A Legal Framework for Enhancing Cybersecurity through Public-Private Partnership

The Honorable Joe R. Reeder
Professor Robert E. Barnsby

ABSTRACT

The Cyberspace Solarium Commission (CSC) published its report in March 2020 offering emphatic, far-reaching recommendations in the cybersecurity domain. This report highlights the rapidly growing importance of public-private partnership (P3) in this domain as a national security cornerstone, and significantly informs the debate over the public-private balance in the cybersecurity system of governance in the United States. While important questions remain as to the best ways to safeguard public law values, the report strongly supports arguments for informed P3 collaboration, and further discourages the notion that cybersecurity should exclusively be an inherently governmental function. A legal analysis of partnering in the cyber domain suggests the risks of violating existing inherently governmental function rules are low, and navigable. Indeed, the CSC's strong, bipartisan report accepts this as a given point of departure from the *ad hoc* P3 system we have today, and recommends concrete steps to advance national security and other public law values such as accountability, transparency, fairness, and privacy. Like legislation that set the stage for the NASA-SpaceX partnership, the CSC's unequivocal embrace of P3 in the cybersecurity realm has great potential to guide legislation and other steps to reshape and adapt "defense-of-nation" Cyber domain efforts.

The Honorable Joe Reeder, a West Point graduate (1970), served in the 82nd Airborne Division and was the Army's 14th Under Secretary and Chairman of the Panama Canal Commission (1993-97). A television commentator on national security and legal issues, he has published a number of articles and editorials, and represented nations, companies, law firms and entertainers as a partner at Greenberg Traurig, LLP, one of the world's largest international law firms with over 2,200 attorneys.

On March 11, 2020, the Cyberspace Solarium Commission (CSC),[1] a Congressionally-established bipartisan task force, released its final 174-page report, covering many pressing national security issues related to cybersecurity.[2] The CSC's "urgent call to action,"[3] recommends selection of a National Cyber Director, creation of a Cybersecurity Bureau within the State Department, and strengthening of the Cybersecurity and Infrastructure Security Agency (CISA). These are but three of the 82 recommendations organized along six policy pillars in the critical Cyber domain. [4] The importance of the issues addressed cannot be overstated, as emphasized by recent authors exploring the impacts of the CSC recommendations, with more commentary to follow.[5]

As lawyers, we appreciate the Commission's efforts to provide a definitive, coherent roadmap for future legislation, particularly iterations of the National Defense Authorization Act (NDAA) that likely will include provisions supporting many Commission recommendations. Although a complete "legal unpacking" of all aspects of the Commission's comprehensive report is an important task, our focus here centers exclusively on the fifth of the Commission's six pillars[6]—and its emphatic view that the United States Government (USG) should take a bold lead in working much more cohesively, collaboratively, and comprehensively with the private sector on national cybersecurity. Calling for significant steps forward in P3 law, the Commission makes strong, unequivocal P3-related recommendations, authored in consultation with several of the nation's brightest legal minds on this subject.[7] The CSC's bipartisan consensus on the heretofore contentious issue as to P3 boundaries will richly inform discussions on the appropriate balance in P3, and shift the debate from "whether" to "when" and "how" governmental actors should share cybersecurity functions with, or in some cases shift them to, the private sector. From a legal perspective, this consensus un-

Professor Rob Barnsby, also a West Point graduate (1996), is the Cyber Law Fellow for the Army Cyber Institute at West Point, where he teaches Cyber Law and Constitutional Law in the U.S. Military Academy's Department of Law. He recently served as a Visiting Assistant Professor at the University of California, Berkeley, School of Law, and has published several scholarly articles on a wide variety of cyber and legal subjects. In his twenty years of service as a U.S. Army officer, Rob led high-visibility legal teams in strategic locations throughout the United States and Afghanistan. Rob earned his J.D. from the William & Mary Law School, where he served as Executive Editor of the *William & Mary Law Review*.

derscores the importance of a successful P3 collaboration in optimizing the nation's cybersecurity, as we illuminate below with a "totality of circumstances" and public law values-based analysis.

