V above found that strong consultative mechanisms will be necessary to help allocate scarce DoD resources in a contested homeland environment.

The Emergency Management Assistance Compact (EMAC) system exemplifies these opportunities. The EMAC is a national mutual aid partnership agreement allowing state-to-state assistance during state or federally-declared disasters and emergencies. The EMAC concept was approved by Congress in 1996 (Public Law 104-321) and provides Governors a means to quickly request assistance for any type of emergency, from earthquakes to acts of terrorism – and, potentially, nation-state cyberattacks on critical infrastructure. When state resources are overwhelmed, other states, including NG units nationwide, can be requested to step in and fill shortfalls.<sup>60</sup>

The ability to flow supporting State assets in this manner could be enormously valuable in a contested homeland environment where NG units available for DSCA may be in short supply, and in which states that are experiencing specific types of resource shortfalls could benefit from EMAC. The NRF is intended to inform local, state, tribal, territorial, and insular area governments, as well as NGOs and the private sector, regarding how the Federal Government responds to incidents. Intergovernmental and agency partners need information for their planning and understand assumptions regarding federal assistance and response and how federal support will be provided are accurate.<sup>61</sup> EMACs can help meet requirements and provide support for federal response to HD.

### **C. Federal Partner Support for DCI Resilience**

DoD has made significant progress in raising awareness internally and with partners regarding understanding DCI risk, building support to reduce it, and understanding DoD’s critical dependencies through the Critical Infrastructure Defense Analysis Center (CIDAC). In order to make progress at scale, OSD(P) is working with partners to formally establish clearer roles and responsibilities for risk management, ensuring that DCI dependencies and vulnerabilities more fully inform DoD risk management efforts, building interagency support for DCI work, pursuing

---

<sup>58</sup> *National Response Framework (NRF)*, Fourth Edition, p. 48, October 28, 2019, US Department of Homeland Security

<sup>59</sup> FEMA Director Criswell, Remarks, 5

<sup>60</sup> *Emergency Management Assistance Compact (EMAC) Fact Sheet*, National Guard Bureau, November 2020; [https://www.nationalguard.mil/Portals/31/Resources/Fact%20Sheets/EMAC%20Fact%20Sheet%20\(Nov.%202020\).pdf](https://www.nationalguard.mil/Portals/31/Resources/Fact%20Sheets/EMAC%20Fact%20Sheet%20(Nov.%202020).pdf)

<sup>61</sup> NRF, p. 49

more organized USG efforts for regional assessments, and improving direct SLTT engagement to support risk management.

Ensuring Federal partners are capable and prepared to help protect the homeland will strengthen DoD's ability to prevail in conflict zones abroad. With vested interests in shared DCI assets, DoD could effectively collaborate with interagency partners to ensure operational capabilities, planning processes, and adequate funding to strengthen DCI resilience. The Federal Senior Leadership Council can serve as a cross-sector council uniting the interagency with a common responsibility of protecting DCI and promoting resiliency. The Council will serve as a platform to guide and develop risk management operations including joint trainings and regular consultation.

DoD has also established robust guidance to components to prepare to operate through disruption, with particular emphasis on contested logistics. In addition, DoD has developed approaches to share strategic level priorities for remediation with key partners and is working to organize outreach to do this at scale with sustained partnership initiatives that are vital for success.

#### **D. HD Exercises**

Exercises are vital to building the ability of DoD's partners to operate through the disruptions that a contested homeland environment would entail, and support DoD as needed while also executing their own critical missions in the absence of available Defense support to federal and civilian authorities.

- Exercising a domestic incident response with reduced or no DoD support. These exercises could: (a) help ascertain the critical minimum level of DoD support (which could be 0); (b) facilitate the identification of alternate sources of support; and (c) highlight capability/capacity gaps that DoD's FSLTT partners should plan to close.
- Exercising a domestic incident response in a contested homeland environment in which DoD HD operations are also being conducted. This could help identify essential gaps and seams in FSLTT incident response frameworks and procedures.

The National Security Council (NSC) can help build such preparedness at a senior level by conducting exercises for the Deputies Committee that include HD components, structured to identify (and then track measures to remedy) gaps in D/A supporting plans and capabilities for operational coordination "under fire."

In addition, the Principals Committee of the NSC sets the Principals' Exercise Priorities (PEPs) that help guide National Level Exercises (NLEs). The NLE is the nation's cornerstone exercise for validating progress toward promoting and sustaining a prepared nation to respond to catastrophic events. NLE 2024 will examine the impact of a large hurricane on the Hawaiian Islands but will also include cyber-attacks in Guam further complicating supply chain issues caused by the damage to Honolulu Harbor. The exercise will include activities that examine

plans and core capabilities within the Mitigation, Response, and Recovery mission areas.<sup>62</sup> Given that focus, DoD and its partners should carefully assess NLE 2024's lessons learned for valuable lessons learned for HD preparedness. Moving forward, PEPs for the next NLE should prioritize HD exercise components, including contested fort to port operations.

HD priorities should also inform the evolution of the four-year National Exercise Program (NEP). This four-year cycle of exercises is the primary national-level mechanism for validating national preparedness. As part of the National Preparedness System, the NEP is a key component in developing a culture of preparedness, empowering communities, and promoting resilience against threats and hazards Americans face.<sup>63</sup> The NEP can be especially useful in building preparedness of SLTT governments for HD, including with respect to exercising plans to save and sustain lives in the absence of DoD support.

*FINDING:*

- Federal D/As require existing plans in place to assist DoD in HD missions related to their authorities, expertise, and industry relationships as Sector Risk Management Agencies for infrastructure critical to national security. DoD should also collaborate with these partners to exercise their support plans and refine coordination mechanism with will be effective “under fire” in a contested homeland environment.

*RECOMMENDATIONS:*

- Collaborate with the National Security Council (NSC) to conduct a Deputies Committee exercise for HD, structured to identify shortfalls in interagency plans to support DoD-led HD missions, assess coordination mechanisms, and approve follow-on exercises that will include participation by operators of defense critical infrastructure.
- Support exercises, experimentation, and collaboration on the cyber resilience of DCEI to support critical DoD missions, especially with the active participation of US Cyber Command and USNORTHCOM. Encourage HD and contested homeland injects for exercises such as USNORTHCOM and USINDOPACOM Defense Coordinating Officer Certification Exercises and others where DoD operates in coordination with SLTT and FEMA.
- DoD should develop and incorporate plans for sustainable, interoperable communication platforms with DCEI utilities and with interagency, state, and local partners for HD Operations.
- In coordination with the Council of Governors, conduct an exercise for Governors, The Adjutants General, and the interagency to assess potential requirements for NG forces in SAD, T-32 (HD), and T-10 missions in an HD scenario involving wide-area power outages. The DoD lead should help conduct regional exercises involving electric utilities essential for fort to port operations.

