Editorial: Emerging Infrastructure Policy of the Biden Presidency and the 117th Congress

Richard M. Krieg
Editor

Introduction

Many years ago, as a public policy graduate student at the University of Chicago, I studied the determinants of successful policy development and implementation. One of the enduring lessons for both domestic and foreign policy was as simple as a saying attributed to Benjamin Franklin: "By failing to prepare, you are preparing to fail."

At the level of Presidential policy leadership, there have been both great achievements and abject failures in our 232-year Presidential history.

John Kennedy's May 1961 policy declaration to land Americans on the moon before the decade's end was a striking success. Three years ago, at the INCOSE EnergyTech Conference in Cleveland, I had a brief conversation with former Apollo astronaut and former U.S. Senator Harrison Schmidt. The Harvard-trained geologist was the only scientist and the last of 12 astronauts to walk on the lunar surface. Since his life had been on the line, he shared how grateful he was for the careful planning and vulnerability assessments that followed Kennedy's pronouncement. Every aspect of moonshot planning was meticulously modelled and tested, with backups for backup systems and more. The best science and scientific minds in the nation were applied to the task.

Some would say that Lyndon B. Johnson's signature program—the Great Society—was, in its own way, just as ambitious. A number of the 226 distinct Great Society bills enacted during President Johnson's two terms were unqualified successes. Again, a Presidential goal was proclaimed: to eradicate poverty in the United States. While there are differences of opinion on whether the billions of dollars flowing from individual Great Society programs were successful in achieving goals, it is undeniable that the lack of adequate planning over an 8-year period led to significant problems and failures. Historian Amity Shlaes writes:

> "By the late 1970s and 1980s, America was ready to look back at the 1960s and evaluate not only the costs but the programs themselves. Had the reforms been worth it? Which individual reform achieved what it had promised? ... the results of many [of these] reforms fell short. Johnson had promised to try to 'cure poverty, and above all to prevent it.' No cure occurred. The government lost the War on

 doi: 10.18278/jcip.2.1.3

> Poverty. Though official poverty levels did decrease over the course of the 1960s, it is hard to prove that the 1960s decrease did not occur because of private-sector growth rather than government efforts. After the 1960s, official poverty stabilized at 10 to 15 percent."[1]

We are now at a crossroads in terms of the nation's critical infrastructure (CI). The centerpiece and core component of all CI sectors is the U.S. electric grid, often described as "the largest and most complex machine ever built by humankind ..." The grid is the structure upon which all of our critical infrastructures rely. And its generation, transmission and distribution components tap into a variety of energy sources that dynamically interact to power American society. It is axiomatic that major public policy shifts impacting the grid be adequately planned and executed.

Since publication of the *Journal of Critical Infrastructure Policy's* Fall/Winter edition, the prospect of a massive federal outlay to infrastructure offers a unique opportunity to address deficiencies in CI resilience.[2] Also, in that brief period, a number of adverse real-world events have underscored the need to do so.

The Colonial Pipeline ransomware attack was the largest oil infrastructure breach in U.S. history, impacting fully 45 percent of gasoline, jet and diesel fuel consumed on the East Coast. The six-day shutdown prompted a Presidential State of Emergency on May 9—and a message delivered in person from President Biden to President Putin to restrict cyberattacks from Russian soil on the sixteen U.S. critical infrastructure sectors.[3],[4] Like the widespread SolarWinds cyber-espionage attack uncovered five months earlier, the Pipeline incident illustrated infrastructure vulnerabilities having national consequence. The attack did not impact operational technology (OT) systems controlling pipeline flow, but rather compromised billing systems and included a 100-gigabyte data theft.[5]

A municipal water system cyberattack three months earlier, however, attempted to usurp system controls. Hackers instructed the public water system in Oldsmar Florida to raise the level of sodium hydroxide in drinking water from

---

1 Shlaes, Amity. (2019). *Great Society: A New History*. Harper Collins.

2 It is important to differentiate between "infrastructure" and critical infrastructure." The latter refers to the 16 national asset sectors established by the Department of Homeland Security: Energy; Defense Industrial Base; Financial Services; Chemical; Commercial Facilities; Communications; Water & Wastewater Systems; Transportation; Nuclear Reactors, Materials & Waste; Information Technology; Healthcare & Public Health; Food and Agriculture; Government Facilities; Dams; Critical Manufacturing.

