AUBURN UNIVERSITY
McCrary Institute

ISSUE AND POLICY BRIEF:

Examining Critical Infrastructure Definitions and Priorities

A report brought to you by the McCrary Institute for Cyber and Critical Infrastructure Security

Auburn University

By Bob Kolasky, Senior Fellow

This brief explains and evaluates how the definition of critical infrastructure has been applied programmatically, in regulation, and normatively over the last thirty years to support cybersecurity strategy. It then looks at the question of whether it is possible to meaningfully narrow the application to more of a risk-based approach on what is critical more consistently. Finally, it recommends a more focused approach to guide national policy and help better prioritize critical infrastructure cybersecurity and resilience efforts in the face of the current threat environment.

Introduction: Critical infrastructure as a core element of National Cyber Strategy ///

In a time where bipartisanship is in short order, cyber strategy remains an area of general agreement across party lines. This strategy includes building more robust cyber defenses, establishing mechanisms for the private sector to collaborate with the government, and prioritizing addressing cyber vulnerabilities that, if exploited, would have cascading impacts on critical functions of society. Those aims come together in a call to prioritize protecting critical infrastructure from cyber attacks as one of the principal aims of cyber defense.

One of the common pillars across multiple National Cyber Strategies, signed by presidents from both parties, is that we must defend critical infrastructure and strive to make attacking it off limits to our adversaries. The 2024 Republican Party Platform, which has seemingly served as a roadmap for the early days of the Trump administration, asserted that "Republicans will use all tools of National Power to protect our Nation's Critical Infrastructure and Industrial Base from malicious cyber actors. This will be a National Priority, and we will both raise the Security Standards for our Critical Systems and Networks and defend them against bad actors."[1]

That was a more direct articulation – or at least used more capital letters – of the first pillar of the most recent National Cybersecurity Strategy, published in March 2023 by the Biden administration, which was to "defend critical infrastructure." The Biden strategy followed on from the first Trump National Security Strategy in 2017 which emphasized the importance of secure and resilient critical infrastructure in the "Cyber Era."[2] A reading of previous strategies, as well as recommendations from "blue-ribbon" commissions and think-tank papers, including work we have done at the McCrary Institute and the Cyberspace Solarium Commission, would identify similar language.

The point is clear: critical infrastructure must be amongst the top national priorities for cyber security. Yet, amidst those calls for focus and prioritization, an inconvenient truth exists: there is not a consistent and well-understood understanding of the businesses, systems, and assets that constitute what critical infrastructure is and how broadly the term should be applied. Moreover, it is easy to see that in the last thirty years, the United States has broadened the use of that term, diminishing the ability for effective prioritization. This fundamentally weakens the strategic value of the very idea of deeming anything as "critical infrastructure."

The statutory definition of critical infrastructure is "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[3] From that definition, policy documents have typically defined critical infrastructure as systems, assets, and networks within a sector structure. While that has had a useful effect of providing general parameters, it does not function effectively in narrowing what is critical and what is not. For example, Education is considered a critical infrastructure subsector. Does that make every school critical infrastructure? What about the Commercial Facilities sector, where there are hundreds of thousands of buildings for which the

[1] https://www.presidency.ucsb.edu/documents/2024-republican-party-platform
[2] https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf
[3] Footnote from USC

term could apply? How do you define critical infrastructure in the context of an IT sector with tens of thousands of hardware and software providers that could be considered critical?

Prioritizing Critical Infrastructure ///

Before diving into a further examination of what critical infrastructure is, it is worth understanding what sort of prioritization is imagined as part of national cyber strategy. In general, when policymakers imagine prioritization of critical infrastructure as part of cyber efforts, it is for the following reasons:

- To identify the most critical vulnerabilities;
- To deter and dissuade adversaries from "crossing a line" in nation-state and other conflicts, as well as better defining escalation paths;
- To set up coordination structures to collaborate with private sector companies and their representatives with legal protections;
- Relatedly, to enable low-friction information sharing;
- To put a legally defensible schema in place to prioritize technical assistance to non-governmental entities; and
- When statutorily feasible, to place additional mandatory requirements for cyber security controls and information sharing.