---

<sup>62</sup> *About the National Exercise Program*, FEMA, February 13, 2024, <https://www.fema.gov/emergency-managers/national-preparedness/exercises/about>

<sup>63</sup> *Id.*

## **SECTION VIII: IMPROVING UNITY OF EFFORT ACROSS THE RC, AND WITH STATE, LOCAL, TRIBAL, AND TERRITORIAL (SLTT) GOVERNMENTS.**

Recent cyber threat advisories by CISA regarding Volt Typhoon and other Chinese campaigns have heightened the awareness of SLTT leaders regarding the risk that such threats pose to critical infrastructure within their jurisdictions.<sup>64</sup> TAGs and the NG teams they lead can play crucial roles in strengthening state plans and capabilities to meet these challenges and provide sustained connectivity with DCI operators to target resilience initiatives of priority to DoD. State's NGs already developed close collaborative relationships with electric utilities. Scaling those efforts up and supplementing them to prepare for HD CEI support activities offers a practical, near-term opportunity for progress.

The National Guard Bureau (NGB) can also help coordinate these state NG initiatives. Moreover, the entirety of the RC also maintains important capabilities to bring to bear in T-10 status to support fort to port operations and other DoD homeland defense missions. Building unity of effort across the RC and with the Total Force and SLTT governments offers an additional opportunity to strengthen HD preparedness.

### **A. NGB, TAGs, and Sustained Partnerships for DCI Resilience**

NGB will be a key partner for OSD in engaging with TAGs, Governors, and SLTT governments for DCI risk management. TAGs work closely with their State Governors and with other State TAGs. State governments are undergoing a major transformation in organizing to align work on critical infrastructure resilience in light of press reports regarding adversary targeting of such infrastructure. Moreover, FSLTT governments and their industry partners can also seek to benefit infrastructure resilience by shaping the distribution of grants under the Infrastructure Investment and Jobs Act (IIJA), the Inflation Reduction Act, CHIPS and Science Act, and other Federal funding. Elevating and enhancing defense programs such as the Defense Community Infrastructure Program and the Installation Resilience Program provide valuable ways to coordinate the allocation of such grants.

TAGs, with guidance from the HQ level, have been forward leaning in understanding and helping shape this work, including explaining DoD equities while supporting governor priorities. They have also excelled at facilitating DoD engagements with key staff members of state governments. OSD should continue to provide the DCI-related data that state NGs need to support resilience efforts and ensure that states are poised to address critical DoD operational needs to execute HD missions.

### **B. Building on NG-utility Exercises and Other State Preparedness Initiatives**

A growing number of State NGs are conducting grid defense exercises in partnership with SLTT governments and utilities that serve key Defense installations. Virginia's 2022 Cyber Fortress exercise provides a prime example. This event brought approximately 20 Virginia National

---

<sup>64</sup> *Threat Advisory: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, CISA, February 7, 2024; <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>

Guard Soldiers and Airmen together with numerous public and private sector partners including Dominion Energy, the Virginia Department of Emergency Management, the Virginia Department of Information Technology, the Virginia State Police and other local, state and federal organizations.<sup>65</sup> In Cyber Fortress 2025, the VA ARNG will collaborate with the Virginia Maryland Delaware Association of Electric Cooperatives to ensure the robust protection of the region's electrical infrastructure.<sup>66</sup>

Future NG exercises should incorporate HD scenarios, missions, and planning factors (including RC force allocation issues). Cyber Shield 2023 constitutes a milestone in this regard. During the event, approximately 800 Guardsmen from 36 states and territories and their partners exercised defensive operations supporting freight railroads. DoD has designated 30,000 miles of freight infrastructure as critical for mobilizing and resupplying U.S. armed forces.<sup>67</sup> Conducting multi-state freight movement in a contested homeland environment constitutes a key HD objective. Expanding such exercises to encompass the full range of DCI essential for integrated fort to port operations should become a prime focus for exercise design.

Exercises and other events should also leverage annual training requirements for NG personnel to perform their T-10 missions, in scenarios where they can also employ their accumulated expertise (military and civilian) to defend critical infrastructure networks and operations. The Maryland Air National Guard's Cyber Blitz exercise, conducted in August 2021, provided this very combined approach. The 175th Cyber Operations Group and 169th Cyber Protection Team conducted a realistic, adversarial cyber exercise to meet their annual training requirements before the event. They, then, conducted the exercise based on the Colonial Pipeline cyberattack that caused fuel supply instabilities.<sup>68</sup>

The NG is also conducting broader partnership initiatives to strengthen utility resilience. For example, the Washington National Guard and Tacoma Public Utilities (TPU) have launched a public-National Guard Cybersecurity Partnership Program. The program draws on the region's military and tech talent to increase cybersecurity awareness supporting multiple sectors. As part of the program, the Washington National Guard has conducted a cyber-security assessment of TPU's industrial control systems to support of our critical infrastructure. The National Guard has also provided findings and recommendations to strengthen the cybersecurity posture of TPU.<sup>69</sup> As state NGs ramp up such partnership efforts nationwide, focusing on utility support for HD-related missions (including the need to protect or rapidly restore power to ports and critical Defense facilities) can make major contributions to HD preparedness.

---

<sup>65</sup> Virginia National Guard, *91st Cyber Brigade*; <https://va.ng.mil/Army-Guard/91st-Cyber/>

<sup>66</sup> Id.

<sup>67</sup> *Guard Cyber Exercise Aims to Stop Transportation Attacks*, National Guard Association of the United States (NGAUS); June 13, 2023, <https://www.ngaus.org/newsroom/guard-cyber-exercise-aims-stop-transportation-attacks>

<sup>68</sup> *Air National Guard Cyber Blitz Exercise*, Maryland National Guard, August 11, 2021; <https://news.maryland.gov/ng/2021/08/11/air-national-guard-cyber-blitz-exercise/>

<sup>69</sup> *Partnership with Washington National Guard to Strengthen TPU Cybersecurity*, Tacoma Public Utilities, July 14, 2020; <https://www.mytpu.org/partnership-with-washington-national-guard-to-strengthen-tpu-cybersecurity/>

### **C. Strengthening Unity of Effort Across the RC: Dual Status Commanders and Beyond**

RC in T-10 status for over a decade performed DSCA missions in the homeland. The 2012 National Defense Authorization Act authorized the employment of the Army, Navy, Marine Corps, and Air Force Reserves to provide DSCA during Stafford Act major disaster and emergency responses. Shortly thereafter, Superstorm Sandy struck the eastern seaboard of the United States. The USAR 99th Regional Support Command and other USAR components effectively assisted response efforts and continue to do so in subsequent natural disasters.<sup>70</sup>