3 Soldatkin, V. and Pamuk, H, "Biden Tells Putin Certain Cyberattacks Should be Off-limits." Reuters, June 16, 2021.

4 Two other ransomware attacks occurred in June: JBS' Agriculture and Food Sector; and July: Kaseya, Commercial Sector.

5 Bertrand, N. et al., "Colonial Pipeline Did Pay Ransom to Hackers Sources Now Say," CNN Politics, May 13, 2021.

100 parts per million (ppm) to the toxic level of 11,000 ppm. While a watchful employee was able to detect the hijack attempt, foreign or domestic perpetrators demonstrated an interest in manipulating plant controls to poison the water.[6]

Unfortunately, water facility vulnerability to cyberattack is more the rule, than the exception. A recent survey found that only 30.5 percent of public drinking water facilities in the U.S. have attempted to identify cyber vulnerabilities, and 22.5 percent are in the process of doing so.[7,8] As presented in Weiss J, "Control System Cyber Security," *Journal of Critical Infrastructure Policy*, Fall/Winter 2020, breaches involving the IT/OT interface have been widespread in individual CI sectors for decades, with a markedly deficient policy response.

Another recent CI event was the February 2021 Texas power crisis. This grid failure, which followed a series of winter storms, resulted in the tragic loss of 151-700 people (depending on the mortality data source).[9] A complete grid breakdown having far greater human impact was narrowly averted. While one of the immediate causes appeared to be inadequately winterized natural gas equipment, Texas energy market deregulation played a prominent role. A 2011 report predicted that such an event would occur unless remedial action was taken.[10]

Like other recent grid failures, the Texas event highlighted the interdependency of state-level energy sources and the importance of understanding how the interplay of each state's unique energy profile (natural gas, solar, coal, hydro, nuclear, wind, and electricity imports) influences vulnerability in its electricity supply.

Finally, since our last issue was published, a massive solar flare erupted on July 7, 2021, at the start of the current 11-year solar cycle. This X-Class flare (the most powerful solar flare category) did not pose a significant danger to Earth since it was not accompanied by a coronal mass ejection (CME) intercepting Earth's solar orbit.[11,12] It is a reminder, however, that a Carrington Event in 1859, which

---

6 Robles, F. and Perlroth, N., "Dangerous Stuff: Hackers Tried to Poison Water Supply of Florida Town." *New York Times,* February 8, 2021.

7 "Cybersecurity: 2021 State of the Sector," Water Sector Coordinating Council, June 17, 2021.

8 Control system devices such as process sensors, controllers, and actuators operate continuously in real time according to preset parameters. While a cyberattack of the IT or OT Internet Protocol (IP) networks may impact overall efficiency, control system devices are generally not affected by IP cyberattacks. However, these devices and their low-level sensor networks generally have no cyber security, authentication, or cyber logging.

9 Milford, L and Robbins S, "Texas Power Outage Deaths: Is Cruelty and Neglect Our New Energy Policy." *The Hill*, June 28, 2021.

10 "Report on Outages and Curtailments during the Southwest Could Weather Event of February 1-5, 2011: Causes and Recommendations," Federal Energy Regulatory Commission (FERC) and North American Electric Reliability Corporation (NERC), August 2011.

11 Definition Coronal Mass Ejection (CME): https://www.swpc.noaa.gov/phenomena/coronal-mass-ejections

12 CME's when directed at Earth can disturb the planet's magnetic fields, which in turn can create geomagnetic-induced currents. These can flow into power lines and transformers, damaging them.

induced equipment-damaging currents in telegraph lines and ignited fires in some telegraph stations, could have devastating impact on the contemporary power grid's electrical and electronic components, without suitable hardening. For example, it has been estimated that telegraph wires and tappers are about 1,000 times more resilient than power grid SCADA (supervisory control and data acquisition) systems.[13,14,15] There is a 10% to 12% probability per decade of such an impactful space weather event occurring.[16]

It is appropriate to view these and other recurrent challenges as harbingers of future disruption to the Nation's critical infrastructure. Given the complexity and connectivity of CI systems, the identification and scaling of appropriate solutions to threats will require careful planning, perseverance, adaptability, and ingenuity. Importantly, the requisite level of resilience for critical infrastructure cannot be achieved unless public policy addresses the vulnerabilities faced. The policy advances necessary must—through incentives, regulations and other provisions—account for the fact that an enormous percentage of CI assets are owned and controlled by private sector entities.