In sum, what prioritization is generally intended to do is establish that critical infrastructure entities should be viewed as critical service providers needing protection and should be viewed as high-risk targets. Therefore, it is incumbent on governments to pay special attention to identified critical infrastructure, offer support, and set up structures for regular collaboration to address risk. Should those processes not work in elevating security and resilience, governments should consider mandating additional requirements. It is important to note, however, that the authority to place additional requirements on critical infrastructure entities is limited and is, for the most part, independent of any specific delineation as critical infrastructure.

On top of that, prioritization holds an important distinction as part of global norms of geopolitical conflicts. Attacking critical infrastructure is generally considered an escalation of conflict – a red line of sorts – and countries reserve the right to defend themselves if adversaries are found to have used cyber means to attack critical infrastructure.

It is clear from the above that U.S. cyber policy is intended for meaningful distinctions on how to defend critical infrastructure as opposed to other private infrastructure. That clarity gets a lot blurrier, however, in application. Part of the reason for this is because there is not a well-defined delineation between what is and is not critical infrastructure.

The Evolution of Critical Infrastructure Policy ///

The Organization of Economic Cooperation and Development (OECD) has found that most of its "member countries have defined critical infrastructure sectors, established an inventory of assets, and put in place regulations, national programs, or incentive mechanisms to strengthen the resilience of critical infrastructure to shock events."[4] The definition across OECD countries, including the United States, is intended to define critical infrastructure in the context of shock events, whether physical, cyber, or hybrid. This is known colloquially as an "all-hazards" definition of critical infrastructure.

PDD 63

In the Unted States, the term was introduced into the popular policy vernacular through Presidential Decision Directive 63 (PDD 63), "Critical Infrastructure Protection," signed by then-President Bill Clinton in 1998. PDD 63 states that "It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. I intend that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."[5] PDD 63, which pre-dates the establishment of the Department of Homeland Security, calls for a five-year effort to protect federal, state, local, and private sector infrastructure from intentional acts and says that "Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States."

PDD 63 also provides some of the institutional foundations for critical infrastructure efforts that remain today. Including the beginning of a sector structure and "lead agencies for sector liaison;" the establishment of a National Coordinator; the call for industry and government collaboration through "public-private partnerships," and; the creation of private sector organizations to help government-industry collaboration, known as Information Sharing and Analysis Centers (ISACs).

HSPD 7

The attacks on 9/11 significantly shifted the focus of critical infrastructure protection to one of anti-terrorism. Viewed one way, the 9/11 attacks can be seen as Al Qaeda targeting the nation's critical infrastructure (the Pentagon and the World Trade Center) using critical infrastructure (the aviation system). Raising the level of physical security and access control became the top critical infrastructure priority. Homeland Security Presidential Directive 7[6] was signed by President George W. Bush in 2003 to replace PDD 63 with an explicit terrorism focus. Coming after the establishment of the Department of Homeland Security (DHS), it empowered DHS to take a lead role in much of the protection efforts while maintaining the same general framework for interagency and industry coordination as PDD 63. It also did allow that the DHS Secretary should "continue to maintain an organization to serve as a focal point for the security of cyberspace."

---

[4] https://www.oecd.org/en/publications/good-governance-for-critical-infrastructure-resilience_02f0e5a0-en.html

[5] https://irp.fas.org/offdocs/pdd/pdd-63.htm

[6] https://www.cisa.gov/news-events/directives/homeland-security-presidential-directive-7

PPD 21, EO 13636, and NSM 22

In 2013, President Obama signed Presidential Policy Directive 21 (PPD 21) to return to a more all-hazards approach to infrastructure protection (now replaced by the term "infrastructure security and resilience") and to bring together physical and cybersecurity efforts more explicitly. Crucially, he issued PPD 21 at the same time as Executive Order 13636 on Critical Infrastructure Cybersecurity and more closely connected critical infrastructure security and resilience efforts to national cyber strategy.

In 2024, President Biden published National Security Memorandum 22[7] (NSM 22) which updated – and was significantly consistent with – PPD 21 and focused on the assertion that "The United States … faces an era of strategic competition with nation-state actors who target American critical infrastructure and tolerate or enable malicious actions conducted by non-state actors." It called for a risk-based approach to critical infrastructure security and resilience and for plans and actions for cyber defense campaigns. It did not, however, change the definition nor delineation of critical infrastructure.