The extent to which the USAR and other non-NG reserve components can and should help defend DCEI, support port to port operations, and execute other HD missions is less clear. The Army, Air, Navy, Marine Corps Reserves continue to build extensive cyber capabilities, including RC specific Cyber Protection Brigade. However, when mobilized to serve in the Cyber National Mission Force (CNMF), these components execute the CNMF's mission of "Defending the Nation in cyberspace through full-spectrum operations to deter, disrupt, and, if necessary, defeat adversary cyber and malign influence actors."<sup>71</sup> This mission falls within USCYBERCOM's focus on three main areas: "defending the DoDIN [DoD Information Network], providing support to combatant commanders for execution of their missions around the world, and strengthening our nation's ability to withstand and respond to cyber-attack."<sup>72</sup>

These focus areas could also apply to HD mission execution, significantly strengthening the ability to withstand cyberattacks. Section V (above) noted USCYBERCOM provides valuable information sharing with civilian infrastructure operators through Under Advisement and other programs. USNORTHCOM, USINDOPACOM - and the RC that help execute their missions - are also deepening their engagement with DCI operators.

Moreover, RC elements include personnel who may be civilian employees of electric utilities or other infrastructure companies. Yet, few non-NG RC units have developed programs to build on these relationships and conduct exercises and cyber resilience programs for DCEI utilities in their local states. Also, there is a lack of systematic ties between state NG organizations and other RC elements, outside of cyber, that would enable the execution of HD missions, as directed by the President, in a pre-planned, integrated manner.

Both, NGB and other RC leaders should explore how to coordinate state and regional HD planning in ways that bring the expertise of the full RC to bear. Of course, all such planning must account for the possible employment of the RC for OCONUS or other T-10 missions apart from homeland defense. Additionally, plans should reflect the possibility that the President will direct the DoD (DoD to the RC) to prioritize the restoration of civilian infrastructure, especially if the disruption of those systems is helping adversaries achieve their goals of 1) undermining the will of the American people (per the NDS), or 2) inducing societal panic (per ODNI).

---

<sup>70</sup> *Army Reserve Command recognized for Superstorm Sandy Relief Efforts*, US Army Reserve, April 21, 2017; <https://www.usar.army.mil/News/News-Display/Article/1160057/army-reserve-command-recognized-for-superstorm-sandy-relief-efforts/>

<sup>71</sup> *About the Cyber National Mission Force*, US Cyber Command, December 6, 2023; <https://www.cybercom.mil/Media/News/Article/3610711/about-the-cyber-national-mission-forces/>

<sup>72</sup> *Our Mission and Vision*, US Cyber Command, <https://www.cybercom.mil/About/Mission-and-Vision/>

## UNCLASSIFIED

If HD activities require the employment of both the NG in T-32 status and other RC elements in T-10 status, the question remains of how to coordinate such operations. Dual States Commanders (DSCs) provide an option to do so. A DSC is an officer of the Army National Guard (ARNG), Air National Guard (ANG), commissioned officer of the Regular Army or Regular Air Force who has completed specialized training and certification. DSC is “a military commander who may, in accordance with the law, serve in two statuses, federal and State, and exercise command on behalf of, and receive separate orders from, a federal chain of command and exercise command on behalf of, and receive separate orders from, a State chain of command simultaneously while performing the duties of those statuses separately and distinctly.”<sup>73</sup> The Commanders of USNORTHCOM and USINDOPACOM, and the CNGB, jointly manage DSC training and certification.. The SecDef and the state’s governor must both agree to the establishment of a DSC, who operates in two capacities.

- *State Capacity.* A DSC is a member of the state’s chain of command, subject to the orders of the Governor and a TAG of the DSC’s state, and exercises command of assigned state NG forces. The Governors of 50 states and 3 territories have established standing memoranda of agreement with the SecDef to establish a DSC to support an incident response or the safety and security of a special event (e.g., a national special security event). Title 32, United States Code, Section 325, authorizes an NG officer to be placed on active-duty orders without losing their State NG status.
- *Federal Capacity.* A DSC is also a member of the federal chain of command, subject to the orders of the President, the Secretary of Defense, and the supported combatant commander. They are subject to the orders of the USNORTHCOM Commander when in the 48 contiguous states, Alaska, the District of Columbia and the territories of Puerto Rico and the U.S. Virgin Islands. DSCs are subject to the ISINDOPACOM Commander when in Hawaii and the territory of Guam. In addition, DSCs exercise command of assigned federal military forces. A Regular Army or Regular Air Force officer is authorized to accept a commission in the NG of a state without losing his/her active-duty status (32 U.S.C., section 315).<sup>74</sup>

DSCs were established to command Federal and State military forces supporting the safety and security of special events since 2004 and supporting incident responses since 2012. To build on their expertise, NGB, OSD, and relevant COCOMs should examine how DSCs might be used to coordinate HD missions in a contested homeland, including cyberattacks on the electric infrastructure essential for port to port operations.

### *FINDINGS:*

- The National Guard Bureau (NGB) could be directed to help coordinate state NG initiatives to prepare for HD DCEI support activities.
  - NGB should work with OUSD(P) to develop and implement sustained roles and responsibilities for the TAGs and State National Guards in supporting DCEI efforts, engagement with the states, and sustaining dialogue on Departmental

---

<sup>73</sup> *Dual Status Command (DSC) Fact Sheet*, National Guard, November 2020;

[https://www.nationalguard.mil/Portals/31/Resources/Fact%20Sheets/DSC%20Fact%20Sheet%20\(Nov.%202020\).pdf](https://www.nationalguard.mil/Portals/31/Resources/Fact%20Sheets/DSC%20Fact%20Sheet%20(Nov.%202020).pdf)

<sup>74</sup> *Id.*

## UNCLASSIFIED

priorities. In addition, TAGs should continue supporting multi-sector Defense Critical Infrastructure resilience efforts (both DoD and civilian-owned facilities) as appropriate, and closely monitor and support State level CI effort.

- Significant capabilities of the full RC, across all duty statuses (i.e., T10, T32, T14, SAD), will be necessary and crucial to support full mobilization (i.e., fort to port operations) and other DoD missions.