As noted, at this point in early July, the movement towards a massive general infrastructure bill is perking in Congress, with partisan disagreement on the definition of "infrastructure," tax hikes, revenue measures—and other major sticking points. It is too early to know the outcome in terms of the amount of funding to be approved, what will appear in the final package or packages, whether a reconciliation bill will be enacted, etc.

But it is important to remember at this moment that there was a reason why the word "critical" was placed before the word "infrastructure" in designating a class of national assets that are of paramount importance. Concern about critical infrastructure has a long legacy, emanating from a stream of federal policy development centered around national emergencies and circumstances where regional and national survival is placed at risk. Policy development in the critical infrastructure space has typically been bipartisan, representing a unity of effort that is required for success in this domain. The concept of critical infrastructure became more explicit and was better defined following 9/11, tied to broad recognition of the need for "homeland security."

The logic for a "Critical" Infrastructure distinction is perhaps best expressed in Presidential Policy Directive 21 (PPD-21), issued on February 12, 2013 by the

13 O'Callaghan, J. "New Studies Warn of Cataclysmic Solar Superstorms" *Scientific American*, September 24, 2019.

14 Lovett, R. "What if the Biggest Solar Storm on Record Happened Today? *National Geographic*, March 4, 2011.

15 Lingle, B. "San Antonio Coalition Takes Aim at Electromagnetic Threats" *Government Technology*, Dec 3, 2020.

16 "Powering Through: Building Critical Infrastructure Resilience," InfraGard National Disaster Resilience Council, 2021.

Obama White House. The PPD's preamble reads:

> "It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats ...
>
> The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure—including assets, networks, and systems—that are vital to public confidence and the Nation's safety, prosperity, and well-being.
>
> The Nation's critical infrastructure is diverse and complex. It includes distributed networks, varied organizational structures and operating models, interdependent functions and systems in both the physical space and cyberspace, and governance constructs that involve multi-level authorities, responsibilities, and regulations.
>
> Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery.
>
> U.S. efforts shall address the security and resilience of critical infrastructure in an integrated, holistic manner to reflect this infrastructure's interconnectedness and interdependency. This directive also identifies energy and communications systems as uniquely critical due to the enabling functions they provide across all critical infrastructure sectors ..."[17]

It is appropriate then to ask—among the billions to trillions of dollars proposed in the nascent infrastructure plans—are policy goals spelled out to avert an extended power grid or major communications system breakdown? At this moment, it is fair to say that the major infrastructure proposals released so far do not squarely address safeguards for this type of high-consequence event.

To be sure, the Biden Administration deserves immense credit for moving aggressively on climate change which, when all is said and done, poses substantial challenges across the full range of critical infrastructure installations. Additionally, the President has been uniquely successful in focusing the polity on infrastructure and the nation's abject need for the maintenance and modernization of roads, bridges and the like.

17 Presidential Policy Directive/PPD-21, The White House, February 12, 2013.

The early Administration plan includes investment tax credits to incentivize the buildout of a minimum of 20 gigawatts of high-voltage power lines as well as other grid modernization provisions. Transportation infrastructure priorities would improve resilience in that sector by safeguarding critical infrastructure and services from extreme weather events. Likewise, comments made by Energy Secretary Jennifer Granholm to fully engage the national laboratories in this work were on target and welcome. In my view—at this point in history—our system of national laboratories is uniquely connected to the country's survival.

Subsequent proposals, including an infrastructure compromise between the White House and a group of 11 Republican and 10 Democrat senators also do not mention existing grid and communications vulnerabilities.[18] The plan endorses the call for a Grid Authority which would expedite the linkage of alternative energy sources to the grid and an Infrastructure Financing Authority to leverage billions of dollars into clean energy.

