DEPARTMENT OF DEFENSE DEPENDENCIES ON CRITICAL INFRASTRUCTURE

DEFENSE SCIENCE BOARD

Executive Summary

August 2024

This report is a product of the Defense Science Board (DSB). The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense.

DEFENSE SCIENCE BOARD

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301–3140

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING

SUBJECT: Defense Science Board (DSB) Report on Department of Defense Dependencies on Critical Infrastructure

I am pleased to forward the final report of the DSB study on Department of Defense Dependencies on Critical Infrastructure.

Per the terms of reference, the study focused on dependencies of DoD installations on outside-the-fence critical civilian infrastructure and the concomitant implications for force projection and continuous sustainment. The DSB made recommendations for Department organization and engagement with infrastructure operators and the interagency building towards a whole-of-nation approach to critical infrastructure resilience.

The DSB provided recommendations for rapid action on infrastructure mission resilience, strategy and analysis, intelligence and threat assessment, gaming and exercising, and organizing and resourcing. The study also provided sector-specific recommendations for electricity, bulk fuel, communications, transportation and logistics, and water.

The findings, observations, and recommendations were presented to the full DSB, received thorough discussion and deliberation, and were approved unanimously. I fully endorse the DSB recommendations and urge their careful consideration and adoption.

Eric D. Evans

Dr. Eric D. Evans
Chair, DSB

THIS PAGE LEFT INTENTIONALLY BLANK

DEFENSE SCIENCE BOARD

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301–3140

MEMORANDUM TO THE CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Final Report of the Defense Science Board (DSB) Task Force on Department of Defense Dependencies on Critical Infrastructure

Much has changed since this Task Force began its work in 2020 on DoD dependencies on civilian-owned and operated critical infrastructure. Attacks on the U.S. homeland are an implicit part of near-peer adversary warfighting doctrine. More recently, there has been a heightened awareness and discussion of their infiltration into civilian infrastructure. If or when the Nation is faced with a major contingency against near-peer adversaries, the Task Force concluded that the consequences of delays and disruptions to force projection are potentially severe. Moreover, the extent of adversary penetration could prolong infrastructure outages in ways that undermine populace support for a longer war. But heightened awareness has yet to be translated into the urgent, concrete action that DoD must take to have confidence in executing its war plans going forward.

The Task Force observed immediately that the distinction between "competition" and "conflict" is not serving the Department well. Adversaries have already moved past simple competition to campaigns with actions that disrupt, degrade, and/or cripple civilian infrastructure that DoD and the American public rely on. In their view, they are already in conflict with us.

The Task Force discovered many laudable activities across the Department, but they were almost universally scattered and episodic, and lacked the scale or urgency needed. As a result, the Task Force believes DoD does not see this problem in its entirety and has therefore not organized to act on it. Because this is a Department-wide challenge, cutting across OSD, all Combatant Commands, Military Services, and defense agencies, a Department-wide approach is needed.

The Task Force developed a set of recommendations to both get started and then sustain attention, effort, and progress. Some obvious initial steps require adjustments to existing Department activities, while sustainment will require an organizational construct for which there is no clear existing model. As such, the principal recommendation is to stand up a "Mission Infrastructure Resiliency" task force, co-led by the Under Secretary of Defense for Acquisition and Sustainment and the Commander of North American Aerospace Defense Command and United States Northern Command, to both implement the initial steps and recommend to the Secretary of Defense the enduring organizational construct. That enduring construct must be enabled by intelligence and threat assessment focused on critical infrastructure, a strong analytical function that informs a "living" strategy that adapts to the changing threat, and gaming and exercising that includes disruptions to the homeland as integral parts.

In parallel, the Task Force took "deep dives" into the four sectors it thought most critical to force projection from the homeland: energy (electricity and bulk fuel), communications, transportation and logistics, and water/wastewater. Recommendations specific to each of those sectors were developed but have in common the need for DoD to partner and engage persistently with both the responsible sector risk management agency and with civilian owner/operators from each of those sectors.

In summary, DoD leadership must take seriously and give priority to their roles and responsibilities to ensure the resiliency of civilian infrastructure on which it is so critically dependent. No longer can the warning signs be downplayed or ignored. Both internal actions and strong partnering outside the Department are paramount.

Dr. Miriam John Co-Chair	Hon. Judith Miller Co-Chair

Table of Contents

THIS PAGE LEFT INTENTIONALLY BLANK

Executive Summary

The Homeland is a Target

Department of Defense (DoD) operations in the homeland, whether day-to-day or in support of urgent force projection, have always held some level of dependency on civilian-owned critical infrastructure. These dependencies have grown significantly since the end of the Cold War. Outsourcing of services (e.g., electricity, water, ground transportation) has been deemed more efficient, reliable, and cost effective for the Department. A similar model has been adopted by the service providers themselves, outsourcing many of their own support services and supplies to lower tier providers. As a result, DoD is dependent on increasingly fragile homeland infrastructure whose interdependencies are difficult to unravel, limiting visibility into infrastructure resiliency against intentional attacks or natural disasters.

Conflict is effectively underway as adversaries acquire ever-expanding access and prosecute sophisticated cyber operations against key civilian infrastructure targets. Their stated intent in both doctrine and practice is to disrupt or disable civilian infrastructure on which DoD depends. If their attacks on the homeland are successful on the scale and in the timeframes they seek, U.S. forces could be prevented from winning—or possibly even getting to—the forward fight altogether.

Adversaries are pursuing—indeed escalating—attacks on the homeland, especially in the cyber domain. Nonetheless, DoD characterizes the current situation as "competition" and not "conflict." Based on its numerous interactions with seniors in the Department, the Task Force concluded that continuing to believe we are in competition detracts from the reality we are already living and the urgency with which we must address it.

This study sought to bring together several factors: an understanding of how those infrastructure dependencies support the flow of forces and supplies from the homeland to prosecute DoD's war plans; if and how infrastructure operations could be threatened and compromised; the ensuing impact on theater operations; where operations could be seriously degraded; and what actions the Department should take to mitigate the consequences. In doing so, the study concluded that:

DoD must prepare for attacks on the homeland.

Significant disruptions in force projection infrastructure most certainly will doom a "short war." But a "long war" is equally fraught—persistent attacks on infrastructure could sap the nation's will to fight.

A Call for Urgency and Persistence

The Department cannot and should not go it alone. DoD's dependencies are sprawling and complex, spanning multiple jurisdictions and authorities (federal, state, local, tribal, territories, Title 10, Title 32) with widely insufficient understanding of responsibilities for infrastructure defense and protection. Because these responsibilities lay at the intersection of homeland defense and homeland security (DoD and Department of Homeland Security (DHS) writs respectively), as well as with sector risk management agencies (SRMAs), ownership of the problem can be ambiguous.

These complexities demand a degree of partnership within the interagency and with civilian stakeholders well in excess of DoD's demonstrated cultural inclinations—despite invitation from DHS and key SRMA counterparts, DoD has failed to partner with and inform infrastructure owners of its priorities and requirements at sufficient scale, scope, and level of leadership. At minimum, DoD can leverage existing processes, agreements, and fora; to wit, by influencing implementation of the 2021 *Infrastructure Investment and Jobs Act* (H.R. 3684/Public Law 117-58) by making its resiliency requirements known.

To avoid severe consequences in the homeland or to war plans, DoD must start to act with both urgency and persistence. The study recommends some "blocking and tackling" actions to get started immediately:

- Normalize engagement between installation commanders and civilian infrastructure owners.
- Conduct tabletop exercises (TTXs) and games for specific installations with involvement from local or regional owners and operators to identify uncertainties and vulnerabilities and assess risk.
- Develop and exercise contingencies for disruptions to force projection and sustainment for war plans.
- Assign DoD points of contact for key infrastructure sectors with authority to commit to necessary actions or agreements.
- Better communicate infrastructure resiliency issues to inform collection, analysis, and offensive action.