### *RECOMMENDATIONS:*

- TAGs should proactively identify areas where State, community, and DoD priorities align as a basis for collaboration. This includes working in tandem with Governors, Mayors, county commissioners and other local elected officials, emergency managers, and the private sector to implement resiliency measures protecting DCI. Ultimately, given the PRC's goal (per the ODNI) of attacking US infrastructure to induce societal panic, a whole of society effort will be needed to strengthen HD preparedness.
- NGB should identify a lead rep for Civilian DCI collaboration at the General Officer/Flag Officer (GOFO) and Staff level, likely in the MA office to facilitate alignment of TAG efforts and collect insights.
- NGB should continue to work closely with OSD(P) DC&MA in this area and stay actively involved in DC&MA-led work to clarify roles and responsibilities for DCI risk management, and foster partnerships for these efforts.



## **IX. RC CONTRIBUTIONS TO DETERRENCE BY RESILIENCE**

The NDS directs DoD to strengthen Deterrence by Resilience, and “take steps to raise potential attackers’ direct and indirect costs while reducing their expected benefits for aggressive action against the homeland, particularly by increasing resilience.”<sup>75</sup> In addition to the support the RC can provide for executing fort to port operations and other HD missions, expanding the capabilities of the RC to help defend DCEI and other infrastructure can strengthen deterrence by denial.

Achieving such deterrence will require more than improved capabilities. DoD and its electric industry partners must also shape the *perceptions* of foreign leaders to diminish the benefits they expect to achieve by attacking the grid, relative to the costs they believe they would incur if they launched such an attack.

Exercises provide a potentially valuable means of shaping adversary perceptions. For example, RC-supported exercises with electric utilities and their partners could highlight improving capabilities to protect and rapidly restore power for fort to port operations and other HD missions.

### *FINDING:*

- The NDS calls for measures to strengthen “deterrence by resilience,” through coordination with the private sector and other partners to reduce the benefits that potential adversaries expect to achieve by aggressive action against the homeland.<sup>76</sup> Existing grid exercises provide the foundation on which to build such deterrence-oriented initiatives. However, such exercises are typically conducted without significant public visibility, and typically do not exploit opportunities to shape adversary perceptions.

### *RECOMMENDATIONS:*

- DoD should partner with the electricity subsector, DOE, and DHS to structure future exercises focused on strengthening deterrence by denial and building the coordination mechanisms and RC support capabilities that will bolster grid defenses. The goal of such exercises: reduce the benefits that adversaries can expect to achieve by attacking the DCEI and other defense critical infrastructure.
- DoD Public Affairs should also leverage RC support for power restoration following hurricanes and other natural disasters to highlight these improving capabilities.

---

<sup>75</sup> NDS, 9

<sup>76</sup> NDS, 8-9

## **APPENDIX A: REPORT FINDINGS AND RECOMMENDATIONS**

### **SECTION IV: ACTIVATING, MOBILIZING, ALLOCATING, DEPLOYING, AND EMPLOYING RC FORCES FOR HOMELAND DEFENSE**

#### *FINDINGS:*

- Current activation authorities and processes to access the RC are complex and inadequate to perform time-urgent HD response missions. For immediate and more efficient mobilization of the RC for emergent HD, DoD would benefit by seeking a legislative amendment to Title 10, authorizing RC activation for HD and the use of the full RC to conduct HD activities in a timely manner, as directed by the Secretary of Defense as a companion statute similar to Title 32, Chapter 9 for NG HD Activities.
- While T32/Ch 9 provides a potentially useful authority for employing the NG for HD missions, it does not apply to the other elements of the RC. Additional measures will be needed to bring the full range of RC capabilities to bear in support of HD. Furthermore, while this statute authorizes DoD to fund NG HD activities requested by Governors, other HD missions (directed by the DoD in its capacity as the Lead Federal Agency (LFA) for HD), will be essential for the military protection of infrastructure critical to US security. New initiatives will be required to address such challenges and help de-conflict competing priorities for the use of the NG and other RC elements.

#### *RECOMMENDATIONS:*

- Review HD policy and statutes for HD sufficiency. Develop policy and legislative proposals for Congress to supplement DoD Title 10 mobilization authorities the RC, including 1) immediate mobilization for HD missions for the whole of the RC, and 2) standing mobilization orders for preplanned HD missions.
- Propose an amendment to Title 10 U.S.C. to authorize the use of the full RC to conduct HD activities, as directed by the Secretary of Defense.
- Use the Council of Governors to build consensus with States on criteria, processes, and consultative mechanisms to de-conflict competing Federal and State priorities for using the NG and, as applicable, other RC elements to conduct homeland defense activities.

### **SECTION V: RC SUPPORT FOR DCEI RESILIENCE**

#### *FINDING:*

- Substantial opportunities exist to strengthen RC support for the resilience of utilities that operate DCEI and other infrastructure essential for homeland defense.

#### *RECOMMENDATION:*

- In coordination with DoD components, the Department of Energy, and the Department of Homeland Security, collaborate with the ESCC to assess priorities for RC support to DCEI and other grid infrastructure critical for HD. Building on the *2023 Homeland Defense Policy Guidance*, OSD will also refine its processes and criteria for the request, approval, and coordination of such support.

### **SECTION VI: DECISION CRITERIA TO HELP SECDEF PRIORITIZE THE ACTIVATION AND ALLOCATION OF RC FORCES AND MEASURES TO ENHANCE**

## THE VALUE OF THE CIVILIAN EMPLOYMENT INFORMATION REGISTRY TO SUPPORT SUCH DECISION-MAKING

### *FINDING:*

- The existing *Civilian Employment Information Registry* does not systematically identify RC members employed as civilians in defense critical infrastructure companies and fails to specify whether they help protect infrastructure from cyberattacks or perform other essential functions in an HD environment. Such data will be crucial to help SecDef decide whether those personnel should continue to support HD in their civilian positions, versus being mobilized to execute T-10 missions.

### *RECOMMENDATIONS:*

- Develop “do no harm”- based policy guidance and decision support criteria to help OSD determine whether RC personnel should remain in their civilian jobs to defend DCEI or be mobilized to perform T-10 missions.
- Reinvigorate and ensure the effective participation of OSD and the Military Departments to update and maintain RC *Civilian Employment Information Registry* and add the data to the Index necessary to support DCEI collaboration.
- Partner with the ESCC to account for utility perspectives on the data that the *Civilian Employment Information Registry* should include, provide necessary privacy protections, and determine how data can be most effectively and efficiently gathered regarding RC employees.

## SECTION VII: STRENGTHENING HD COORDINATION WITH FEDERAL PARTNERS

### *FINDING:*

- Federal D/As should have plans in place to assist DoD in HD missions related to their authorities, expertise, and industry relationships as Sector Risk Management Agencies for infrastructure critical to national security. DoD should also collaborate with these partners to exercise their support plans and refine coordination mechanism with will be effective “under fire” in a contested homeland environment.