Sharpening the Focus on Critical Infrastructure Resilience

The *Journal's* publication deadline and the pressing issue of CI resilience call me to offer up some initial thoughts on the emerging infrastructure policy.

As mentioned, this is written in early July. Senators from both political parties will soon return to Washington following a two-week July 4th recess to draft their own legislative packages, with the House returning a week after that. The situation is unprecedented. On the Democrat side alone, $3 trillion could be approved,[19] or that plan could come apart as Democrats try to keep moderate Republicans in the fold while accommodating their most progressive members. At the same time, Republicans will draft legislation following the $579 billion agreement they reached for hard infrastructure projects.

In other words, this commentary sits on shifting sands as it is impossible to predict at this point what specific legislative measures will be approved. Moreover, it is possible that serious bills aimed directly at CI resilience may be offered up as free-standing legislation or be merged into the major infrastructure bills of the 117th Congress.[20]

Beyond the infrastructure initiatives spelled out thus far, it is important to state that apart from these bills, the Administration deserves high marks for quick-

18 Fact Sheet: President Biden Announces Support for the Bipartisan Infrastructure Framework. The White House, June 24, 2021.

19 Senate Budget Committee Chair Bernie Sanders has called for $6 trillion.

20 For example, on June 24, a meeting of the full Senate Committee of the Committee on Energy and Natural Resources convened to in part to discuss a lengthy "Energy Infrastructure Act" that does address specific shortcomings in electric grid protection. Likewise, the House Energy and Commerce Committee is reintroducing a number of infrastructure protection bills on the heels of the Colonial Pipeline breach.

ly implementing measures intended to address a number of previous shortcomings in CI protection. In the cyber arena, chief among them was rapid adoption of some core recommendations of the Cyberspace Solarium Commission to solidify and install an Office of the National Cyber Director who will lead development of a National Cyber Strategy. Commission Co-Chairmen Senator Angus King (I-ME) and Representative Mike Gallagher (R-WI) were wise to forward a transition document to the White House in January 2021 delineating Solarium recommendations that were amenable to early approval. These appointments were accompanied by other excellent leadership choices by the Administration in the homeland security and national security spheres that will pay dividends in future CI resilience.

As the contours of a national infrastructure approach and potential budget reconciliation fully emerge, it is important that a full-bore review of CI protection and resilience be planned. Here, it is worth saying that when President Kennedy announced his 10-year moon shot, the longest time an American had spent in space was 15 minutes. Many of the strategies and technologies to secure the nation's CI are yet to be devised, especially on the cusp of the 5G/Artificial Intelligence revolution. But it is also true that the most cost-effective way to harden new power and communications infrastructure is at the point that new installations are designed and built. It would be a missed opportunity of enormous consequence if this does not occur.

The simple fact is that the complex CI threat environment is dynamic and becoming more challenging by the day. Adversaries include nation states, their proxies, and sophisticated private actors. A new national commitment to protect our most essential national assets is necessary both now and as alternative energy sources and other modernization programs come online.

We are living in an era where the remote disruption or incapacitation of critical infrastructure has become a military tool. *Wall Street Journal* writer Rebecca Smith said, "just a few years ago, the idea that foreign enemies could knock out electricity through cyber strikes was the stuff of science fiction ... Ukraine got a small taste of what can happen. Cyber hackers working for Russia crippled 3 Ukrainian utilities on December 23, 2015, plunging hundreds of thousands of civilians into darkness on a chilly winter's eve. A year later, Russian hackers knocked out a major transmission substation, causing another major blackout in the capital city of Kiev."[21]

A week before the Cyberspace Solarium Commission Report was released, Senator King stated, "we are the most wired society on Earth; therefore, we're the most vulnerable society on Earth, and the status quo is not good. One of our [Commission] members represents a utility—they get 3 million malicious hits a day on their systems ...."[22]

---

21 Smith, R "U.S. Officials Push New Penalties for hackers of Electric Grid" *Wall Street Journal*, August 5, 2018.

22 Meeting transcript "Hacking Democracy: A Super Tuesday Kickoff with the Cyberspace Solarium

Having participated in tabletop (TTX) and functional exercises where the power grid goes down for weeks—and having lived through the recent Texas grid failure—it is clear to me personally that after two or three weeks of electric grid outage, communities and families are at extreme risk. Other infrastructures go out as the situation cascades through the economy and local life support systems cease operation. For example, the Water and Wastewater Sector is highly dependent on reliable electric power. Among the sixteen critical infrastructure sectors, healthcare facilities are the most water dependent—after only two hours without water, 67%-99% of hospital functions are fully degraded.[23] In a long-term grid down event covering a wide geographic area, society breaks down due to the general absence of food, water fuel, communications, healthcare and civil order.