As of March 2025, the Trump administration had maintained NSM 22 but has begun to take action to eliminate some of the enabling elements of it, including the DHS Secretary's use of the Critical Infrastructure Partnership Advisory Council (CIPAC) authority.[8]

What Constitutes Critical Infrastructure? ///

Since 2001 and passage of the *PATRIOT Act*, the definition of critical infrastructure has been codified in law as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of them would have a debilitating impact on U.S. security, economic stability, public health or safety, or any combination of these factors."[9]

This transcends policy shifts. Without a change in law, presidential policy does not have the discretion to redefine the term. Instead, what can be done through policy directive is to define how it should be interpreted. That interpretation is very important for policy implementation, however, as it allows for a common understanding of what is critical infrastructure and the ability to identify specific systems, assets, or networks as such.

[7] https://irp.fas.org/offdocs/nsm/nsm-22.pdf
[8] https://www.cnn.com/politics/live-news/trump-tariffs-doge-news-03-10-25/index.html
[9] 42 U.S.C. § 5195c(e).

Critical Infrastructure Sectors

Throughout the four relevant Presidential Directives cited above, critical infrastructure has been delineated primarily in terms of a sector structure, with the most recent NSM maintaining the sixteen sectors identified in PPD 21.

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector

Many of these sectors have, through the work of Sector Risk Management Agencies, Government Coordinating Councils (GCCs), and industry-led Sector Coordinating Councils (SCCs), identified subsectors either directly based on policy guidance or through interpretation. Prominent examples include the Energy Sector, which is divided between Electricity and Oil and Natural Gas subsectors; Transportation Sector, which is divided via modes (Rail, Maritime, Postal and Shipping, etc.); the Government Facilities Sector which has two subsectors that essentially act as stand-alones – Education and Elections; and, Commercial Facilities, which have seven subsectors that literally are made up of hundreds of thousands (if not more) of facilities, such as Real Estate and Lodging.

It was the list of sixteen sectors that then President Biden notably handed to Russian President Vladimir Putin in a 2021 meeting and effectively told him "hands off."

"I talked about the proposition that certain critical infrastructure should be off-limits to attack, period, by cyber or any other means," President Biden, 2021

Relating sectors with assets and systems

As appealing as a sector list is in its simplicity, it has not been very effective in separating what is really critical or, for that matter ,what is "off limits." The simplest way to demonstrate this is start to add up the things that could fall into some of the sectors. There are more than 300,000 water and

wastewater facilities, 100,000 schools; a similar number of hotels and motels; a larger number of government buildings[10] and on down the line.

At purely an asset level, it is possible to quickly come up with a number in the millions in terms of assets, systems, and networks that meet the definition of critical infrastructure by counting assets using the sectoral interpretation. It was this line of thinking that originally got the Department of Homeland Security in trouble[11] in its initial efforts to build a National Asset Database in 2006. This database had an undoubtedly incomplete but relatively manageable list of 77,000-plus assets but included headline-generating exceptions like festivals, popcorn factories, and petting zoos.

Contemporaneously to this critique, DHS sought to address a new congressional requirement through the 2004 *Intelligence Reform and Terrorism Prevention Act* through a change of focus to move from an asset database to a prioritized list of critical infrastructure assets, and, thus, was born the National Critical Infrastructure Prioritization Program (NCIPP).

The NCIPP Process

Originally developed in 2006, the NCIPP identifies critical infrastructure that would result in national consequences if disrupted or destroyed. The NCIPP is supposed to annually prioritize critical infrastructure based on the consequences of an incident impacting those assets.

More than anything, it has been the NCIPP—managed and maintained by the National Risk Management Center, which I led from 2018-2022—that has served as the authoritative analytic view of what is high-consequence critical infrastructure. The NCIPP list, however, has proven elusive at being a clear set of prioritized infrastructure. In 2022, the Government Accountability Office (GAO) reported that, "CISA and other critical infrastructure stakeholders we spoke with reported that the program's results are presently of little use and raised concerns with the program. These concerns included the relevance of the program's criteria given the current threat environment, limited state participation, and lack of use among critical infrastructure stakeholders." GAO also questioned whether the NCIPP was effective for cyber prioritization.