### *RECOMMENDATIONS:*

- Collaborate with the National Security Council (NSC) to conduct a Deputies Committee exercise for HD, structured to identify shortfalls in interagency plans to support DoD-led HD missions, assess coordination mechanisms, and approve follow-on exercises that will include participation by operators of defense critical infrastructure.
- Support exercises, experimentation, and collaboration on the cyber resilience of DCEI to support critical DoD missions, especially with the active participation of US Cyber Command and USNORTHCOM. Encourage HD and contested homeland injects for exercises such as USNORTHCOM and USINDOPACOM Defense Coordinating Officer Certification Exercises and others where DoD operates in coordination with SLTT and FEMA.
- DoD should develop and incorporate plans for survivable communication platforms that are interoperable with DCEI utilities and with interagency, state, and local partners for HD Operations.

- In coordination with the Council of Governors, conduct an exercise for Governors, The Adjutants General (TAGs), and the interagency to assess potential requirements for NG forces in SAD, T-32 (HD), and T-10 missions in an HD scenario involving wide-area power outages. The DoD lead should help conduct regional exercises involving electric utilities essential for fort to port operations.

## **SECTION VIII: IMPROVING UNITY OF EFFORT ACROSS THE RC, AND WITH STATE, LOCAL, TRIBAL, AND TERRITORIAL (SLTT) GOVERNMENTS.**

### *FINDINGS:*

- The National Guard Bureau (NGB) can also help coordinate state NG initiatives to prepare for HD DCEI support activities.
  - NGB should work with OUSD(P) to develop and implement sustained roles and responsibilities for the TAGs and State National Guards in supporting DCEI efforts, engagement with the states, and sustaining dialogue on Departmental priorities. In addition, TAGs should continue supporting multi-sector Defense Critical Infrastructure resilience efforts (both DoD and civilian-owned facilities) as appropriate, and closely monitor and support State level CI effort.
- Significant capabilities of the full RC, across all duty statuses (i.e., T10, T32, T14, SAD), will be necessary and crucial to support full mobilization (i.e., fort to port operations) and other DoD missions.

### *RECOMMENDATIONS:*

- TAGs should proactively identify areas where State, community, and DoD priorities align as a basis for collaboration.
- NGB should identify a lead rep for Civilian DCI collaboration at the General Officer/Flag Officer (GOFO) and Staff level, likely in the MA office to facilitate alignment of TAG efforts and collect insights.
- NGB should continue to work closely with OSD(P) DC&MA in this area and stay actively involved in DC&MA led work to clarify roles and responsibilities for DCI risk management, and foster partnerships for these efforts.

## **SECTION IX: RC CONTRIBUTIONS TO DETERRENCE BY RESILIENCE**

### *FINDING:*

- The NDS calls for measures to strengthen “deterrence by resilience,” through coordination with the private sector and other partners to reduce the benefits that potential adversaries expect to achieve by aggressive action against the homeland.<sup>77</sup> Existing grid exercises provide the foundation on which to build such deterrence-oriented initiatives. However, such exercises are typically conducted without significant public visibility, and typically do not exploit opportunities to shape adversary perceptions.

### *RECOMMENDATIONS:*

- DoD should partner with the electricity subsector, DOE, and DHS to structure future exercises focused on strengthening deterrence by denial, and well as building the

---

<sup>77</sup> NDS, 8-9

## UNCLASSIFIED

coordination mechanisms and RC support capabilities that will bolster grid defenses. The goal of such exercises: reduce the benefits that adversaries can expect to achieve by attacking the DCEI and other defense critical infrastructure.

- DoD Public Affairs should also leverage RC support for power restoration following hurricanes and other natural disasters to highlight these improving capabilities.

## **APPENDIX B: RECOMMENDED TASKS TO ORGANIZATIONS**

### **OSD**

- OSD and JS should examine the options in which HD plans should account for simultaneity challenges and develop courses of action when DoD forces are available;
- Direct the development of flexible decision support criteria to help the Secretary of Defense plan and determine whether to 1) keep RC personnel at their civilian duty stations at electric utilities, or 2) mobilize those personnel to perform their T-10 missions;
- Engage with the ESCC, in coordination with the Joint Staff, DOE and DHS, to:
  - Identify likely utility requests for DoD support that can be sourced to the RC in an HD environment;
  - Explore opportunities for collaboration with the ESCC to experiment with RC support, focused on HD operations when as DoD projects power, while adversaries are attacking DCEI, and structured to leverage Emergency Support Function-12 (Energy Annex) and other existing emergency plans as appropriate;
  - Develop for OSD consideration options to refine the RFA processes that OSD would employ for requests to support the protection or prioritized restoration of DCEI;
- Refine OSD criteria for approving/denying such requests for assistance;
- Engage with the National Security Council and the Federal Interagency to:
  - Develop exercise and other activities to 1) increase the Federal departments and agencies familiarity with HD, how HD differs from homeland security, and the distinctions between HD activities and DSCA; and 2) refine Federal departments' and agencies' plans to support DoD in conducting HD missions, including fort-to-port operations
- Engage with the Council of Governors to:
  - Increase awareness of contingencies in which State NG personnel might be mobilized for HD missions, versus being available for SAD missions, in homeland environments characterized by the disruption of electric systems that support public health and safety;
  - Inform Governors and their Adjutant Generals about state or territory-specific critical infrastructure through unclassified and classified briefings; and
  - Discuss options for the employment of NG forces for HD activities.

### **Joint Staff**

- Identify RC HD capabilities and missions; and allocate RC forces to CCMDs as appropriate;
- Develop HD plans for RC mobilization that also accounts for simultaneous requests for DSCA by other Federal Department/Agencies and Governors;
- Draft an execution order specifically for HD, separate from DSCA;
- Identify and request legislative proposals to Congress to provide mobilization authorities to access the RC for HD (e.g., expansion of, or modeled from, T-10 USC 12304, 12304(c)\*, 12034a, 12304b);
  - Immediate mobilization for HD missions – (\*12304(c), policy implementation under development);
  - Preplanned missions, standing mobilization order;

## UNCLASSIFIED

- Review and expand the criteria/threshold for determining HD vs Homeland Security (JP 3-27); coordinate across United States Government (USG) agencies;
- Refine the Civilian Employment Information Registry to develop an adequate data base to support RC force management decisions, including measures to:
  - Examine the specific shortfalls within the Civilian Information data base structure and data-gathering mechanisms;
  - Assess whether RC civilian employment information data calls should be voluntary or coordinate with the Subsector council to develop priorities and mechanisms for data collection that reflect both DoD and industry priorities, including privacy and protection requirements;
  - Engage with DCI stakeholders to solicit input on the proposed data base; and
  - Tailor to achieve broader benefits of the Total Force.