Four years to the day before the recent Texas blackouts, I conducted an evaluation of an extended grid outage TTX at the City of Houston's Emergency Operations Center.[24] The exercise outage was caused by a Coronal Mass Ejection (CME). A large group of emergency management agencies, first responders, the Coast Guard, hospitals, and others from the Houston and Galveston areas received a detailed briefing from William Graham, former Presidential Science Advisor and Chair of the *Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack*. Dr. Graham addressed the probabilities and likely impacts of a CME on the grid, telecommunications and other equipment. Following other briefings on CME, and before the TTX began, experts responded to the participants' questions.

I believe that this may be the only time that emergency managers, first responders, and other front-line organizations in a major metropolitan area have been asked to assess the relative importance of grid security compared to other priorities. With a 94% post-event survey return, 76% of the TTX participants felt that "compared to other threats faced" by their organizations or agencies, the electric grid's survivability is "Extremely Important," and 24% believed that it is "Very Important." In response to the survey question, "How important is it to harden the electric grid in order to avert the threats associated with an extended grid failure?" 94% said "Extremely Important" and 6% said it was "Very Important."

The Houston/Galveston TTX participants were correct. Alongside any planning to modernize our electrical infrastructure, it is my view that we need to build adequate power grid and communications system resilience against cyber-threats, physical attacks (especially against extra-high-voltage transformers), and electromagnetic threats (solar storms, nuclear EMP, radio frequency weapons),

Commission" Center for Strategic and International Studies, March 4, 2020.

23 *National Infrastructure Advisory Council (NIAC), DHA OCIA, Sector Resilience Report,* 2014, pp. 19-20.

24 Krieg, R. *"Exercise Evaluation: The 2017 Texas High Impact Threat's Workshop."* Harris County Office of Homeland Security and Emergency Management, February 15, 2017.

and combined attacks. Any infrastructure plan that does not protect against these high-impact lower probability events will be incomplete and imprudent. For example, a buildout of the long-distance transmission system to move renewable energy to metropolitan centers invites a calamity of major proportions if it is not protected against natural disasters and deliberate attack.

While attention is paid to the modernization of resilient transmission lines, infrastructure plans to date appear to be silent on the grid's generation and distribution components. Although the descriptors "transmission" and "distribution" may seem only subtly different since both are pathways to deliver electricity, the substance of the distinction is important. Distribution lines comprise over 90% of the national grid's electric lines. This distribution infrastructure delivers electricity to private citizens, commercial, government, and other customers providing essential services, including hospitals, water-wastewater management and delivery, emergency management, essential communications, businesses, strategic industries, transportation, etc. For example, a team from the Johns Hopkins University Bloomberg School of Public Health reported in our Spring/Summer edition that healthcare delivery systems are extremely vulnerable to a prolonged loss of electric power, particularly an extended regional or multi-region breakdown of the electric grid's distribution system.[25]

While a major build out of localized clean energy sources can inherently make the overall power system more resilient through alternative power generation, microgrid islanding, long-distance transmission and through other means, there is still a need to smartly harden these assets. This includes regional control centers, sub-stations, supervisory control and acquisition (*SCADA*) systems to which they connect. The focus should include grid and communications system resilience to electromagnetic and geomagnetic threats as well as cyber intrusions, including those having the capacity to impact OT controls. Critical components include the internal communications systems that permit the electric grid to function.

Attention is also needed to compensate for the intermittent nature of solar and wind power and enabling renewable sources to function during long-term emergency situations. Policy makers must also understand that renewable resources can increase the cybersecurity threat to utilities compared to many fossil fuel facilities. Solar installations and wind turbines generally have little cyber protection. "Controlling renewable resources is complicated and requires advanced control techniques that are highly sensitive to sensor input. Consequently, renewable resources are very good for the environment and reduce consumer costs, but they are not a panacea to reduce electric grid cyber threats ..."[26]

A major ambiguity in infrastructure bills as presently described, are a de-

25 Sell, T.K., Lien, O. and Toner E. "A Framework for Healthcare Resilience During Widespread Electric Power Loss" *Journal of Critical Infrastructure Policy*, Spring/Summer 2020.