I can attest to those concerns from a firsthand perspective. At different stages, we tried to use the NCIPP to identify priority assets for recovery after hurricanes, organizations that were important to keep functioning during the COVID-19 pandemic, ways to evaluate the prevalence of cyber risks, and protection priorities for potential nation-state attacks. And while it was a helpful starting point, it always fell short as a real-world list because of the ways that the information was collected through state and local government data calls (which were not consistently applied) as well as the

[10] https://www.cato.org/blog/selling-federal-government-buildings
[11] https://www.oig.dhs.gov/sites/default/files/assets/Mgmt/OIG_06-40_Jun06.pdf

way the data was maintained. DHS also places fairly tight information restrictions on the list, limiting its ability to be utilized broadly in real time.

The NCIPP is not the only list of critical infrastructure that exists, however. Perhaps because of the inapplicability of the NCIPP to evaluate criticality from a cyber perspective, in 2013 Executive Order 13636 mandated the creation of what became known as the "Section 9 List," which is also maintained by the NRMC. Section 9 entities are defined as "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects."[12]

The Section 9 list is not public, and, because of the high bar for "catastrophic" effects, is limited to entities in the low hundreds – defined largely as corporations, rather than assets. So, while the NCIPP list may include a critical asset like a data center, an airport, or a nuclear power plant, the Section 9 list would include the corporate owner of that critical infrastructure and be linked to their headquarters. The Section 9 list is largely made up of energy, telecom, and financial sector companies making it a more focused list of high consequence companies but does not well-define the assets and systems those companies operate that must be protected.

Other lists of critical infrastructure exist, too: the Department of Defense tracks "Defense Critical Infrastructure" and other Sector Risk Management Agencies maintain records of critical infrastructure they consider most significant. That said, it is the CISA-maintained lists that serve as the most official analytically-derived standard.

Self-defined and governed sector membership

Another way of defining critical infrastructure is through council membership. Mandated by presidential directive, each critical infrastructure sector and subsector has a Sector Coordinating Council (SCC), established using the CIPAC structure, which is currently being evaluated for continued use. By policy, these non-federal led Sector Coordinating Councils are self-governed and self-defined. Therefore, membership decisions are made by non-governmental organizations, and entities can nominate themselves for membership with peer and near-peer organizations evaluating whether they meet inconsistently applied critical infrastructure criteria.

On its website, CISA hosts many of the membership lists for SCCs, providing a insight into which entities identify as critical infrastructure. The Information Technology SCC[13], for example, has more than one hundred members, including well-known companies like Amazon, Microsoft, Hewlett Packard, Google, and Palo Alto Networks, while also including lesser-known organizations like Obscurity Labs and Hemisphere Cyber Risk Management. It also includes industry associations, such as the Information Technology Industry Council (ITI). And the diverse nature of the IT Sector list is not unique, but, rather, is emblematic of most of the other sector lists.

These lists should not be viewed as an authoritative statement of what is critical infrastructure, however, because, in many sectors industry associations are also members and potentially representative of hundreds of businesses within each sector and subsectors. Additionally, the self-selection methodology used for SCCs allows lesser critical entities to opt in and entities that likely

[12] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
[13] https://www.it-scc.org/current-members.html

would clearly be identified as critical infrastructure to opt out. For example, Bechtel and Nvidia are not members

The Reality: A Broad Definition

The above demonstrates the reality that there is no single list of which entities are considered critical infrastructure and which are not; nor, is there a clear definition of which part of the entity is the most critical. It would seem clear to most that a data center operated by Microsoft in a major urban area is critical infrastructure. The same is likely true for a JP Morgan processing center, a Southern Company nuclear power plant, the Houston Shipping Channel, and a Google or Meta operated underseas cable landing. In such cases the combination of the criticality of the entity to the economy; the function of what they do as it relates to defense, community, and public well-being; and the scale of operations that makes each clearly critical.