### **COCOMs - NORTHCOM / INDOPACOM**

- Determine their mission, capabilities, and capacity involving 10 US Code 12304(c) cyber incidents and Homeland Defense.

**APPENDIX C: Reserve Component’s Role in Homeland Defense and Defense Support to Civil Authorities Subcommittee Members**



**Hon. Paul N. Stockton – Board Member and Chair, Reserve Component’s Role in Homeland Defense and Defense Support to Civil Authorities Subcommittee**

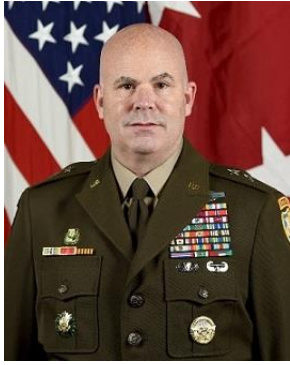
From June 2022 to present, Dr. Paul Stockton serves as a Board Member of the RFPB and serves as the Chair of the RFPB Reserve Component’s Role in Homeland Defense and Defense Support to Civil Authorities Subcommittee.

Dr. Paul Stockton is the President of Paul N Stockton LLC, a strategic advisory firm in Santa Fe, NM. From 2009-2013, Dr. Stockton served as Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, where he helped lead the Department's response to Hurricane Sandy. He was responsible for Defense Critical Infrastructure Protection, Western Hemisphere security policy, domestic crisis management, continuity of operations planning, and a range of other responsibilities. While Assistant Secretary, Dr. Stockton also served as Executive Director of the Council of Governors. After serving as Assistant Secretary, Dr. Stockton was the Managing Director of Sonecon LLC, an advisory firm in Washington, D.C. from 2013 - 2020.

In September 2013, Secretary of Defense Chuck Hagel appointed Dr. Stockton to co-chair the Independent Review of the Washington Navy Yard Shootings, which recommended major changes to the Department's security clearance system that are now being implemented.

Dr. Stockton is the Chair of the Grid Resilience for National Security subcommittee of the Department of Energy's Electricity Advisory Committee. He is a Senior Fellow at the Johns Hopkins University Applied Physics Laboratory. He also chairs the Board of Directors for Analytic Services Inc. and serves on advisory boards for the Idaho National Laboratory and other organizations.





## **Major General John B. Hashem, U.S. Army Reserve, Board Member and Military Executive**

Major General (MG) John Hashem assumed duties as the Military Executive and Non-Voting Board Member, Reserve Forces Policy Board, in August 2020. He most recently served as the Deputy J5, United States Africa Command, Stuttgart, Germany.

MG Hashem enlisted in the Army Reserve in February 1984, was commissioned a Lieutenant of Infantry in 1986. He is a 1988 graduate of the University of Scranton with a Bachelor of Science in Electronic Engineering and Business, Math minor. He holds a Master's Certification in Homeland Security from the University of Colorado, a Master of Science in International Relations from Troy University, and a Master of Science in National Security and Strategic Studies from the National War College. Major General Hashem's military education includes the Infantry Officer Basic Course, Civil Affairs Officer Advanced Course, Psychological Operations Officer Qualification Course, the Basic Strategic Arts Program, Defense Strategy Course, Joint Task Force (Dual Status) Commander Course, Joint Senior Reserve Officer Course, and the Senior Force Integrators Course.

MG Hashem served in a variety of command and staff positions within the Infantry, Psychological Operations, Civil Affairs, and Army Strategist (FA59). Assignments include: 98th Division (Training); 2nd Infantry Division, Korea; 101st Airborne Division (AASLT); The United States Army Civil Affairs and Psychological Operations Command; United States Northern Command, Joint Force Headquarters-National Capitol Region (JFHQ-NCR); The Office of the Secretary of Defense (OSD); Office, Chief of Army Reserve (OCAR); and as DCG-S/Army Reserve Engagement Cell Chief, US Army North/Fifth Army. He served two tours in Iraq; Anti-Armor Platoon Leader during Desert Shield/Storm, 1/187th Infantry, 101st Airborne Division (AASLT); and Commander, Psychological Operations Task Force-Iraq, Operation Iraqi Freedom.

MG Hashem's awards include the Distinguished Service Medal, Defense Superior Service Medal (with Oak Leaf Cluster), Legion of Merit, Bronze Star Medal (with Oak Leaf Cluster), Combat Infantryman Badge, Ranger Tab, Parachutist Badge, Air Assault Badge, Office of the Secretary of Defense Staff Badge, and the Army Staff Badge.



## **Brigadier General Haldane B. Lamberton, Army National Guard, Board Member**

Brigadier General (BG) Haldane B. Lamberton, served as a Board Member of the Reserve Forces Policy Board from June 2022 to June 2024. BG Lamberton, is The Adjutant General for Kentucky appointed by Governor Andy Beshear. As Kentucky's 53rd Adjutant General, BG Lamberton commands the nearly 8,000 military members of the Kentucky Army and Air National Guard. He also oversees the statewide Department of Military Affairs, Kentucky Emergency Management, the Appalachian and Bluegrass Challenge Academies and Bluegrass Station in Avon, Kentucky.

BG Lamberton previous command position in the Kentucky National Guard was the commander of the 238th Regiment in Greenville, KY. He is an infantry soldier with five deployment to include service in Honduras, Panama, Saudi Arabia, Korea, Germany and Iraq. BG Lamberton commissioned through the Reserves Officer Training Corps program at the University of Kentucky in May of 1986. He has a degree in Psychology from the University of Kentucky and was earned a Master's Degree in Strategic Studies from the U.S. Army War College in 2009.

His significant active duty assignments include Infantry Platoon and Mortar Platoon Leader for the 504th Parachute Infantry Regiment, 82nd Airborne Division at Fort Bragg, North Carolina; Rifle Company Executive Officer with the 504th; S-1 and Rifle Company Commander for the 1st Battalion, 506th Infantry, 2nd Infantry Division, Korea.

For the National Guard, he served in many positions from the 149th Brigade, 35th Infantry Division, Commander of 1st Battalion, 149th Infantry, 42nd Infantry Division, Director of Military Support, Director of Human Resources, and Director of Logistics. Among the his numerous awards, BG Lamberton has received the Combat Infantryman's Badge, Master Parachutist wings with a combat star, the Legion of Merit and Bronze Star.