26 Weiss, J. "Renewable Resources Can Increase Cyber Threats" Control Global.com, July 22, 2018.

scription of the full roles and functioning of the proposed Grid Authority. The primary intent of the Authority is to expedite the movement of renewable energy by expanding transmission lines from wind and solar sources to population concentrations in large metropolitan areas. It would be useful to consider assigning responsibility to this body, or another highly positioned group, to oversee a sufficiently staffed effort to protect the nation's power and communications infrastructures from major threats faced. In order to act efficiently and independently, it is recommended that the Authority or alternative group be receptive to input from the Federal Energy Regulatory Commission (FERC) and the North American Energy Reliability Corporation (NERC), but also be formally aligned with national security and homeland security agencies.

There are two interconnected timeframes within which to consider suitable grid protections for the major vulnerability and threats faced. The first is the 10-year interval estimated for completion of the transmission lines incorporated in current infrastructure plans.[27] The second is for the period after that. Again, emphasis should be placed on grid resilience, focusing on cyberthreats, physical attacks (especially against extra-high-voltage transformers), electromagnetic threats (solar storms, nuclear EMP, radio frequency weapons), and combined attacks.

In this pursuit, it will be helpful to review the full body of previous work aimed at upgrading electric grid and communication systems resilience. They include the findings of (and technical updates to) the federal Commission to Assess the Threat to the United States of Electromagnetic Pulse (EMP) Attack[28] and subsequent Commission reports. Among other recommendations, in its most recent (2017) report, the Commission recommended that "the President establish an Executive Agent with the authority, accountability, and resources to manage U.S. national infrastructure protection against the existential EMP threat." A 2018 "Electromagnetic Defense Task Force Report," produced at Air University/Maxwell Air Force Base following a conference of national experts on the topic, is useful.[29] While one may differ with individual report assumptions or conclusions, its call for robust national policy in response to the current electromagnetic threat environment is correct. The findings of national space weather action plans should also be carefully reviewed as well as other work produced or compiled by the Space Weather Operations, Research and Mitigation Group (SWORM).[30] Finally, as previously mentioned, the bipartisan *Cyberspace Solarium Commission Report* created by the National Defense Authorization Act for FY 2019 should be utilized.

27 Stein, J. and Eilperin, J. "What's in the White House, Senate Bipartisan Infrastructure Package." *The Washington Post*, June 25, 2021.

28 Title XIV, National Defense Authorization Act FY2001 (enacted into law by PL 106-398, 114 Stat. 1654A-345.

29 Stuckenberg, D., Woolsey, J., and DeMaio. Electromagnetic Defense Task Force 2018 Report. Air University Press, Maxwell Airforce Base.

30 Space Weather Operations, Research, and Mitigation (SWORM) Interagency Working Group Site.

In addition, pilot projects that have emerged locally should be fully supported and studied. The bubble up approach to CI protection has applicability to both traditional and clean energy sources. The Joint Base San Antonio Electromagnetic Defense Initiative (JBSA-EDI) is a robust collaboration intended to create resiliency across the Base and San Antonio to a catastrophic electromagnetic pulse and other events that could cause a long-term regional power outage.

The Lake Wylie Pilot Study is an important South Carolina effort that, like JBSA-EDI, consists of a broad coalition of participants including local utility companies, universities, a large number of community organizations, and other committed partners. Among core priorities, Lake Wylie has focused on assuring distribution grid viability by protecting key life supporting infrastructures against EMP. While based in York County, the initiative template can be readily expanded to adjoining counties and to other states in that region.

In considering the above suggestions, it is appropriate to ask whether the current set of infrastructure designations—the sixteen broad Federal CI sectors—are sufficient to rapidly build CI resilience. It is arguable that a new basis to identify and codify by law the most critical nodes and components of our CI should be seriously considered. The new approach could facilitate screening CI sites to produce a more manageable and affordable set of subsystems and nodes that would be the highest priority targets for protection.