But this is not a problem with a stopping point; adversaries will adapt. As such, the Department must institutionalize a permanent approach organized and executed around managing an evolving set of risks. Investments, especially in time and people, will be required, with persistent messaging with a campaign mindset from the top down. Partnerships, within the interagency and with civilian stakeholders, are indispensable in forging the necessary whole-of-nation approach to mission infrastructure resilience.

The initial steps listed above require adjustments to existing Department activities, while sustainment will require an organizational construct for which there is no clear existing template. As such, the principal recommendation is to stand up a "Mission Infrastructure Resiliency" (MIR) task force, co-led by the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) and Commander, North American Aerospace Defense Command and United States Northern Command (CDR N&NC), directed and resourced to both implement the initial steps and recommend to the Secretary of Defense the enduring organizational construct. The task force should be given a deadline of no longer than 18 months.

The enduring organizational construct requires the support and integration of key elements, illustrated in Figure 1. Intelligence and threat assessment should inform strategy and analysis, which comprises a mutual feedback loop with gaming, exercises, and sustainment fed by organization and resources. These in turn support the mission.

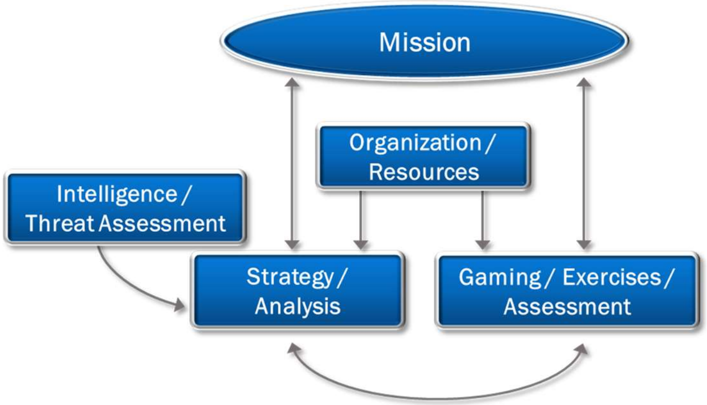

Mission
Organization / Resources
Intelligence / Threat Assessment
Strategy / Analysis
Gaming / Exercises / Assessment

Figure 1. Key Elements of an Enduring Organizational Construct

Four Sectors Critical to DoD Operations

The study also provides more specificity around four sectors critical for force deployment and operations from the homeland: **energy** (both electricity and fuel), **communications**, **transportation**, and **water.** Each is critical to DoD operations in and of themselves but are also highly interdependent.

Each sector proved to be at different stages of maturity in recognizing the critical roles they play in national security, in understanding the threats to their operations, and in doing—or being able to do—anything about improving their resiliency.

- The electricity sub-sector of the energy sector is well organized and progressive under the leadership of the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) at the Department of Energy (DOE). Unfortunately, DoD has not articulated its priorities for functions and their Military Service-level requirements to enable timely and orderly restoration from a serious or prolonged outage.
- The communications sector is probably the most mature, based on its long-standing partnership with the U.S. government starting from the early days of AT&T. While more proliferated today with a greater number of providers, the sector has nonetheless retained a focus on resilience and its role in national security, in large part due to long-standing mechanisms for routine interactions with the U.S. government. Once its most engaged government partner, DoD involvement with the communications sector has unfortunately lapsed since the advent of DHS as communications SRMA.
- The transportation sector, which enables its close cousin "logistics," is diffuse and overseen by the Department of Transportation (DOT) whose dominant mission is maintaining a healthy flow of commerce. The air and maritime domains have suffered from underinvestment for some time and need attention to meet the demands of the new threat environment. Ground transportation within the United States is reliant on commercial rail, whose reliability and security are uncertain, or on the highway system with its aging bridges. Moreover, ports of embarkation are operated with equipment produced in the Peoples Republic of China.
- The water sector is focused on safety instead of security and consists of a plethora of water systems across the nation, for which uniform security practices will be difficult to implement. Despite recent warnings, intrusions, and disruptions in several water systems around the country, the sector's culture has yet to transition to prioritize security as it does health and safety.

Conclusion

During the Task Force's work, there was increasing focus on threats to critical infrastructure, and how to organize to deal with these threats, culminating in the April 2024 *National Security Memorandum on Critical Infrastructure and Resilience (NSM-22)*. In the view of the Task Force, NSM-22 details a comprehensive set of roles and responsibilities across the government. While encoding much of what is already in practice, it also makes clear the expectations of the SRMAs, both within and among themselves. While not explicitly linked to NSM-22, the Task Force findings provide DoD with an assessment of where the Department is meeting its obligations and recommendations to close the gaps where it is not.

In summary, DoD leadership must take seriously—and give priority to—their roles and responsibilities to ensure the resiliency of civilian infrastructure on which it is so critically dependent. No longer can the warning signs be downplayed or ignored. While this does not mean that DoD must pay for all that needs to be done, it does mean that DoD must become a highly committed and visible partner with the civilian owner/operators, both directly and through key government agencies, to help them bolster their resilience. Doing so will erode adversary confidence in the homeland attack pillar of their doctrine and contribute to deterring war altogether.

Recommendations

Immediate “Doable-Dos"

The findings point to some straightforward, low-cost steps for which there should be little debate or delay:

- Within the control perimeters of DoD installations and facilities, commanders responsible for the health and operations of the installation/facility should be informed by the mission owners on its premises of what infrastructure services are critical to the mission and what level(s) of resiliency mission operators may need.
- Senior civilians at installations or facilities should be tasked to develop and maintain ongoing relationships with local civilian infrastructure operators that support them to establish points of contact in outages and emergencies, as well as priorities for restoration of services. Consideration should be given to using the National Guard in these roles as individual Guardsmen are often dual-hatted in the civilian sector to operate the infrastructure services on which the installation/facility depends.
- Frequently asked questions, checklists, templates, and/or playbooks should be developed that allow installation leaders, mission owners, and civilian service providers to identify the most common uncertainties and vulnerabilities, as well as assess options for risk reduction. (Such a checklist should evolve over time as additional shortfalls are identified.) A gaming capability could also be developed that captures the essentials in a virtual format readily customizable to best characterize the local environment.
- Adding a reporting requirement on progress to address installation issues to motivate engagement and remediation (although installation commanders are required to report on disruptive events that occur which would support force deployment from garrison, reporting on the remediation plan is not).
- There should be an immediate shift to develop and exercise contingencies for disruptions to the flow of forces and their continuous sustainment.
- Points of contact (POCs) from DoD should be assigned to each of the key sectors to engage the SRMAs and their sector and government coordinating councils. The POCs should be given the authority to commit or staff various actions or agreements on behalf of the Department.

Many of the infrastructure resiliency issues the United States faces are the same "enjoyed" by our adversaries. Those issues should be routinely communicated to the intelligence community (IC).

Getting Started

Secretary of Defense should empower and direct USD(A&S) and CDR N&NC to establish a Mission Infrastructure Resilience (MIR) task force with an 18-month suspense to identify and ameliorate the infrastructure resilience issues most important to successful USINDOPACOM and supporting Combatant Command (CCMD) war plan execution starting in the homeland. The MIR task force should include representatives from DHS Cybersecurity and Infrastructure Security Agency (CISA), key SRMA representatives, associated civilian infrastructure operators, as well as Military Service and United States Cyber Command (USCYBERCOM) participation and be tasked as follows:

- Start with implementation of the "doable-do" list noted above.

- Make use of analysis capabilities at both DoD and DHS, as well as the expertise of the infrastructure operators, to assess options for improving infrastructure resilience to meet mission requirements.
- Define baseline infrastructure resilience standards for installation and facilities.
- Provide tailored threat products releasable to installation commanders and civilian operators to support this effort.
- Recommend the scope and structure for a DoD-wide permanent organization to replace the MIR at its suspense date.