## **Rear Admiral (Ret) Miriam L. Lafferty, U.S. Coast Guard Reserves, Board Member**

Rear Admiral (RADM) Miriam L. Lafferty serves as a Board Member of the Reserve Forces Policy Board. She retired in May 2022 as the Assistant Commandant for Reserve at Coast Guard Headquarters, Washington, D.C., where she provided operationally capable and ready Reserve personnel to support Coast Guard surge and mobilization requirements worldwide.

Previously, RADM Lafferty served as the Deputy Director of Operations for U.S. Northern Command advising the Combatant Commander on operational matters including planning and executing land, air and maritime Homeland Defense, as well as Defense Support of Civil Authorities operations. Prior to her tour at U.S. Northern Command, she served in various reserve leadership roles as the Reserve Officer, Deputy Commandant for Operations in Washington, DC; Reserve Chief of Staff, Atlantic Area in Portsmouth, VA; and Senior Reserve Officer, District Seven in Miami, FL, where she provided expertise and strategic guidance on the mobilization and augmentation readiness, training, and employment of Reserve forces. Other Reserve assignments include the Executive Officer for the Coast Guard Reserve Unit at U.S. Southern Command, Atlantic Area Cutter Forces Branch and Sector North Carolina in the Contingency Planning Department.

RADM Lafferty mobilized in support of five hurricanes, serving as the Liaison Officer to FEMA Region IV's Regional Response Coordination Center coordinating Coast Guard and FEMA efforts. She also served as the Homeland Security Task Force – Southeast representative to U.S. Army South for maritime mass migration planning and operations. During the 2010 Deepwater Horizon oil spill, Rear Admiral Lafferty was mobilized to serve at the National Incident Command coordinating critical resources and facilitating international offers of assistance to aid in the oil spill clean-up.

She spent over 10 years on active duty in operational and intelligence positions. Her afloat assignments include Deck Watch Officer USCGC HARRIET LANE, Executive Officer USCGC DRUMMOND, and Commanding Officer USCGC CHANDELEUR where she conducted law enforcement, search and rescue, and homeland security operations. Her shore side tours include Intelligence Officer for the 13th District's Office of Law Enforcement, Maritime Intelligence Unit in District 7, and the Secretary of Transportation's Office of Intelligence and Security. Rear Admiral Lafferty is a 1993 graduate of the U.S. Coast Guard Academy with a Bachelor of Science degree in Marine Science. She earned her Master of Science in Strategic Studies at the Joint Military Intelligence College (now known as the National Intelligence University).

Rear Admiral Lafferty's awards and decorations include the Defense Superior Service Medal, Meritorious Service Medal, Coast Guard Commendation Medal and Coast Guard Achievement Medal. In addition, she holds a permanent Cutterman's insignia.

## Mr. John F. Sampa, Board Member



Mr. John F Sampa has served as a Board Member of the Reserve Forces Policy Board since June 2022. He was appointed as the 12th Command Sergeant Major (CSM) of the Army National Guard in 2018 and retired in 2022. He was appointed by Secretary of Defense Lloyd J. Austin in May 2024, as the National Chair for the Employer Support of the Guard and Reserve.

He joined the United States Army in 1987 and served in the Army National Guard and the United States Army for nearly 35 years. He completed basic training as a Tank Armored Crewman at Fort Knox Army Post in Fort Knox, Kentucky. CSM Sampa was promoted to the rank of Sergeant Major in 2009. Prior to becoming the Command Sergeant Major of the Army National Guard,

CSM Sampa served as the Command Senior Enlisted Leader for the Texas Military Department. He also served as the Command Sergeant Major for the 36th Infantry Division. CSM Sampa was mobilized three times and deployed overseas for combat operations in Bosnia and twice to Iraq. CSM Sampa served as a key leader in the Texas Army National Guard during the 2003 Space Shuttle Columbia Search and Recovery Mission in East Texas.

CSM Sampa's military and civilian education includes all levels of the Noncommissioned Officer Education System. He is a graduate of the National Defense University Keystone Command Senior Enlisted Leader Course and the U.S. Army Sergeants Major Academy. CSM Sampa is also a graduate of the Texas Highway Patrol Academy. He will receive his Bachelor of Science Degree for Business Administration and Management in May 2022 from the University of the Cumberland. He attended the University of Houston for Civil Engineering Technology and worked as a Structural Steel Draftsman prior to becoming a Texas State Trooper

CSM Sampa was awarded numerous awards and decorations including the Distinguished Service Medal, Legion of Merit (2nd Award), Bronze Star Medal, Defense Meritorious Service Medal, Meritorious Service Medal, Army Commendation Medal (4th award), Air Force Commendation Medal, Army Achievement Medal (2nd award), Good Conduct Medal, National Defense Service Medal (2nd award), Armed Forces Expeditionary Medal, Global War on Terrorism Expeditionary Medal, Global War on Terrorism Service Medal, Iraq Campaign Medal w/Campaign Star, Army Service Ribbon, NATO Medal, the Combat Action Badge, the Army Staff Identification Badge and other awards from the State of Texas.

He was employed with the Texas Department of Public Safety in the Highway Patrol Division for more than 27 years in concurrence with his military service.

## Mr. Atul Vashistha, Board Member



Mr. Atul Vashistha has served as a Board Member of the Reserve Forces Policy Board since June 2022. He previously served on the U.S. Department of Defense Business Board for over 12 years, including as former Vice Chairman from 2018-20.

Mr. Vashistha is a serial entrepreneur with deep expertise around the intersection of technology, global supply chain and risk management. He currently serves on the boards of Shared Assessments and IAOP. He is a former Chair of YeQ Norcal chapter and is currently a YPO Gold

Suncoast member.

Mr. Vashistha is the Founder of Supply Wisdom & Neo Group, and is also the visionary behind the GBSBoard and RiskBoard. Since 2017, he has served as the Chairman & CEO of Supply Wisdom, the fast growth patented risk management platform that continuously prevents and mitigates full stack third party risk exposure for enterprises. For more than 21 years, his teams at Neo Group have worked with nations and corporations to leverage global talent, big data, automation and other technology mega-trends to accelerate new capabilities, increase resiliency, mitigate risks and enable better corporate and societal outcomes.

Prior to founding Neo Group and Supply Wisdom, Mr. Vashistha was Senior Vice President of International at Cardinal Health where he led the international operations of the Fortune 25 Company. He and his seasoned team at Cardinal expanded profitable operations to Australia, New Zealand, Spain, UK, Singapore, Brazil, Mexico, Japan and other global locations.

Media and Wall Street analysts at CNN, ABC, CNBC, Fortune, Forbes, Business Week, Wall Street Journal, Investor's Business Daily, Economist, CIO, CFO and other global organizations seek Mr. Vashistha's expert opinion. He is constant vocal proponent of global supply chain security and has authored three books: Globalization Wisdom, Outsourcing Wisdom, and The Offshore Nation. Additionally, he is a frequent contributor to many leading business publications his bylines include the influential American Bankers Association (ABA) Journal, Forbes.com and Corporate Board Member. Forbes: The Future of Risk Management is Automated Corporate Board Member: The Dangers of Underinvesting in Risk.