But while there are obvious critical infrastructure sites and businesses, there is also plenty of ambiguity in terms of whether there should be a threshold of criticality, and, if so, where the line is. Water and wastewater are essential to all communities' standard of living. Does that mean that all 300,000+ water facilities are critical? If stadiums are critical infrastructure, then is that just at the professional and major collegiate level or does it include minor league stadiums? What does it mean for commercial real estate entities and malls to be critical infrastructure when every mid-sized city in America is full of them?

Perhaps the most significant regulatory effort around critical infrastructure and cyber security to date is the *Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA). The CIRCIA-mandated rule imagines a very expansive view of critical infrastructure which would largely answer the above questions in an inclusive manner.

The proposed rule states that "CISA's proposed Applicability section is designed to focus the reporting requirements primarily on entities that own or operate systems or assets considered critical infrastructure under the PPD-21 definition, while still requiring reporting from a small subset of entities that might not own or operate critical infrastructure but that could impact critical infrastructure to help ensure CISA receives an adequate number of reports overall, including reports of substantial cyber incidents from entities that are most likely to own or operate critical infrastructure."[14] Throughout the proposed rule, CISA maintains that covered critical infrastructure entities should be not based on a criticality threshold as much as a sector linkage, even if the entity is relatively small and the impact of a shutdown of operations would likely not be nationally critical.

[14] https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements

The CIRCIA approach is similar to what is the *de facto* reality of defining critical infrastructure in use today. That is to take a broad interpretation based on sector alignment with little to no emphasis of criticality thresholds. This is because it is hard to know when something becomes critical, and it is important for information sharing purposes.

Work during the COVID-19 pandemic, done largely in a non-cyber context, further demonstrates that the current approach is likely overly broad. During the pandemic response in 2020 and 2021, CISA led an effort to develop an Essential Critical Infrastructure Workers list. The list had several iterations – each more expansive than the last. By the time it was over, researchers found that "the CISA advisory list is highly inclusive and contains most industries and U.S. workers; 71.0% of Census industries comprising 80.6% of workers and 80.7% of NAICS industries comprising 87.1% of workers were designated as essential."[15]

What such an expansive definition of critical infrastructure means is that, in practical terms, critical infrastructure policy has failed as a meaningful driver of risk-based policy and has not effectively allowed for prioritization of security and resilience efforts.

Narrowing the approach to prioritizing criticality ///

So, is there a better approach? While it is true that it is absolutely appropriate to cast a broad net on critical infrastructure for the purpose of information sharing, such an approach should not be the driving default in defining critical infrastructure. Government should not unnecessarily limit information they have about cyber threats and vulnerabilities to only a "critical" subset; nor, should private sector and state and local entities only share information about cyber incidents if they reach some hard-to-measure high threshold. It is important to recognize, however, that a broad applicability for critical infrastructure should not equate to broad prioritization.

There needs to be an ability to more dynamically prioritize the most "critical" infrastructure in the face of cyber and hybrid threats. That prioritization should be done with two metrics in mind: Where does the nation face the most risk from a failure of critical infrastructure and where is there the most opportunity to make an investment that will have the most risk reduction?

Earlier in this document, I laid out reasons why critical infrastructure prioritization matters for cyber security. Several of those needs are not well served by the current approach. They include: identifying the most critical vulnerabilities; having the ability to prioritize critical infrastructure for the purpose of engagement and technical assistance; prioritizing security efforts in the face of incidents, and deepening partnerships with those responsible for the most critical services.

Taking a Lifeline Approach

To meet those imperatives, there should be a new prioritization approach. It should rely on prioritizing the critical infrastructure that supports Critical "Lifeline Functions," which can be defined as functions in which "reliable operations are so critical that a disruption or loss of one of

[15] https://pmc.ncbi.nlm.nih.gov/articles/PMC9347652/

these functions will directly affect the security and resilience of critical infrastructure within and across numerous sectors."[16]

The National Infrastructure Protection Plan defines four lifeline functions as **Communications, Energy, Transportation,** and **Water**. To that list, I would add a fifth: **Cloud Computing and Data Management**.[17] The reason for prioritizing these is that functioning those related infrastructure systems is necessary for national defense, continuity of government, and continuity of operations for Americans' daily lives. Any significant degradation to those systems is likely to have the most immediate and broadest impact (risk exposure), but if they are resilient the scale of harm will be limited (risk reduction).