Before the Commission's work, legal discussions on public-private partnerships in the cyber realm meandered among interesting but ultimately inconsequential cybersecurity P3 "cocktail party" conversations.[8] Some legal scholars voiced concern that cybersecurity partnerships in defense of the nation could violate longstanding rules that bar the outsourcing of "inherently governmental functions,"[9] and that fundamental "public law values [may be violated] when government functions are contracted out to private parties."[10] On the other hand, national-level cyber policy, along with unclassified Presidential and Department of Defense (DoD) strategy documents, increasingly have suggested otherwise and, over the course of several recent iterations, included policy pronouncements "incentiv[izing] cybersecurity investments ... [to] work with private ... sector entities to ... realize benefits from those investments,"[11] and urged DoD to "build trusted private sector partnerships."[12]

The bipartisan CSC team—including both public- and private-sector partners with executive and legislative, legal and non-legal members—resoundingly calls for lasting partnerships without even a mention of legal impediments. This should guide further debate as to USG partnering with the private sector in "defense of the nation" from a cybersecurity perspective.[13] "Totality of the circumstances" analysis amply supports the conclusion that national-level cybersecurity per se is not—and, essentially, cannot be—an inherently governmental function.[14] Rational analysis also confirms that our nation's current cybersecurity construct neither violates the law nor, with appropriate governance and CSC-recommended legislation, will it unduly risk undermining public law values going forward.

The recent SpaceX launch of the first-ever commercially built spacecraft provides a good example of a successful and highly functional public-private partnership executed at the highest levels of government and industry.[15] From a national and legislative perspective, this successful partnership would never have formed without passage of the NASA Transition Authorization Act of 2017, wherein Congress affirmed its "commitment to the use of a commercially developed, private sector launch and delivery system to the [International Space Station] for crew missions."[16] This Congressional language enabled NASA to work with the private SpaceX company to accomplish the historic space mission our nation witnessed this summer.[17]

Until quite recently, few believed space exploration would begin to include private sector competition for direct and large-scale work with the USG, yet SpaceX and its private competitors—with fulsome USG cooperation—changed that narrative. The USG has not abandoned its dominant Space domain role. Nor should or will it abandon its preeminent "defense-of-nation" role in the cybersecurity domain. Nevertheless, Congress must prioritize focus on the CSC recommendations and better enable the respective public and private cybersecurity actors to collaborate effectively, as occurred with public and private space actors in 2017.

The Pacific and Atlantic Oceans—7,000- and 4,000-mile geographical barriers that have militarily protected the United States for nearly 250 years—provide not even speed-bump protection from cyber devastation. Equally if not even more ominous is the ubiquitous nature of cyber "weapons," so easily accessible to the general public, unlike tanks, missiles, and military aircraft. These evolving circumstances mean certain P3 roles and missions in cybersecurity must be clarified, and even codified, given the pervasive private sector presence in, and ownership and/or control of, critical cyber infrastructure—in some estimates as high as 85% of the overall infrastructure.[18] CSC Recommendation 5.2 calls upon Congress to establish and fund a Joint Collaborative Environment, a common and interoperable environment for the sharing and fusing of threat information, insight, and other relevant data across the federal government and between the public and private sectors. CSC Recommendation 5.3 urges Congress to establish a public-private, integrated cyber center within CISA in support of the critical infrastructure security mission and to conduct a one-year, comprehensive review of federal cyber and cybersecurity centers, including plans to develop and improve integration.[19]

The Commission's Final Report also underscores the serious vulnerability of our nation's infrastructure, forewarning the threat not only to structures, (e.g., energy plants and power grids), but also to the US water supply. Typically, local municipalities oversee the water supply, with governance and security standards varying widely, sometimes falling well below our nation's lowest common denominator vis-à-vis "best practices." Cyber protection of our nation's water utilities and resources may lack the security alarm bells that accompany reportable metrics, and can be shortchanged by municipalities that face budgetary constraints.[20] These vulnerabilities illustrate that with or without enabling legislation, going forward, private security actors will play an increasingly larger role in the nation's cybersecurity. For the sake of US

national security, laws are urgently needed not only to empower P3 collaboration but also to provide clarity as to the lines and divisions of labor and authority between the public and private actors. Such clarity has become time-urgent, as some of our closest allies have recognized and already addressed.[21]