The Secretary of Defense awarded Atul "The Office of the Secretary of Defense Medal for Exceptional Public Service" in 2014 and again in 2021. Atul was recognized by Consulting Magazine as both a "Top 25 Most Influential Consultant" and "Top 6 IT Powerbroker." Globalization Today recognized Atul as an "Industry Most Influential Powerhouse 25", and Near Shore Americas recognized him as one of the "Power 50." In 2018, he was inducted into the prestigious IAOP Hall of Fame and has received Shared Assessments "Evangelist Award". NeoGroup was recognized by IAOP in 2019 as a "Best of the World's Best Outsourcing Advisor." Also, in 2019, Enterprise Security Magazine recognized Supply Wisdom as a "Top 10 Risk Management Service Provider". USPTO granted Mr. Vashistha a patent in 2020 for his system for supply chain risk intelligence, which is the foundation of Supply Wisdom's data science and automation.

**APPENDIX D: ACRONYMS**

AC	Active Component
ANG	Air National Guard
ARNG	Army National Guard
CCMD	Combatant Commands
CDF	Critical Defense Facilities
CEI	Civilian Employment Information Registry
CEO	Chief Executive Officer
CESER	Office of Cybersecurity, Energy Security, and Emergency Response
CHIPS	Creating Helpful Incentives to Produce Semiconductors
CI	Critical Infrastructure
CIDAC	Critical Infrastructure Defense Analysis Center
CISA	Cybersecurity and Infrastructure Security Agency
CMA	Cyber Mutual Assistance
CNGB	Chief of the National Guard Bureau
CNMF	Cyber National Mission Force
COCOM	Combatant Commands
CONPLAN	Concept Plans
CONUS	Continental United States
COVID	Coronavirus
D/A	Departments and Agencies
DC&MA	Defense Continuity and Mission Assurance
DCEI	Defense Critical Electric Infrastructure
DCI	Defense Critical Infrastructure
DHS	Department of Homeland Security
DoD	Department of Defense
DoDI	Department of Defense Instruction
DoDIN	Department of Defense Information Network
DoDM	Department of Defense Manual
DOE	Department of Energy
DSC	Dual Status Commanders
DSCA	Defense Support of Civil Authorities
E-ISAC	The Electricity Information Sharing and Analysis Center
EMAC	Emergency Management Assistance Compact
EO	Executive Order
ESCC	Electricity Subsector Coordinating Council
ESF	Emergency Support Function
ETAC	Energy Threat Analysis Center
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSLTT	Federal, State, Local, Tribal, and Territories
GFM	Global Force Management
GOFO	General Officer/Flag Officer
GSE	Grid Security Emergencies
HD	Homeland Defense
IJA	Infrastructure Investment and Jobs Act



UNCLASSIFIED

<u>IOU</u>	<u>Investor-owned Utilities</u>
<u>IRR</u>	<u>Individual Ready Reserve</u>
<u>ISO</u>	<u>Independent System Operators</u>
<u>JMET</u>	<u>Joint Mission Essential Tasks</u>
<u>JP</u>	<u>Joint Publication</u>
<u>JS</u>	<u>Joint Staff</u>
<u>LFA</u>	<u>Lead Federal Agency</u>
<u>MA</u>	<u>Mission Assurance</u>
<u>MOU</u>	<u>Memorandum of Understanding</u>
<u>NCIRP</u>	<u>National Cyber Incident Response Plan</u>
<u>NDS</u>	<u>National Defense Strategy</u>
<u>NEP</u>	<u>National Exercise Program</u>
<u>NERC</u>	<u>North American Electric Reliability Corporation</u>
<u>NG</u>	<u>National Guard</u>
<u>NGB</u>	<u>National Guard Bureau</u>
<u>NGO</u>	<u>Non-Governmental Organization</u>
<u>NIMS</u>	<u>National Incident Management Systems</u>
<u>NLE</u>	<u>National Level Exercises</u>
<u>NRF</u>	<u>National Response Framework</u>
<u>NSC</u>	<u>National Security Council</u>
<u>OCONUS</u>	<u>Outside the Continental United States</u>
<u>ODNI</u>	<u>Office of the Director of National Intelligence</u>
<u>OE</u>	<u>Office of Electricity</u>
<u>OPLAN</u>	<u>Operation Plan</u>
<u>OSD(P)</u>	<u>Office of the Secretary of Defense for Policy</u>
<u>OSD</u>	<u>Office of the Secretary of Defense</u>
<u>OUSD(P)</u>	<u>Office of the Under Secretary of Defense for Policy</u>
<u>PEPs</u>	<u>Principals' Exercise Priorities</u>
<u>PPD</u>	<u>Presidential Policy Directive</u>
<u>PRC</u>	<u>People's Republic of China</u>
<u>RC</u>	<u>Reserve Component</u>
<u>RFA</u>	<u>Request for Assistance</u>
<u>RFPB</u>	<u>Reserve Forces Policy Board</u>
<u>RTO</u>	<u>Regional Transmission Operators</u>
<u>RU</u>	<u>Responsible Utilities</u>
<u>SAD</u>	<u>State Active Duty</u>
<u>SCIF</u>	<u>Sensitive Compartmented Information Facilities</u>
<u>SD</u>	<u>State Department</u>
<u>SLTT</u>	<u>State, Local, Tribal, and Territories</u>
<u>SRMA</u>	<u>Sector Risk Management Agencies</u>
<u>T-10</u>	<u>Title 10 US Code</u>
<u>T-14</u>	<u>Title 14 US Code</u>
<u>T-32</u>	<u>Title 32 US Code</u>
<u>TAG</u>	<u>The Adjutants General</u>
<u>TPU</u>	<u>Tacoma Public Utilities</u>
<u>US</u>	<u>United States</u>
<u>USAR</u>	<u>United States Army Reserve</u>
<u>USCG</u>	<u>United States Coast Guard</u>

**UNCLASSIFIED**

USCGR.....United States Coast Guard Reserves  
USCYBERCOM.....United States Cyber Command  
USG.....United States Government  
USHRIS.....Uniformed Services Human Resources Information System  
USINDOPACOM.....United States Indo-Pacific Command  
USNORTHCOM.....United States Northern Command  
USTRANSCOM.....United States Transportation Command  
VA ARNG.....Virginia Army National Guard  
WMD.....Weapons of Mass Destruction