It is important to note that the five lifeline functions listed above are not simply synonyms for the current sectors, but, instead, are the end state of what multiple sectors produce and what we rely on for the operations of the economy, community well-being, and national security and defense. Each of the sixteen critical infrastructure sectors named in U.S. policy contribute to Lifeline Functions, as well as other important critical infrastructure, such as space systems. But the major distinction is that it is not everything that those sectors that should be prioritized but those that contribute to lifelines.

To operationalize this approach, there should be an immediate effort to document the nodes that are most critical in each of these five Lifeline Functions, based on the scale and scope of the infrastructure within functions. This is a manageable exercise because each of the functions has "use" or "volume" metrics which relate to their criticality to U.S. society. This is the kind of thinking that the RAND Corporation proposed that CISA undertake in delineating Systemically Important Critical Infrastructure, focused on size and interconnectedness[18]. As a starting point, use and volume metrics help define the most critical infrastructure across the five proposed functions. Identifying the companies/entities (if not publicly) that are responsible for the most significant portion of that volume will be important; as, too, will be identifying those systems and assets for key nodes that should form the basis for critical infrastructure asset prioritization.

There should be an intentional effort to learn the most critical and ubiquitous hardware and software – both operational technology and information technology – that enable those functions, because those serve as the basis of needed cyber security enhancements. Important to this will be

[16] https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf
[17] https://www.hstoday.us/featured/column-a-new-lifeline-to-prioritize-in-infrastructure-protection/
[18] https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1500/RRA1512-1/RAND_RRA1512-1.pdf

the identification of materials necessary to produce such functions and adding a supply base that needs to be maintained.

Operationalizing the Approach

What I am proposing is a standing list of: Lifeline functions; major corporate and public entities that operate in those functional markets; key nodes of interconnectedness that facilitate operations; supporting technologies; and enabling materials. In each case, the volume of services delivered, as well as ubiquity in use—a proxy for concentration risk—and the degree to which there are upstream technologies and materials can become the metrics used to measure criticality. This effectively becomes the prioritization of critical infrastructure, as failure of those elements will presumably cause the most risk exposure.

This list should be maintained independently of various attack or failure scenarios but can be customized based on new threat intelligence, prioritized defense scenarios, potential geographic impacts, or other events which could cause harm or threaten operations. There should be a process for this. And the process must include the owners and operators that are most significantly important for the government to engage in setting security priorities and incentivizing security investments. This is why it is crucial that the Secretary of Homeland Security maintain the Critical Infrastructure Partnership Advisory Council, which allows for close industry-government collaboration for planning and risk assessments.

Identifying systemically important critical infrastructure is important, even though such a process has not been fully operationalized within the U.S. government. Nor, has the private sector been empowered to participate. This must change.

There are arguments that this approach is too limiting in terms of prioritization, and that functions such as healthcare delivery, provision of food, and financial services should be on the list of lifeline functions. Those debates can be had, and the initial lifeline list may not be the final one. But it is time to get serious about prioritizing. Focusing on five lifeline functions has the benefit to focus first on things that are most important for national defense and continuity of operations, providing a more streamlined approach to critical infrastructure policy. Bringing discipline to critical infrastructure prioritization must also be aligned with national security priorities and national cyber strategy.

Further critical to this work is that there be a process by which a standing list of priority infrastructure is used to guide security and resilience objectives during normal operations, as well as defense and continuity priorities in periods of heightened risk of incidents. The organization structure is outside of the scope of this paper but there remain natural places like the National Risk Management Center within CISA that can be given this mandate. To be successful, the mandate needs to be explicit from the Executive Branch and have related statutory backing. It also must involve representatives of critical industries most responsible for producing lifeline functions in the process to benefit from their expertise and set the conditions for operational collaboration.

Conclusion ///

The cyber risk from adversaries is not diminishing. Many of those potential adversaries, most prominently the Chinese government, are likely to be strategic in their efforts to cause harm via

cyber and hybrid attacks. The United States has to be equally strategic in its approach to defense. While lip service has been given in the past, it is time to focus on what is most critical and prioritize that in security and resilience efforts. Building off the current approach, while driving toward a meaningful definition of what is most critical is a needed advancement. Focusing on Lifeline Functions allows for that.