The MIR task force should keep a list of limiting authorities or other roadblocks to effective action as they are encountered for the purpose of informing potential policy or legislative changes.

To inform and focus the efforts of the MIR, Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs (ASD(HD&HA)) and Director, Joint Staff should prioritize installations and other functions required to execute USINDOPACOM war plans. The focus should be on those installations, routes, and embarkation points required for the initial flow of forces and their sustainment.

Under Secretary of Defense for Personnel and Readiness (USD(P&R)) should develop and add a mission infrastructure resilience metric to the Defense Readiness Reporting System (DRRS). Consider adapting the Army's set of metrics which rank resilience from green to black. Metrics generally should describe sustainability for greater than 30 days (green) to no capability (black).

A Permanent Organization

Secretary of Defense should act promptly to approve the follow-on recommendation of the 18- month MIR task force for a permanent organization charged to continually address mission infrastructure resilience across all areas of responsibility (AORs) and all domains to:

- Ensure that the organization is structured and resourced to support long-term partnerships across key sectors in the interagency and with civilian infrastructure owners.
- Ensure that the organization is given the authorities to consolidate, direct, and assess DoD-wide efforts.

Strategy

Secretary of Defense should direct:

- Under Secretary of Defense for Policy (USD(P)) to adjust operational planning guidance to include planning assumptions that address threats/contested environments that relate to critical civilian infrastructure.
- Combatant Commands, starting with USINDOPACOM, to revise plans in accordance with the former adjustment.

USD(P) through ASD(HD&HA) should develop a strategy for ongoing work to assess risks and prioritize action to ensure the flow of forces and continuous sustainment in a major contingency. The strategy should include:

- Development of a time-phased approach that improves resiliency where needed, increases uncertainty for the adversary, and promotes deterrence through a persistent messaging campaign.
- Establishment of information sharing mechanisms with mission element owners, SRMAs, and civilian infrastructure owners.
- Define the roles and responsibilities of a supporting analytical capability.

Secretary of Defense in close partnership with the Director of National Intelligence (DNI) should establish a program that is informed by the issues identified in the Department's own infrastructure dependencies and employs the best practices of successful past DoD operations.

Analysis

The permanent organization, established after the 18-month MIR task force stands down, should charter and secure the resources to establish a joint interagency analysis center (JIAC) that would:

- Provide the analysis and assessment functions to support prioritizing risks.
- Leverage the maturing tool set from DHS/CISA as a baseline for getting started.
- Focus "beyond the fence line," initially to address assurance/resiliency requirements for critical assets, but as tools mature, for force mobilization and projection.
- Be informed by the IC analysis of threats to critical infrastructure.
- Recommend mitigation plans, investments, and activities.

The JIAC should include participation by DHS, the IC, key sector owners and operators and their SRMAs (e.g., DOE, Environmental Protection Agency (EPA), DOT), making use of both physical and virtual capabilities.

With the establishment of the JIAC for critical infrastructure risk reduction, the permanent organization should direct the use of a formal risk assessment methodology by the Military Services for more localized assessments.

- Assess adaptation of the National Risk Management Center (NRMC) in CISA for the JIAC and/or integrating aspects of the NRMC with the Critical infrastructure Defense Analysis Center (CIDAC).

Intelligence and Threat Assessment

If the threats to critical infrastructure are to be seriously addressed, then:

- National Security Council (NSC) should resolve perceived and real barriers to robust information sharing with the goal of establishing an enduring institutional approach to assessing and informing critical infrastructure owners of threats to their operations.
- DNI and Director of the Federal Bureau of Investigation (FBI), with participation from DHS, DOE and DoD should establish a “center for threats to critical infrastructure" modeled after the original concept for the Analysis and Resilience Center but focused on the sectors critical to homeland defense and force projection.

Because the above recommendations will require some time to be acted upon, some stop-gap actions should be enacted, as follows:

- **DNI and Director FBI** should ensure a robust intelligence collection and analysis program in support of threats to critical infrastructure. Authorities and resources should be provided to the National Counterintelligence Officer (NCIO) at the National Counterintelligence and Security Center (NCSC) to function across the IC, with a charter to:
  - Provide timely threat assessments to SRMAs for dissemination to critical infrastructure owners.
  - Work closely with the DoD's critical infrastructure lead to ensure timely communications with defense infrastructure owners.
  - **USD(P)** should ensure force planning guidance includes serious disruptions of critical civilian infrastructure services for power projection scenarios.

Gaming and Exercises

USD(P) through ASD(HD&HA) and DNI should expand the critical infrastructure gaming approach into a more widely applicable and ongoing capability. This should include a periodic examination of all exercise results to identify if/how current strategy and priorities should be revised.

Overarching the entire Department's approach, exercises should be designed and executed with realistic disruptions to the homeland and other key supply chain(s). In almost every case, key civilian infrastructure owners/operators and local/regional government representatives should be included as advisors, if not players. Specific actions include:

- **Secretary of Defense** require all CCMDs exercise under conditions in which operations in the homeland are simultaneously disrupted during execution of operation plans.
- **Secretary of Defense** require all CCMDs identify commercial supply chain infrastructure that exists in their AORs and determine their criticality, risk to mission, and mitigation to ensure their resiliency if disrupted, and direct that United States Transportation Command (USTRANSCOM) and Defense Logistics Agency (DLA) support their efforts.
- **Chairman of the Joint Chiefs of Staff (CJCS)** require that all globally integrated exercises (GIEs) include realistic attacks on the homeland as a starting point and in parallel with overseas contingencies.
- **CIDAC** (or its replacement as recommended in the Analysis section) develop and maintain a gaming and exercise assessment program to monitor progress.

Any of the above exercises or assessments should include red team expertise, not only to provide realistic descriptions or pathways to attacks, but to be part of the play or assessment to represent adversary adaptation. Advantage should be taken of the Federal Emergency Management Agency (FEMA) and CISA national exercise programs.

Energy (Electricity Sub-Sector)

Planning and Resourcing.

The **18-month MIR task force, followed by the permanent organization established after, should partner with CISA and CESER** to establish an integrated resource and infrastructure planning process.

- Aligned with the Federal Energy Regulatory Commission (FERC), state public utility commissions (PUCs) regulatory processes, and industry standards with respect to resilience.

- Address restoration prioritization and requirements, hardening, and mission-specific service needs with local utility providers.
- Under CESER's leadership, help form and support a working group to create a playbook for using DOE's specific Defense Critical Electric Infrastructure (DCEI) authorities for national security needs.
- Working with CESER, under its DCEI authorities, identify DoD-specific needs and priorities that should be addressed in the infrastructure grants (especially for co-ops) to address service-level requirements in a national security emergency.

Mission Essential Civilian Infrastructure. **Each Military Service installation and energy office should:**

- Prioritize installations serving mission critical assets to identify—in partnership with the utility(ies) servicing the installation—the subset of civilian infrastructure that are single points of failure.
- Update service-level agreements (SLAs), or issue new templates, to include "resilience-as-a-service,"
- Extend black start/energy resilience and response exercises to include civilian infrastructure beyond the fence line.

Industry Best Practices. Each **Military Service installation and energy office** should:

- Ensure procurement of generators and controllers from a single vendor at each installation.
- Review existing renewable energy assets for potential retrofit to enable islanded, off-grid operation and delivery of power to critical mission facilities on the installation.
- Solicit independent power producers to integrate stranded backup generation assets into a virtual power plant during blue-sky conditions to assure the health of backup power sources.

Energy (Bulk Fuel Sub-Sector)

USD(A&S) should consolidate responsibilities for bulk fuel oversight within a single office in OUSD(A&S).

- Task the office with identifying sustainment dependencies on critical civilian infrastructure and communicate to the DHS Transportation Security Administration (TSA), CCMDs, and critical industry partners annually.

USTRANSCOM and DLA partner to expand capabilities for monitoring bulk fuel in transit.