Despite decades of debate evolving on the role of private actors in "defense-of-nation" cybersecurity, official direction for the USG to partner with the private sector has consisted mostly of generic pleas to "work with the private sector."[22] Even the most recent DoD cyber strategy document contained only generic guidance to "expand DoD cyber cooperation with . . . industry," "work with the private sector," and "[b]uild trusted private sector partnerships."[23] Congress upgraded the conversation for the first time in the 2019 National Defense Authorization Act,[24] with its call for a formal commission to report on the nation's cybersecurity.

Following ten months of concentrated effort, the CSC proposed a P3 plan to "[o]perationalize cybersecurity collaboration with the private sector."[25] The CSC plan also urges the USG to unleash its "unique authorities, resources, and intelligence capabilities to support [private-sector entities]."[26] Its plan envisions an overall layered approach to deterrence. It also features "international engagement and cooperation," enforcement of already agreed norms in the cyber realm, and use of non-military tools (including information sharing). The CSC Report also urges "align[ment] of market forces" and "explor[ation of] legislation, regulation, executive action, and public- as well as private-sector investments," featuring "partner[ship] with the private sector and [an adjustment to] incentives to produce positive outcomes."[27] CSC Recommendation 5.2, calls for a "joint collaborative environment," and is further etched by CSC's Recommendation 5.3, which calls for the physical housing and ownership of this collaboration mission within the Department of Homeland Security's CISA. These recommendations are key to a culture of real-time P3 information sharing and joint analysis, and should be deemed essential.

We turn now to how CSC Report P3 recommendations help to illuminate the path toward an optimal design and governance of our nation's cybersecurity P3 relationships—whether through soft regulation, such as CSC's high-visibility recommendations, or with implementing regulations. One important requirement will be to avoid delegating missions to the private sector for which it is either unsuited, or hopelessly conflicted, for example, by profit considerations. Subpoena powers of the court, and other missions historically policed or performed by the government provide yet other examples of missions many believe are governmental per se and should stay there. Since 1983, such "contracting out" of functions to the private sector has been circumscribed by the Office of Management and Budget's (OMB) Circular Number A-76, which delineates those activities that private-sector entities are authorized to perform. Most recently revised in 2003, OMB Circular A-76 has consistently barred the USG from using commercial sources for functions "inherently Governmental in nature,"[28] which it describes as those functions "so intimately related to the public interest as to mandate per-

formance by Government employees."[28] Put another way, A-76 flagged certain activities as off limits for "contracting out" to the private sector, because the private sector's profit motive could undermine or otherwise conflict with the public's best interests. Under this reasoning, certain policy making decisions are quintessentially governmental in nature, and thus to be entrusted to and performed solely by the government. Examples include "act[s] of governing [which involve the] discretionary exercise of Government authority [e.g.,] criminal investigations, prosecutions and other judicial functions; . . . management and direction of the Armed Services . . . [and] direction of intelligence and counter-intelligence operations."[30] In recent armed conflicts, the inherently governmental nature of classic battlefield operations reserved to States under the Law of Armed Conflict, including detention and interrogation on the battlefield, has also been reinforced.[31]