A starting point is the National Critical Functions Set released by DHS's Cybersecurity and Infrastructure Security Agency (CISA) in April 2019 and last revised in February 2021. These designations are useful from the vantage point of risk and dependency analyses, consequence modeling and other priority needs. They are essential to produce useful public-private sector dialogue.

The need for more fine tuning of the sixteen CI sectors also emanates from security lapses that have occurred between government and the private sector in planning, controlling and operating CI. One need only look at the war fighting aircraft of specific adversaries to surmise that cyber espionage may have occurred with respect to private entities in the Defense Industrial Base and Critical Manufacturing Sectors.

But any attempt to expand government prerogatives places in counterpoint two vital needs: the need to provide upgraded security in a dangerous world with the need for excellence, innovation and other advantages (including security) conferred by private sector CI control. This distinction was quickly overcome—and trust levels immediately enhanced—by the national mobilization needs of World War II. In peacetime, it is far harder to develop trust between relevant public and private players who are essential to national security.

In the cybersecurity area, the Solarium Commission recommended that a concept of "Systematically Important Critical Infrastructure (SICI)" be codified into law. The private entities responsible for the most important critical systems

and assets in the U.S., would be granted special assistance from the federal government as well as assume increased responsibility for additional security and information security requirements that are vital to their unique status and importance. Following the Colonial Pipeline Attack, co-chairs Senator King and Representative Gallagher said,

> "The systemically important critical infrastructure (SICI) entities, and their most vital systems and assets, are pressure points in our grid, and targets for both nation-state adversaries and criminal actors, allowing them to scale up the effects of cyber campaigns and thus the risk they can pose to the United States in peacetime and in crisis. It is well past time for the Federal government to enhance its partnership with these entities and ensure these companies are executing their security responsibilities effectively."[31]

The logic for this approach—along with its benefits and burdens—is effectively stated in Jhangiani, T. and Kennis, G.'s "Protecting the Critical of Critical: What is Systematically Important Critical Infrastructure,"[32] and political considerations are summarized in: "A Plan to Label Companies Vulnerable to Hacking is Set to Spark Debate on Capitol Hill."[33]

In this area, it is also desirable to consider the benefits, costs and risks of organizing a large complement of Red Team monitors.[34],[35] These well-trained individuals would attempt to penetrate the defenses of specific critical infrastructure installations in both the public and private sectors. It has been estimated that 85% to 90% of cyber-attacks could be stopped if facility personnel (1) did not respond to phishing emails; and (2) maintained two-factor authorization. A near zero tolerance policy for workers and supervisors who violate basic cyber hygiene principles as well as other safeguards might be configured for our most important infrastructures—where national security or public safety is put at risk by negligence.

---

31 Press Release, Cyberspace Solarium Commission Co-Chairs Issue Statement on Colonial Pipeline Cyberattack, May 10, 2021.

32 Jhangiani, T and Kennis, G, "Protecting the Critical of Critical: What is Systematically Important Critical Infrastructure?" Lawfare Institute/Brookings, June 15, 2021.

33 Starks, T. "A Plan to Label Companies Vulnerable to Hacking is Set to Spark Debate on Capitol Hill." Cyberscoop, June 22, 2021.

34 Red Team: "A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders in an operational environment. Also known as Cyber Red Team." U.S. Department of Commerce, National Institute of Standards and Technology.

35 The specific functions and institutional placement for such a capability must be carefully considered to minimize distrust and to obtain a buy-in for all players. Among other options, a quasi-governmental agency or similar body might be considered.

My view is that the SICI designation or something like it needs a fair hearing and decisive action. Ronald Reagan's 1986 refrain that "the nine most terrifying words in the English language are 'I'm from the government and I'm here to help'" still resonates in the private sector, and a deep national schism continues to exist in relation to government regulation. The debate is an important one. But in some respects, the stakes today are comparable to, if not more immediately serious to the homeland, than those faced prior to the 1940s.

Our critical assets must be secured before it is too late. The Administration and Congress have a historic opportunity to protect the electric grid and other CIs against high impact, lower frequency events while achieving other important policy goals.