- Provide CCMDs, Military Services, and OSD near real-time visibility of all fuel that is en route to prosecute readiness and wartime requirements.
- Extend to overseas sources.

Communications

The **18-month MIR task force supported by the Defense Information Systems Agency (DISA)** should establish a focused effort between DoD and industry through the Enduring Security Framework to re-evaluate the global architectures associated with continuity of government/continuity of mission in the context of a contested environment.

Immediate, short- and long-term mitigation strategies should be created, and the organizational construct for enduring engagement with the communications sector. Specific areas to be addressed include:

- Transforming the current DoD network architecture to be software defined networking and network functions virtualization (SDN/NFV) ready (policy, plans—implementation at installation level) to support distributed processing and a higher level of resilience at the command/regional level.
- Creating stand-by on-ramps to DoD network architecture for key partners/peers/critical infrastructure support including fiber and spectrum (policy, planning).
- Adopting and mastering new environments/technologies (policy, planning "sandboxes"), such as:
  - Distributed, next-gen wired/wireless access, transport, and processing infrastructure.
  - SDN/NFV/Network slicing.
  - Underlying technologies such as quantum computing, artificial intelligence/machine learning, and neuro linguistic programming.
- Lead organizations to represent DoD in new environment frameworks should be identified (policy, planning, in cooperation with other U.S. government agencies and internationally); e.g.,
  - 5G/6G wireless standards.
  - Interoperability: open radio access network (OpenRAN), metro ethernet forum (MEF), application programming interface (API).
  - Defining the next-gen for internet protocol (IP) networks.

Installation commanders and mission owners at the local and regional levels should communicate their communications and disruption mitigation requirements and collaborate with their local service providers to ensure the degree of resiliency sought is addressed via contractual means.

DISA should identify options and implement a subset to ensure critical communications across command/regional borders, e.g.,

- Space: leverage multiple satellite transport providers to provide higher level of assurance for cross border communications.

DoD Chief Information Officer (CIO) direct transition next-gen DoD architecture throughout the entire DoD enterprise from hub-and-spoke to highly distributed architectures that leverage private and public assets.

- Create a global meshed architecture balancing comparable missions and capabilities by geographic regions.
- Manage the DoD enterprise as a highly distributed, highly resilient collection of command/regional enclaves using SDN/NFV.
- "Mesh" the base/installation to bring higher assurance for individual installations. In addition to communications, considerations for ensuring sufficient power/water/fuel to sustain mission critical communication operations should be incorporated.
- Connect self-sufficient installations to enable a self-sufficient regional enclave that can execute comparable missions.

Transportation, Logistics, and Supply Chain

Immediately, MIR task force should conduct modeling and simulation studies to assess impacts of complications facing USTRANSCOM in support of war plans.

- Provide for deliberations in the next program objective memorandum (POM) cycle.

DLA and USTRANSCOM team with the CCMDs to generate options for managing logistics demands from the homeland for timely delivery of limited supplies.

- Identify and provide to all CCMDs the commercial supply chain infrastructure that supports their war plans.
- CCMDs then determine the criticality, risk to mission, and mitigation measures where needed for the elements in their war plans specific supply chain.
- USTRANSCOM and DLA "close the loop" with the CCMDs to develop contingency plans for limited supplies, as well as for limited transportation assets.
- CCMDs include supply disruptions in annual exercises, as well as request supporting analyses to define minimum quantitative logistics requirements for war plan execution.

USD(A&S) identify opportunities to expand the Warstopper Program.[1]

Water and Wastewater

The MIR 18-month task force should recommend how DoD should manage the water sector on an enduring basis, akin to what is already underway for energy. Tasks include:

- Piloting outreach to waste and wastewater systems, starting with collective defense for the Metropolitan Water District.
- Building on DHS Regional Resiliency Assessment Program (RRAP) and the winter storm challenges that Texas recently faced to enlist San Antonio Water System to pilot DoD installations cooperation with a water system that has done significant resiliency work, but not with DoD as of this writing.
- Promoting close, "joined-at-the-hip" relations between electric utilities and water/wastewater systems. They are naturally interdependent and need to work together. "Energy supply depends on water. Water supply depends on energy[2]."

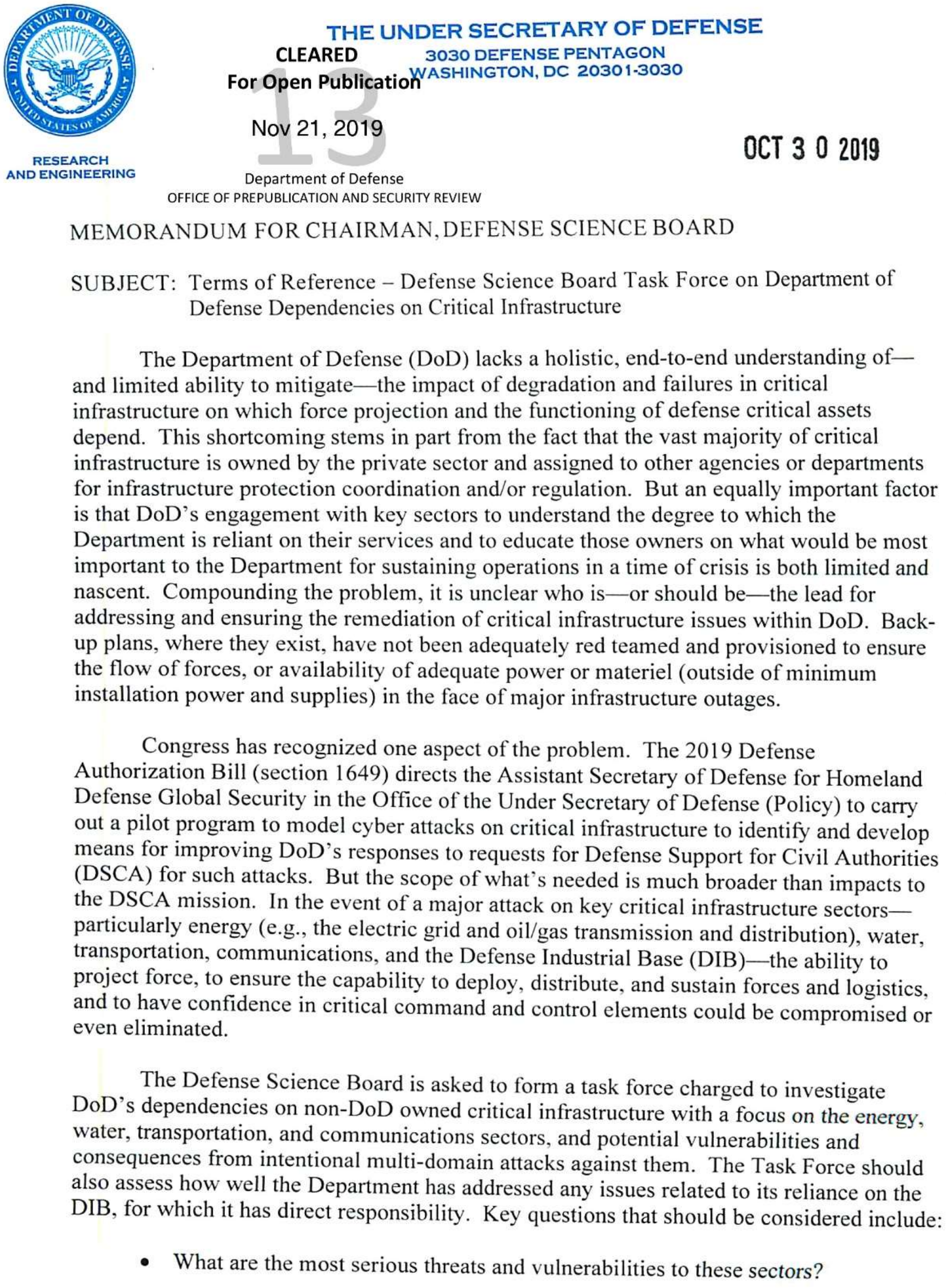
Water and wastewater sector issues cannot be "white carded." Solutions that solve disruptions or outages for a day or two are not sufficient. What is required is sustained analysis, outreach, and advocacy by DoD to fix both short- and long-term problems once they are identified.