Recent legal scholarship adds to the A-76 understanding in this area, particularly in the skillful analysis of cyber law scholars such as Kristen Eichensehr.[32] She suggests that—whether or not OMB Circular A-76 should bar privatizing certain aspects of cybersecurity—our existing cybersecurity system exposes to abuse certain fundamental public law values (e.g., privacy, fairness and transparency). In her 2017 *Texas Law Review* article, Professor Eichensehr advanced three basic reasons for not outsourcing cybersecurity to the private sector: (1) a well-functioning government should be capable of defending computer networks at the national level; (2) to do otherwise places the private sector in a quasi-governmental role, and otherwise compromises public law values with corporate profit motives; and (3) it is important to avoid undue private-sector corporate access to sensitive private individual information—despite Eichensehr's observation that "individuals . . . are typically more concerned about the government accessing their private information than about corporations accessing it."[33] Eichensehr essentially argues that "certain [cybersecurity] functions exist solely in the realm of government and within the expectations of the state."[34] While we would take issue with any blanket assertion that our government alone can ever be the sole, stand-alone guarantor of our nation's cybersecurity, Professor Eichensehr's analysis undoubtedly will and should inform further thought as to optimal legal ground rules for policing public-private partnerships in the cyber domain, and where lines should be drawn to prevent the privatizing of inherently governmental functions.

Unlike judicial activities and other conspicuously governmental functions,[35] computer network functions are neither obviously nor exclusively designed to be delivered by governmental elements. Such activities thus warrant further analysis under the OMB Circular's Supplemental Guidance and what it styles as "totality of the circumstances." The "determin[ation as to] whether a function is. . . inherently governmental. . . depends upon . . . a number of factors, and the presence or absence of any one is not in itself determinative of the issue."[36] OMB's guidance requires examination of many factors likely to impact any of the public law values alluded to above, and allows for the informed judgment of decision makers on a case-by-case basis. Such judgments will play a key role in the evolution of Cybersecurity P3. For example,

a most important question is whether defense of the nation's computer networks, in totality, should—or even could, as a practical matter—be exclusively regulated by the government, and hence beyond the purview of the CSC-envisioned public-private partnerships. Fortunately, this question, at least for now, has been resolved in favor of P3.

Another OMB factor in the proper division of labor between the government and private sectors is the "status quo ante." The OMB Circular's Supplemental Guidance observes that those functions already being performed by private parties are more likely to remain acceptable under P3 legal analysis.[37] It would be hard to overstate the pervasive extent to which the private sector already is deeply embedded in myriad aspects of our nation's cybersecurity, a subject others have described at length in this and many other publications.[38] While not by itself a dispositive factor, the private sector's long-standing performance of cybersecurity functions strongly supports the conclusion that continued private-sector participation should be considered "A-76 permitted," especially the P3 undertakings contemplated in the CSC Report. Similarly, the Supplemental Guidance allows for disclosure to the private sector of sensitive technical complexities, particularly where private actors possess as much, if not more, technical knowledge. Again, rudimentary knowledge of computer networks confirms that highly sophisticated cyber-sensitive technical expertise resides in the private sector—another factor under A-76 that supports fully integrated public-private partnerships and collaboration. For example, Eichensehr notes that the private sector, led by industry titan Microsoft, essentially pioneered the legal tactics (which necessarily utilize public-private collaboration) employed to take down operations of various cybercriminal-deployed botnets.[39]

Cost concerns also figure into analysis as to whether a particular function should be privatized. Redundant, expensive, and pre-existing national structures obviously are undesirable. Yet expensive and often sophisticated cybersecurity measures generally coexist wherever both private and public sector computer networks reside. Thus, from a cost perspective, requiring a uniquely governmental cybersecurity apparatus—parallel to a pre-existing private apparatus—essentially would call for a function falling outside A-76's "inherently governmental" scope.