[1] The Warstopper Program was created in 1994 in part to replace war reserves not used during Operation Desert Storm. Vendors are contractually obligated to maintain shelf life of medical material identified as critical to the Services if/when they go to war by rotating it with commercial stock. DoD becomes "customer number one" with ready access to contracted supplies.

[2] "Energy and Water – Topics," IEA, https://www.iea.org/topics/energy-and-water.

THIS PAGE LEFT INTENTIONALLY BLANK

Appendix A: Terms of Reference



THE UNDER SECRETARY OF DEFENSE
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

RESEARCH
AND ENGINEERING

CLEARED
For Open Publication
Nov 21, 2019
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

OCT 3 0 2019

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

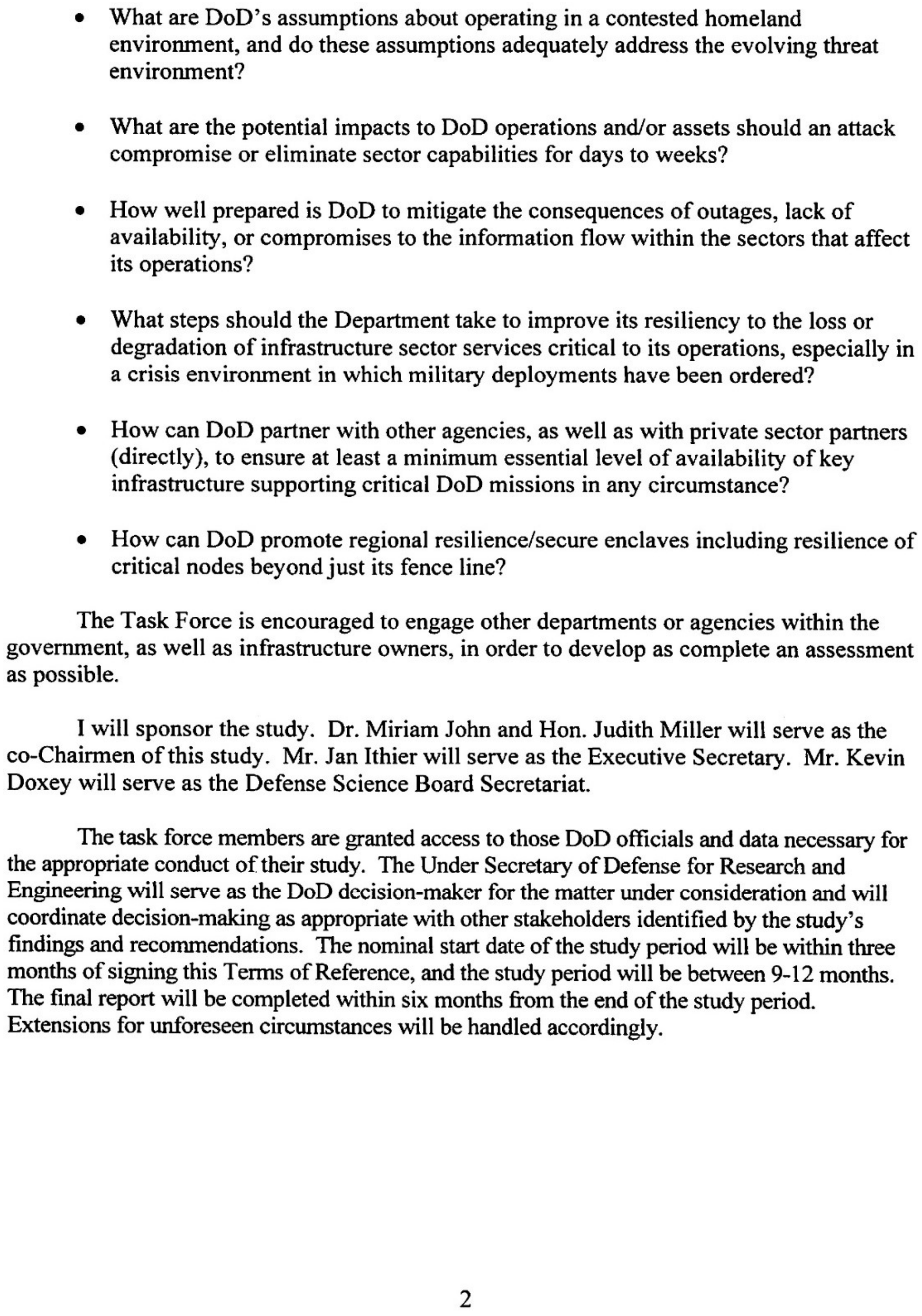
SUBJECT: Terms of Reference – Defense Science Board Task Force on Department of Defense Dependencies on Critical Infrastructure

The Department of Defense (DoD) lacks a holistic, end-to-end understanding of—and limited ability to mitigate—the impact of degradation and failures in critical infrastructure on which force projection and the functioning of defense critical assets depend. This shortcoming stems in part from the fact that the vast majority of critical infrastructure is owned by the private sector and assigned to other agencies or departments for infrastructure protection coordination and/or regulation. But an equally important factor is that DoD's engagement with key sectors to understand the degree to which the Department is reliant on their services and to educate those owners on what would be most important to the Department for sustaining operations in a time of crisis is both limited and nascent. Compounding the problem, it is unclear who is—or should be—the lead for addressing and ensuring the remediation of critical infrastructure issues within DoD. Back-up plans, where they exist, have not been adequately red teamed and provisioned to ensure the flow of forces, or availability of adequate power or materiel (outside of minimum installation power and supplies) in the face of major infrastructure outages.

Congress has recognized one aspect of the problem. The 2019 Defense Authorization Bill (section 1649) directs the Assistant Secretary of Defense for Homeland Defense Global Security in the Office of the Under Secretary of Defense (Policy) to carry out a pilot program to model cyber attacks on critical infrastructure to identify and develop means for improving DoD's responses to requests for Defense Support for Civil Authorities (DSCA) for such attacks. But the scope of what's needed is much broader than impacts to the DSCA mission. In the event of a major attack on key critical infrastructure sectors—particularly energy (e.g., the electric grid and oil/gas transmission and distribution), water, transportation, communications, and the Defense Industrial Base (DIB)—the ability to project force, to ensure the capability to deploy, distribute, and sustain forces and logistics, and to have confidence in critical command and control elements could be compromised or even eliminated.

The Defense Science Board is asked to form a task force charged to investigate DoD's dependencies on non-DoD owned critical infrastructure with a focus on the energy, water, transportation, and communications sectors, and potential vulnerabilities and consequences from intentional multi-domain attacks against them. The Task Force should also assess how well the Department has addressed any issues related to its reliance on the DIB, for which it has direct responsibility. Key questions that should be considered include:

- What are the most serious threats and vulnerabilities to these sectors?



- What are DoD's assumptions about operating in a contested homeland environment, and do these assumptions adequately address the evolving threat environment?

- What are the potential impacts to DoD operations and/or assets should an attack compromise or eliminate sector capabilities for days to weeks?

- How well prepared is DoD to mitigate the consequences of outages, lack of availability, or compromises to the information flow within the sectors that affect its operations?

- What steps should the Department take to improve its resiliency to the loss or degradation of infrastructure sector services critical to its operations, especially in a crisis environment in which military deployments have been ordered?

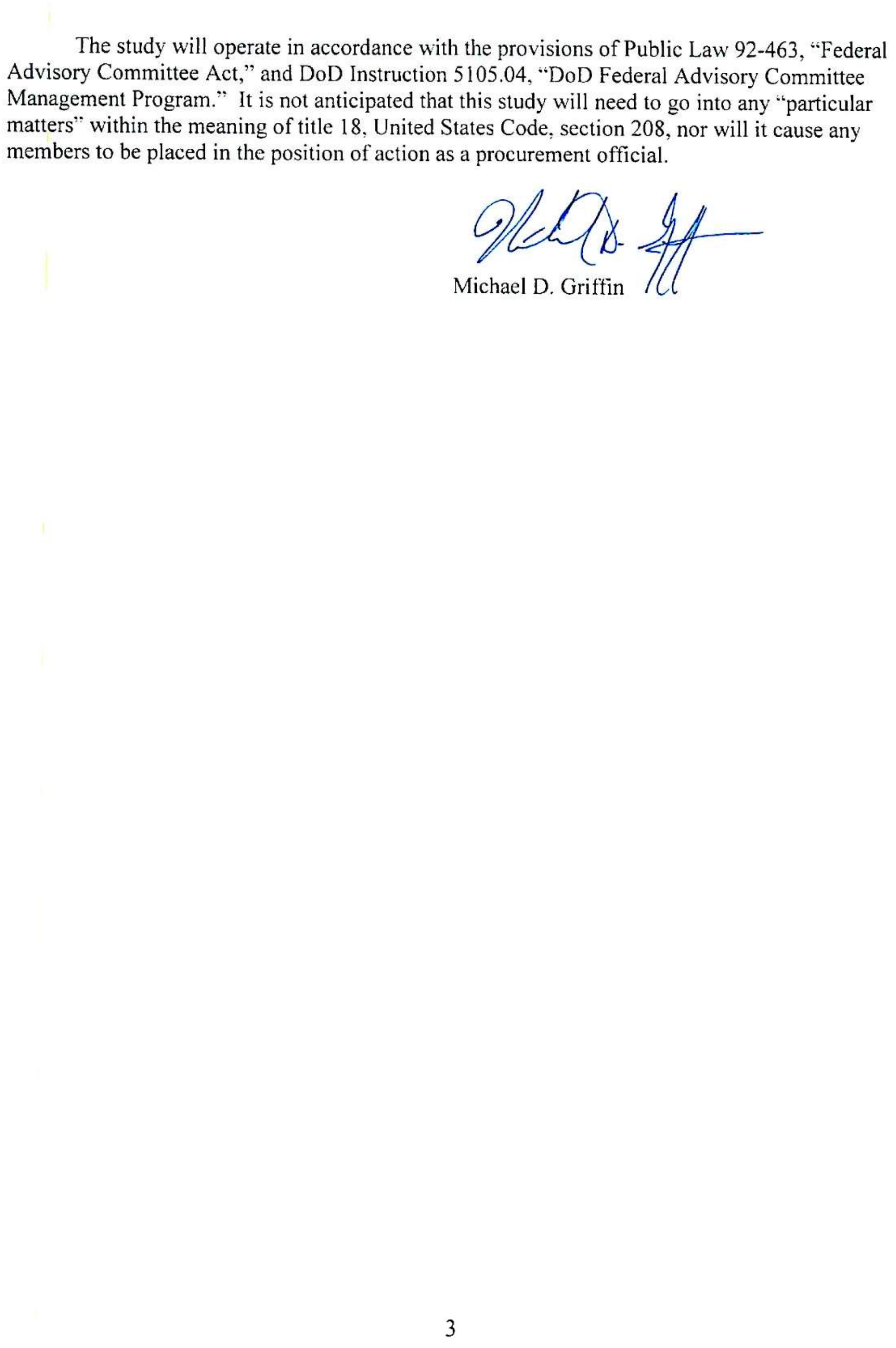
- How can DoD partner with other agencies, as well as with private sector partners (directly), to ensure at least a minimum essential level of availability of key infrastructure supporting critical DoD missions in any circumstance?

- How can DoD promote regional resilience/secure enclaves including resilience of critical nodes beyond just its fence line?

The Task Force is encouraged to engage other departments or agencies within the government, as well as infrastructure owners, in order to develop as complete an assessment as possible.

I will sponsor the study. Dr. Miriam John and Hon. Judith Miller will serve as the co-Chairmen of this study. Mr. Jan Ithier will serve as the Executive Secretary. Mr. Kevin Doxey will serve as the Defense Science Board Secretariat.

The task force members are granted access to those DoD officials and data necessary for the appropriate conduct of their study. The Under Secretary of Defense for Research and Engineering will serve as the DoD decision-maker for the matter under consideration and will coordinate decision-making as appropriate with other stakeholders identified by the study's findings and recommendations. The nominal start date of the study period will be within three months of signing this Terms of Reference, and the study period will be between 9-12 months. The final report will be completed within six months from the end of the study period. Extensions for unforeseen circumstances will be handled accordingly.



The study will operate in accordance with the provisions of Public Law 92-463, "Federal Advisory Committee Act," and DoD Instruction 5105.04, "DoD Federal Advisory Committee Management Program." It is not anticipated that this study will need to go into any "particular matters" within the meaning of title 18, United States Code, section 208, nor will it cause any members to be placed in the position of action as a procurement official.

Michael D. Griffin

Appendix B: DSB Membership

Dr. Eric Evans, Chair

Mr. Michael Appelbaum

Dr. Jennifer Bernhard

Dr. Alison Brown

Dr. Kimberly Budil

Mr. James Carlini

Dr. Tomás Díaz de la Rubia

Mr. Fred Dixon

Adm William Fallon, USN (ret.)

Ms. Laetitia de Cayeux

Mr. Robert Giesler

Dr. Johney Green

Dr. Robert Grossman

Dr. Daniel Hastings

Dr. Ayanna Howard

Dr. Evelyn Hu

Hon. Shirley Ann Jackson

Dr. Ashanti Johnson

Dr. Paul Kaminski

Dr. Ann Karagozian

Dr. John Manferdelli

Dr. Katherine McGrady

Dr. James Miller

Dr. DJ Patil

Dr. Gary Polansky

Dr. Sanjay Raman

Dr. David Relman

Gen Paul Selva, USAF (ret.)

Dr. Nashlie Sephus

Dr. Reshma Shetty

Dr. Alfred Spector

Dr. Vincent Tang

Dr. Dorota Temple

Dr. Jan Tighe

Dr. Bradford Tousley

Dr. David Van Wie

Ms. Mandy Vaughn

Dr. Dinesh Verma

Dr. Steven Walker

Dr. Robert Wisnieff

Appendix C: Task Force Membership

Task Force Co-Chairs

Dr. Miriam John

Hon. Judith Miller

Task Force Members

Mr. Guy Beougher*

Mr. Robert Butler

Ms. Kathryn Condello

ADM William Fallon (USN, Ret.)

GEN Paul Kern (USA, Ret.)

Mr. Erik Limpaecher

Dr. John Manferdelli

Mr. Dave McRee

Mr. Jim Shields

Dr. Jim Tegnelia

Brig Gen Paul Welch (USAF, Ret.)

Additional Members (Pre-Zero-Based Review)[i]

Mr. John Forte

Mr. Jim Gosler

Mr. Jonathon Monken

Dr. Len Napolitano

Hon. Paul Stockton

VADM Ed Straw (USN, Ret.)