Apart from her A-76 analysis, Professor Eichensehr eloquently explains why we also must ask whether privatization of cybersecurity violates public law values such as privacy, fairness, or transparency. Here, bipartisan operation and reporting of CSC, including its strong call for robust public-private partnerships, serves as a model of transparency.[40] As is true of accompanying Congressional oversight, enabling laws and regulations likely to implement CSC recommendations, by their nature, will be transparent in governing our public-private partnerships. New legislation combined with enforcement of existing Competition in Contracting Act (CICA) oversight should further mitigate fairness concerns, as CICA was enacted in order to even the playing field in competition for government contracts.[41] Actual awarding, administering, and terminating contracts are inherently governmental functions that generally are not outsourced.[42]

We are wary of urging blanket rules in the evolving governance of P3 cybersecurity partnerships, absent compelling exigencies, yet decision-making functions tainted or impaired by a competing profit motive should never be outsourced to a non-governmental authority. For example, much has been written about the Army's ill-fated Future Combat Systems that, but for a few spin-off technologies, had no fielded system and nothing else to show for the over $18 billion in taxpayer dollars expended.[43] This costly lesson traces directly to a procurement decision that empowered two companies, Boeing and SAIC, that were neither disinterested parties nor otherwise rendered so, and yet essentially made contract award decisions in selecting participating contractors. Privatizing this decision-making power of what many consider an "inherently governmental function" simply did not work.

A more workable example, we hope, is the ongoing Cybersecurity Maturity Model Certification (CMMC) requirement, wherein DoD is outsourcing a key function of this requirement. Specifically, DoD has empowered (a) Cybersecurity Maturity Model Certification Accreditation Body, Inc., an independent non-profit entity, to accredit CMMC Third Party Assessment Organizations (C3PAOs), and (b) individual evaluators to perform CMMC assessments of current and potential DoD contractors. A CMMC assessment and certification is now being required at one of several different levels as a prerequisite for doing business with DoD. This process includes a cadre of non-government auditors deciding which companies will, or will not, qualify for DoD contracts. No direct profit motive impairs the CMMC process, but we anticipate legislative concerns as to the oversight of this now delegated function, which potentially will influence tens of billions of dollars of DoD contract awards. Indeed, on September 16, 2020, it was reported that two members of CMMC's Advisory Board were forced off the Board, due to an alleged "pay for play" partner program, with charges as high as $500,000 "as a way to promote certain companies over others."[44]

Enforcement of existing legislation, accompanied by other policy changes and executive actions, must continuously include monitoring of the oversight of protections for delegated core public law values, and this should be integral to codification of the CSC's P3 recommendations described above. Properly monitored and protected with checks and balances, the proliferation of partnerships over time should reinforce a level of trust between public and private sector actors—a trust that must be nurtured and can never safely be taken for granted.[45]

In *The Cyber Defense Review*'s Spring 2020 issue, Professor Jim Chen underscores the importance of trust in effectively administering cyber security in the continuum of public-private interface, *i.e.*, in the spectrum running from "cooperation, to collaboration, to full integration, and explains why and how a sound framework for full-scale public-private collaboration can and ultimately should exist."[46] Moreover, with focus on laws designed to protect public-value interests, as discussed above, the CSC's strong endorsement of the technical and pragmatic reasons for expanding our P3 provides a major step forward. Realistic analysis of what are and are not "inherently governmental functions" should continue, but

more attention must focus on assuring a robust role for an empowered private sector which already is pervasively invested in the nation's cybersecurity. With thoughtful design, that role, consistent with public-value interests, can be greatly expanded and much better integrated. This discussion of A-76 and "totality of circumstance" analysis, to include the importance of "trust" Professor Chen highlights, all go to reinforce the CSC's strong argument in support of the P3 partnership.[47] For our national cybersecurity efforts to work optimally, the legal scales must tip to align better with broader and deeper private-sector participation.