Executive Secretary

Mr. Jan Ithier, NORAD/USNORTHCOM

Mr. Phil Kellogg, USD(P)

Mr. Arthur Lord, USD(P) (Pre-ZBR)

Government Advisors

Mr. Steve Harris, CISA

Mr. Brad Koerkenmeier, USTRANSCOM

Government Advisors (Pre-Zero-Based Review)

Mr. Steve Harris, DHS/CISA

Mr. Chris Lowery, DHS/CISA

Ms. Sue Armstrong, DHS/CISA

Mr. Guy Beougher,* DLA

Ms. Pat Hoffman, DOE/Office of Electricity

Mr. Chuck Kosak, DOE/Office of Electricity

Mr. Sean Plankey, DOE/SESER

Mr. Chris Sledjeski, DOE/IN

Dr. Bill Tedeschi, DOE/IN

Dr. Dakota Robertson, White House Fellow

Ms. Lisa Jung, DASD(Energy)

Dr. Ariel Castillo, ODASD(Energy)

Mr. Bruce Krapovicky, OUSD(I)

Mr. Mike McAndrew, OUSD(A&S)

DSB Secretariat

Ms. Elizabeth Kowalski, DSB Designated Federal Officer (DFO)

Mr. Kevin Doxey, DSB DFO (former)

Mr. Sean Hagerty, Alternate DFO (ADFO)

Mr. Troy Techau, ADFO

Support Staff

Ms. Allison Holbert (SAIC)

Mr. Mark Brophy (SAIC)

Ms. Brenda Poole (SAIC)

[i] "Pre-ZBR" refers to the zero-based review of DoD advisory committees that commenced in February 2021. The zero-based review (ZBR) paused work and changed overall DSB membership. When the Task Force resumed their work in late 2022, individuals noted with "Pre-ZBR" did not continue on the Task Force.

*Mr. Guy Beougher, an advisor to the Task Force pre-ZBR became a member of the Task Force post-ZBR.

Appendix D: Briefings Received

Meeting 1 (19-20 February 2020)

Summary of the DSB Report on DoD Roles in Homeland Security
Task Force Co-Chair

The Mission Assurance (MA) Construct; Developing an Understanding of Infrastructure Dependencies; and Risk Management – Guidance, Oversight and Process
J36

Key Homeland Mission 1: Flow of Forces
USTRANSCOM

Key Homeland Mission 2: Logistics and Supply
Defense Logistics Agency (DLA)

Key Homeland Mission 3: Homeland Defense
NORAD & USNORTHCOM (N&NC)

Meeting 2 (27-28 May 2020)

Some Insights from the COVID Pandemic and Implications for Critical Infrastructure
N&NC

Cyber Supply Chain
DSB Task Force Cyber Supply Chain

Defense Logistics Agency's Lessons Learned in COVID19
DLA Notes

The Cyberspace Solarium Commission – Background, Emerging Strategy and Recommendations
Solarium Commission

Survivable Logistics
Survivable Logistics Task Force Chair

Bulk-Power System (BPS) Executive Order Implementation
Deputy Assistant Secretary, Office of Electricity, Department of Energy (DOE)

Meeting 3 (18-19 June 2020)

Grid 101: Grid Threats and Resilience Options
Task Force members and Defense Critical Electric Infrastructure (DCEI)/DOE

Discussion Points: Gas-Electric Interdependencies
Task Force members

New Attack Windows, Gas-Electric Interdependencies, and DCEI Resilience Options
Deputy Assistant Secretary (DAS), DOE, Infrastructure Security and Emergency Response (ISER)

Electricity Information Sharing and Analysis Center (E-ISAC), North American Electric Reliability Corporation (NERC)
NERC

Defense Installation Energy Resilience ("inside the fence line"): DoD Installation Energy Resilience Policies, Guidance, Tools, Initiatives, and Partnerships
Deputy Assistant Secretary of Defense for Energy (DASD(Energy)) and Massachusetts Institute of Technology Lincoln Laboratory (MIT-LL)

Building Electromagnetic Pulse (EMP) Resilience
EIS Council

Emerging Threats to the Energy Sector and Implications for DOD Mission Assurance
Task Force member

Meeting 4 (16-17 July 2020)

Analysis of Potential Adversary Actions on the Power System from a Long Standoff Distance
Schweitzer Engineering Labs

Power Systems Infrastructure Protection
DASD(Energy)

Projects Improving DoD Installation Energy Posture Using Available Financing Authorities
DASD(Energy)

Collaboration Efforts with DoD: EEI Collaboration
Edison Electric Institute (EEI)

Collaboration Efforts with DoD: NRECA Collaboration
NRECA

Alternative Financing
Converge Strategies

Industry Perspectives on Strengthening DCEI Resilience and Key Opportunities for Progress
National Infrastructure Advisory Council (NIAC) and Dominion Energy

Energy Resiliency Perspective
Dominion Energy

DOE Defense Critical Electric Infrastructure Effort
DOE

Research and Development (R&D) Initiatives in Support of Broader Grid Resilience: DOE, National Labs, and Industry – Building a Resilient Electric Grid
DOE

R&D Initiatives in Support of Broader Grid Resilience: DOE, National Labs, and Industry – Electric Grid Security & Resilience
Sandia National Laboratories (SNL)

R&D Initiatives in Support of Broader Grid Resilience: DOE, National Labs, and Industry – Idaho National Laboratory (INL) Grid Resilience Initiatives
INL

DoD R&D for Energy Resilience: More Situational Awareness for Industrial Control Systems (MOSAICS) and Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS)
SNL

DoD R&D for Energy Resilience: Regional Identification of Gaps for Operational Resilience (RIGOR) – piloted at Joint Base Elmendorf Richardson (JBER)
INL and Converge Strategies

DoD R&D for Energy Resilience: Micro-Reactor Effort
DASD(E)

Meeting 5 (20-21 August 2020)

Framework for CI and Critical DoD Mission Resilience
Task Force member

DoD Energy Resilience for Mission Assurance
Office of the Under Secretary of Defense for Policy (OUSD(P))

Mission Assurance Identification Process
OUSD(P)

Jack Voltaic Research Project
U.S. Army Cyber Institute

SoCal Tech Bridge
NavalX

San Antonio-Electromagnetic Defense
Electromagnetic Defense Initiative (EDI)

National Security Collaboration Center (NSCC)
NSCC

NSCC Overview
NSCC

Regulatory Issues and Opportunities for Progress
National Association of Regulatory Utility Commissioners (NARUC)

Meeting 6 (10-11 September 2020)

Communications Sector Introduction
Task Force member

National Critical Functions
National Risk Management Center (NRMC)

Contingency Planning for Significant Cyber Incidents
Cybersecurity and Infrastructure Security Agency (CISA)

Regional Resiliency Assessment Program
CISA

PNT-EMP Risks for Telecommunications
CISA

2012 National Sector Risk Assessment for Communications
Department of Homeland Security (DHS)

Optical PNT: Fiber-based National Terrestrial Timing Network
OPNT

CI: Undersea Cable Concerns
SubCom, LLC

Meeting 7 (27-28 October 2020)

Dependency on Power
Task Force member

China, COVID, and Comms/Supply Chain
WBKLaw

Cybersecurity Concerns: BGP, DNS, DMARC, Enterprise, WFH, Consumer Behaviors
The Internet & Television Association (NCTA)

48 Hours—Are We Prepared for that Speed of Response?
Task Force member

COVID-19 Communications Sector Performance and Initiatives
Task Force member and USTelecom

Assuring Resiliency: DoD Missions and Critical Infrastructure Partners
USTelecom

How Can USTelecom Help Solve DoD Problem
USTelecom

Meeting 8 (18-19 November 2020)

DOE Efforts at Testing, Joint Work with DoD, Risk Assessments and Hardening: EMP Threats
DOE

DOE Efforts at Testing, Joint Work with DoD, Risk Assessments and Hardening: Cyber Threats
DOE

DOE Efforts at Testing, Joint Work with DoD, Risk Assessments and Hardening: Homeland Threats
DOE

Meeting 9 (16-17 December 2020)

Reducing DoD Energy Sector Risks – Planning and Finance
Task Force member and Converge Strategies

Project Athens: DCI Application
DARPA

Pipeline Cybersecurity Initiative – Considerations for DoD Infrastructure
NRMC

Civil Reserve Air Fleet Overview/VISA Overview
USTRANSCOM

Programs for National Defense (Highways/Railroads/Ports)
USTRANSCOM

Safeguarding Seaport and Airport Functions
Port of Seattle

Meeting 10 (12-13 January 2021)

Surge Layer Defense
Office of the Director of National Intelligence (ODNI)

Department of Transportation Maritime Administration (MARAD) Overview
DOT MARAD

National Critical Functions: Insights for DSB
NRMC

Security Plan, Implementation, Priorities
NRMC

Meeting 11 (30 Nov - 1 Dec 2022)

Updates since January 2021 – Logistics and EMP
Task Force member

Cyber Risks Posed by the Transformation of the Grid
Task Force member

Current Trends in Energy Security Risk
Task Force member

DOD Critical Infrastructure Efforts
OSD(P)

Critical infrastructure Defense Analysis Center (CIDAC)
CIDAC

Deputies' Committee-Directed Interagency Critical Infrastructure Project
OSD(P)

USNORTHCOM DCI List and PLANORD
OSD(P)

Force Protection
OSD(P)

DCI Project Overview
OSD(P)

Meeting 12 (12-13 January 2023)

Global Perspectives
NORAD and USNORTHCOM (N&NC), J55

N&NC Guidance, Plans, and Infrastructure Protection
N&NC, J55

Defense Critical Infrastructure: Commander's Estimate Appraisal
N&NC, J55

N&NC J8 – Quiver Model
N&NC, J8

The CISA Briefings
CISA

Meeting 13 (15-16 February 2023)

Cyber Security and Infrastructure Security Agency
CISA

Assessment of Threats
U.S. Army G2

Energy and Control Systems Resilience Exercise Findings
MIT/LL

Meeting 14 (22-23 March 2023)

Threat Brief
N&NC, U.S. Air Force, Defense Intelligence Agency

Transportation Logistics
White House Supply Chain Task Force

Water and Wastewater Systems Security and Resilience
CISA

U.S. Army Corps of Engineers (USACE) Overview of Civil Works: Water Resources
USACE

Water Systems and Vulnerabilities – Water 101: How Water Works
American Water Works Association

Meeting 15 (19-20 April 2023)

Joint Concepts for Contested Logistics
Joint Staff, J-4

Arctic Infrastructure and MOSAICS
N&NC

Theater Sustainment Structure
USINDOPACOM

DLA Illumination on Commercial Dependencies, Warehousing, Defense Fuel Support Points, All Pipelines and Recommendations
Task Force member

Operational Requirements & Commercial Dependencies
DLA

Operational Requirements & Commercial Dependencies
DLA

The Military Surface Deployment and Distribution Command (SDDC) – Delivering in Support of Global Combatant Command Requirements
Capability Development Integration Directorate (CDID), U.S. Army

Meeting 16 (17-18 May 2023)

Threats to Critical Infrastructure
ODNI, MITRE

Insights from Mission Level Cyber Risk Assessments
Cyber Warfare – Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))

Intel Brief
CISA

Critical Infrastructure Defense Analysis Center (CIDAC) – updates from 1 Dec 2022
OSD(P) and The Defense Threat Reduction Agency (DTRA)

Framework for Aligning Domestic and Defense Resources
OSD(P) and DTRA

DoD and Critical infrastructure
OSD(P) and DTRA

Meeting 17 (28-29 June 2023)

Threat Discussion
Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S))

Discussion on the Electric Sector Handout*: A* Communication from Bruce Walker
Southern Company

BNSF Railway: Logistics, Operations, Technology, Resource Protection Network
BNSF Railway

NORAD/USNORTHCOM Perspectives
N&NC

Meeting 18 (25-26 July 2023)

Landscape of Critical Infrastructure (Strategic Plan, Threats, DoD Engagement, Authorities and Policy) – A Office of Cyber Security, Energy Security, and Emergency Response (CESER) Overview
CESER/DOE

Water and Wastewater Infrastructure in the Metropolitan Washington Region
Metropolitan Washington Council of Government

Washington Suburban Sanitary Commission *(WSSC)* Overview
WSSC

Fairfax Water Overview
Fairfax Water

Perspectives of Resilience and Response
National Security Council

Water Resiliency in San Antonio
San Antonio Water System (SAWS)

Meeting 19 (23-24 August 2023)

Installation Readiness
Office of the Assistant Secretary of the Army for Installations, Energy & Environment
Office of the Deputy Chief of Staff, G-9 (Installations)
Headquarters, Army Materiel Command
Headquarters, Installation Management Command
Pacific Northwest National Laboratories (PNNL)

Installation Resiliency and Awareness of Dependencies on Critical Infrastructure
Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs (ASD(HD&HA) and OSD(P)

Appendix E: Acronym List

AORs	areas of responsibility
API	application programming interface
ASD(HD&HA)	Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs
BPS	bulk-power system
CDR	Commander
CCMD	Combatant Command
CDID	Capabilities, Development and Integration Directorate, U.S. Army
CESER	DOE Office of Cybersecurity, Energy Security, and Emergency Response
CIDAC	Critical infrastructure Defense Analysis Center
CIO	Chief Information Officer
CISA	DHS Cybersecurity and Infrastructure Security Agency
CJCS	Chairman of the Joint Chiefs of Staff
DARPA	Defense Advanced Research Projects Agency
DASD(Energy)	Deputy Assistant Secretary of Defense for Energy
DCEI	Defense Critical Electric Infrastructure
DCI	defense critical infrastructure
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
DNI	Director of National Intelligence
DoD	Department of Defense
DOE	Department of Energy
DOT	Department of Transportation
DRRS	Defense Readiness Reporting System
DSB	Defense Science Board
DTRA	Defense Threat Reduction Agency
EDI	Electromagnetic Defense Initiative
EEI	Edison Electric Institute
E-ISAC	Electricity Information Sharing and Analysis Center
EMP	electromagnetic pulse
EPA	Environmental Protection Agency
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency

FERC	Federal Energy Regulatory Commission
GIEs	globally integrated exercises
IC	intelligence community
INL	Idaho National Laboratory
IP	internet protocol
JIAC	joint interagency analysis center
MA	mission assurance
MARAD	United States Maritime Administration
MEF	metro ethernet forum
MIR	Mission Infrastructure Resilience
MIT/LL	Massachusetts Institute of Technology/Lincoln Laboratory
MOSAICS	more situational awareness for industrial control systems
N&NC	NORAD/USNORTHCOM
NCIO	National Counterintelligence Officer
NCSC	National Counterintelligence and Security Center
NCTA	National Cable & Telecommunications Association
NERC	North American Electric Reliability Corporation
NORAD	North American Aerospace Defense Command
NRECA	National Rural Electric Cooperative Association
NRMC	National Risk Management Center
NSC	National Security Council
NSCC	National Security Collaboration Center
NSM-22	National Security Memorandum on Critical Infrastructure and Resilience
OpenRAN	open radio access network
OPNT	optical position, navigation, and timing
OUSD(A&S)	Office of the Under Secretary of Defense for Acquisition and Sustainment
OUSD(I&S)	Office of the Under Secretary of Defense for Intelligence and Security
OSD(P)	Office of the Secretary of Defense for Policy
PNT	position, navigation, and timing
POCs	points of contact
PUCs	public utility commissions
R&D	research and development
RIGOR	regional identification of gaps for operational resilience
RRAP	Regional Resiliency Assessment Program
SAWS	San Antonio Water System

SDN/NFV	software defined networking and network functions virtualization
SLAs	service-level agreements
SNL	Sandia National Laboratories
SPIDERS	smart power infrastructure demonstration for energy reliability and security
SRMAs	sector risk management agencies
TSA	Transportation Security Administration
TTXs	tabletop exercises
USACE	U.S. Army Corps of Engineers
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USD(P)	Under Secretary of Defense for Policy
USINDOPACOM	United States Indo-Pacific Command
USNORTHCOM	United States Northern Command
USTRANSCOM	United States Transportation Command
WSSC	Washington Suburban Sanitary Commission

THIS PAGE LEFT INTENTIONALLY BLANK

Defense Science Board

DSB

Department of Defense