NOTES

1. Established in the John S. McCain National Defense Authorization Act for Fiscal Year 2019, the Cyberspace Solarium Commission comprised fourteen commissioners, including four currently serving legislators, four executive branch leaders, and six experts with extensive backgrounds in industry, academia, and government service, (https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.) The Commission's definition describing cybersecurity, adopted here, is the "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication. This includes ensuring the availability, integrity, authentication, confidentiality, and nonrepudiation of the information contained therein, " (United States Cyberspace Solarium Commission, Final Report, March 2020, 132). The authors thank CSC members Professor Frank Cilluffo (Commissioner), RADM (Ret.) Mark Montgomery (Executive Director), and Professor Erica Borghard (Senior Director) for sharing valuable insights as to some of the critical aspects of the Commission's work. Thanks also go for suggestions provided by John Felker, former Director of the National Cybersecurity & Communications Integration Center (2015-19), and earlier, Deputy Commander of the U.S. Coast Guard Command (2010-12). The authors also thank Chip Leonard (USMA 1970) and Greenberg Traurig's Shomari Wade for their valuable editorial insights and suggestions. Views and shortcomings expressed here are exclusively the authors' responsibility, and do not necessarily reflect official policy or positions of the U.S. Military Academy or any DoD agency.
2. United States Cyberspace Solarium Commission, Final Report, March 2020, https://www.solarium.gov/report.
3. Ibid.
4. Ibid. *See also* Cyberspace Solarium Commission Testimony Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation of the Committee on Homeland Security, U.S. House of Representatives, July 17, 2020, 2.
5. *See, e.g.*, Kristen Eichensehr, "Public-Private Cybersecurity," *Texas Law Review,* 2017, further described throughout this work.
6. Ibid. Those six pillars are: (1) Reform USG's Structure and Organization for Cyberspace; (2) Strengthen Norms and non-military Tools; (3) Promote National Resilience; (4) Reshape the Cyber Ecosystem toward Greater Security; (5) Operationalize P3 Cybersecurity Collaboration; and (6) Preserve and Employ the Military Instrument of Power.
7. CSC Legal Advisors included Stefan Wolfe, General Counsel; Corey Bradley, Deputy General Counsel; Cody Cheek, Legal Advisor; David Simon, Chief Counsel for Cybersecurity and National Security; Veronica Glick, Deputy Chief Counsel for Cybersecurity and National Security; and Joshua Silverstein, Deputy Chief Counsel for Cybersecurity and National Security. U.S. Cyberspace Solarium Commission, Final Report, March 2020, *supra* note 2, 151.
8. *See infra* notes 11, 12, 22, 23, and accompanying text.
9. *See infra* notes 28-31 and accompanying text.
10. Kristen Eichensehr, "Public-Private Cybersecurity," *Texas Law Review,* 2017, *supra* note 5 (although Eichensehr describes an informal public-private *system*, not a partnership).
11. National Cyber Strategy of the United States of America, September 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
12. Department of Defense Cyber Strategy Summary, 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF). *See also* H.R. McMaster, "Battlegrounds—The Fight to Defend the Free World," Harper-Collins (September 2020), 71-79. The General explains why today's battlefield goes far beyond kinetic military operations. And, pertinent here, in the context of Russian aggression, he concludes that, while no combination of P3 efforts to counter foreign cyberattacks will permanently resolve the threat, [p]rivate-sector effort can create a firehose of truth to counter [any] firehose of falsehoods." Ibid., 74.

NOTES

13. Law enforcement (e.g., power to issue subpoenas), and classified access/need to know considerations bring some aspects of the nation's cybersecurity closer to the ambit of "inherently governmental," and hence less susceptible to public-private partnering. The CSC Final Report itself discusses at least one specific example, wherein current laws impede victim companies from effectively "stalking" the cyber-stalker, or at least identifying such bad actors in defending their assets. United States Cyberspace Solarium Commission, Final Report, March 2020, *supra* note 2, 104 (https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkfl0MxIXJGT4yv/view). Notwithstanding the law enforcement and classification functions which fall closely if not squarely within the ambit of "inherently governmental," *Wired Magazine* flags another function many consider "inherently governmental," to include the collecting, counting, and recording of election votes. This article recounts the extraordinary collaborative efforts now and for more than a decade underway, in what may prove to be the most promising voting technology breakthrough since the late 19th century, when voter privacy was enshrined as a top priority, but at the cost of sacrificing another pivotal public interest value—transparency, and one's ability to confirm that his/her vote was actually counted. Harnessing Microsoft Research, a mammoth, private sector replica of DARPA, every American voter, using a homomorphically encrypted voting scheme, may soon be able to validate his/her vote without compromising the privacy of that vote. *See* "Lone Star—A More Perfect Election" *Wired Magazine*; (October 2020), https://www.wired.com/story/dana-debeauvoir-texas-county-clerk-voting-tech-revolution/.
14. Indeed, as we enter the eighth month of the COVID-19 pandemic, private sector assumption of aspects of cybersecurity have become more important than ever. As Committee Chairman Langevin noted in his July 17, 2020, opening statement during the House Hearing on the CSC, almost from the beginning "nearly half of employed adults became teleworkers, adding stresses on our infrastructure and creating new opportunities for hackers to wreak havoc." *See* Cyberspace Solarium Commission Testimony Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation of the Committee on Homeland Security of the U.S. House of Representatives, July 17, 2020, *supra* note 4.
15. *See also* Pulitzer-prize winning author Neil Sheenan's 2009 book *A Fiery Peace in a Cold War: Bernard Schriever and the Ultimate Weapon*, which provides an extraordinary account of the public-private development of the ICBM, under the general (sometimes even direct and personal) supervision of President Eisenhower, who many times spoke directly with then Colonel (and later 4-star Air Force General) Schriever.
16. NASA Transition Authorization Act, 2017, https://www.congress.gov/bill/115th-congress/senate-bill/442/text.
17. In particular, in Section 302, Congress reaffirms "its commitment to the use of a commercially developed, private sector launch and delivery system to the ISS for crew missions [and] the requirement that NASA shall make use of US commercially provided ISS crew transfer and crew rescue services. Section 702 of the same bill declares NASA "shall partner with ... private industry ... as appropriate," while in Section 825 it states, "NASA shall work across all (its) mission directorates to evaluate opportunities for the private sector to perform services." Ibid.
18. Kristen Eichensehr, "Public-Private Cybersecurity," *Texas Law Review*, 2017, *supra* note 5, 494.
19. U.S. Cyberspace Solarium Commission, Final Report, March 2020, *supra* note 2, 101 & 105.
20. Two very recent attacks by Iran against Israel underscore this vulnerability. On April 24 and 25, 2020, Iranian hackers were linked to attempted cyberattacks aimed to disrupt water supplies in at least two Israeli locations- attacks Israel Water Authority employees detected and quickly alerted Israel's cybersecurity agency, https://www.washingtonpost.com/national-security/intelligence-officials-say-attempted-cyberattack-on-israeli-water-utilities-linked-to-iran/2020/05/08/f9ab0d78-9157-11ea-9e23-6914ee410a5f_story.html. U.S. Cyberspace Solarium Commission, Final Report, *supra note 2*, 62, https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkfl0MxIXJGT4yv/edit.
21. The British government has already recognized the threat, establishing the National Cyber Security Centre in October 2016; the NCSC provides a single point of contact between industry and government to offer advice, guidance, and support on cybersecurity, including management of cybersecurity threats, https://www.ncsc.gov.uk. *See also* H.R. McMaster's "Battlefields," and the General's discussion of Finland's National Cyber Security Centre, and Estonia's cybersecurity initiatives following Russia's 2007 cyber attacks, "which now include high-functioning e-government infrastructure, digital identity, mandatory baselines, and a central system for identifying and responding to attacks." Ibid., 74-75.
22. Department of Defense Cyber Strategy Summary, 2018 (https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF), 4.

NOTES

23. Ibid., 3-5, committing DoD to "streamline [its] public-private information-sharing mechanisms and strengthen the resilience and cybersecurity of critical infrastructure networks and systems." Ibid. at 4. Interestingly, this Cyber Strategy pledges that the Department "will hold DoD personnel and our private sector partners accountable for their cybersecurity practices and choices." Ibid., 5.
24. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232.
25. United States Cyberspace Solarium Commission, Final Report, March 2020, https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view, *supra* note 2, 105.
26. Ibid., 5.
27. Ibid., 4.
28. Executive Office of the President, Office of Management and Budget, *Circular No. A-76*, August 1983 (most recently revised 2003).
29. Kirsten Eichensehr, "Public-Private Cybersecurity" *Texas Law Review*, 2017, *supra* note 5 (emphasis added, *citing* OMB Circular No. A-76). *See* the Federal Activities Inventory Reform (FAIR) Act of 1998, P.L. 105-270. The FAIR Act directs Federal agencies to issue each year an inventory of all commercial activities performed by federal employees. The OMB reviews each agency's commercial activities inventory and consults with the agency regarding content. Upon the completion of this review and consultation, the agency is required to transmit a copy of the FAIR Act Inventory of Commercial Activities to the Congress and make it available to the public. The FAIR Act then establishes a limited administrative challenge and appeals process under which an interested party may challenge the omission or the inclusion of a particular activity on the inventory as a commercial activity. Inherently governmental functions are also codified in the Federal Acquisition Rules Subpart 7.5 ("Contracts shall not be used for the performance of inherently governmental functions").
30. *See* Executive Office of the President, Office of Management and Budget, *Circular No. A-76*, August 1983 (most recently revised 2003), *supra* note 28.
31. *See, e.g.*, "Inherently Governmental Functions and Department of Defense Operations: Background, Issues, and Options for Congress," Congressional Research Service, July 22, 2009, https://fas.org/sgp/crs/misc/R40641.pdf, *passim.*
32. Former University of California, Los Angeles, School of Law, now University of Virginia School of Law Professor who is cited throughout this paper.
33. Kristen Eichensehr, "Public-Private Cybersecurity," *Texas Law Review*, 2017, *supra* note 5, 519. While we do not disagree with these three important points, the infeasibility of the first suggestion, and the likely over-regulation inherent in the second suggestion give us some pause; the third—describing threats to individual privacy—should give all of us considerable pause. A cyber 9/11 event no doubt would revisit the nation's approach to these public law valuations like a bombshell.
34. Ibid.
35. Over time, even these governmental functions increasingly are becoming blurred -for example with the use of private security firms such as Blackwater and Triple Canopy, and extensive use of private arbitrators and mediators in lieu of court proceedings.
36. Executive Office of the President, Office of Management and Budget Circular No. A-76—Revised Supplemental Handbook, *Performance of Commercial Activities*, 1999, 57.
37. Ibid.
38. *See, e.g.*, Jim Chen, "A Framework of Partnership," *The Cyber Defense Review*, Spring 2020.
39. Kristen Eichensehr, "Public-Private Cybersecurity," *Texas Law Review,* 2017, *supra* note 5, 481-82.
40. While aspects of CSC's deliberations and reporting were classified, CSC's overriding effort was to provide an open and publicly accessible report, fully explaining its 82 recommendations.
41. The Competition in Contracting Act of 1984 (CICA), 41 U.S.C. 253, generally governs competition in federal procurement contracting by requiring eligible contracts to be entered into after "full and open competition through the use of competitive procedures."
42. "New Definition of 'Inherently Governmental Function' Affects Government Insourcing Decisions," *National Law Review*, September 24, 2011, https://www.natlawreview.com/article/new-definition-inherently-governmental-function-affects-government-insourcing-decisions.

NOTES

43. Sebastian Sprenger, "Defense News," https://www.defensenews.com/30th-annivesary/2016/10/25/30-years-future-combat-systems-acquisition-gone-wrong/.
44. Federal News Network, https://www.google.com/amp/s/federalnewsnetwork.com/cybersecurity/2020/09/turn-over-on-the-cmmc-advisory-board-continues/amp/.
45. Kristen Eichensehr, "Public-Private Cybersecurity," *Texas Law Review*, 2017, *supra* note 5.
46. Jim Chen, "A Framework of Partnership," *The Cyber Defense Review,* Spring 2020, *supra* note 38, 18.
47. U.S. Cyberspace Solarium Commission, Final Report, March 2020, https://www.solarium.gov/report.