Cybersecurity on Retainer

Supporting National Incident Response Capability Through the Private Sector

By Andrew S. Pasternak and Rachel R. Gaiser

In a recent issue of *Foreign Affairs*, Chris Inglis and Harry Krejsa argued that the current state of affairs in the cyber ecosystem needs to be fixed, with too much risk pushed down to users, small businesses, and local governments. What is needed instead, they argue, is "a new social contract for the digital age," one that changes the current cybersecurity paradigm between the public and private sectors. This paradigm shift would include governments and large firms shouldering more of the burden, transitioning to a more "collective, collaborative defense."[1] This kind of paradigm shift is even more crucial for response to severe cyber incidents, defined in the *National Cyber Incident Response Plan's* (NCIRP) Cyber Incident Severity Schema (CISS) as an incident or group of incidents "likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties."[2, 3, 4]

Mr. Andrew S. Pasternak is a Senior Policy Advisor in the Office of the National Cyber Director. **Ms. Rachel R. Gaiser** is an Advisor at the Cybersecurity and Infrastructure Security Agency. The authors completed this article in their personal capacity and prior to beginning their positions in their respective offices.

The United States has been fortunate so far that no cyberattack has matched the level of a severe cyber incident, but this may not always be the case. State and non-state actors continue to improve their offensive cyber capabilities, threatening the critical infrastructure vital to the United States. Ransomware gangs attack organizations fundamental to everyday life, from city governments to hospitals to pipelines. The return of great power competition to interstate relations between the United States, the People's Republic of China (PRC), and the Russian Federation is, at this point, treated as a fact in U.S. national security policy.[5] With great power competition comes the remote yet real possibility of great power conflict, increasing, in turn, the likelihood of a severe cyber incident.

During a severe cyber incident, the public expects the government to defend the Homeland, including critical infrastructure disruption of which would affect national security, economic stability, or public health and safety.[6] The technical capacity to respond to severe cyber incidents is vital for the federal government to mitigate the effects on the nation's security. At the time of this writing, however, the government cannot provide non-federal entities Digital Forensics and Incident Response (DFIR) services at scale, nor is there a mechanism for the government to rapidly coordinate and deploy private sector DFIR services to prioritized critical infrastructure partners.[7] Over 700,000 cybersecurity positions are unfilled in the United States, including approximately 40,000 vacancies in the public sector. With the higher salaries offered by the private sector, it seems unlikely that the federal government will be able to develop the necessary DFIR capacity internally any time in the near future.[8]

With the government unlikely to internally develop the DFIR capacity needed to respond to severe cyber incidents, policymakers should consider paying to retain private sector DFIR capacity. A Cybersecurity Retainer Program (CRP) would allow the government to rapidly expand DFIR capacity during a severe cyber incident. A CRP would also incentivize private sector partners to maintain DFIR teams optimized for national security incident response services and improve readiness by training and exercising with CRP teams before a severe cyber incident occurs.

This article first assesses the current strategic environment, including how DFIR services are provided and the challenges with providing DFIR services during severe cyber incidents. The following section details the concept of the CRP and compares it to two alternative options: a civilian cybersecurity reserve and the use of the Defense Production Act. The final section examines issues that must be considered and further researched if the government is to develop the CRP, including costs and who can access DFIR services.

UNDERSTANDING THE CURRENT STRATEGIC ENVIRONMENT

Private sector entities and state and local governments without DFIR capabilities rely primarily on private cybersecurity vendors for DFIR services when a cyber incident occurs. These vendors can hire personnel and charge clients at rates reflecting the demand for these services. Organizations can obtain these services ad hoc or through a retainer agreement. Many vendors provide incident response activities, though the capability of these vendors can vary significantly.[9] The National Cyber Incident Response Plan highlights the role of the private sector during severe cyber incidents, with the private sector providing for the security of its networks and often providing support or assistance to federal agencies.[10]

Great power competition, and with it the remote yet real possibility of great power conflict, increases the likelihood of severe cyber incidents, with U.S. competitors demonstrating the capability and intent to target civilian infrastructure. The PRC, for example, has demonstrated the capability

to target U.S. critical infrastructure, including compromising thousands of organizations simultaneously and targeting U.S. infrastructure to develop cyberattack capabilities.[11, 12, 13] The People Liberation Army's 2020 *Science of Military Strategy* (SMS) calls out "national information infrastructure" as a critical target for "cyber electromagnetic space warfare,"—a phrase that includes cyber warfare as one of its primary forms.[14, 15, 16] Finance, energy, and transportation are mentioned explicitly in the SMS, though other infrastructure sectors are likely targeted. The SMS also uses the 1999 campaign of bombing Yugoslavia by NATO as an example of successfully targeting civilian infrastructure, saying that switching from military to civilian infrastructure crushed the will of the Yugoslav Federation. This example is given in a section on cyberspace, suggesting that the authors believe offensive cyber operations could have a similar effect.[17]

While the almost exclusively private sector arrangement is typically beneficial given the private sector's resources, severe cyber incidents, most notably those occurring during a conflict, would challenge the ability of the private sector to respond due to the issues of scale, prioritization, and coordination. Severe cyber incidents could affect hundreds or thousands of organizations. Cybersecurity vendors exist within a business model that could prioritize organizations for restoration differently than would the federal government, leaving vital infrastructure operators without needed assistance. Some level of communication and coordination currently exists across prominent cybersecurity vendors through organizations such as Information Sharing and Analysis Centers and the Cybersecurity and Infrastructure Security Agency(CISA)'s Joint Cyber Defense Collaborative (JCDC), but not nearly on the scale to allow coordinated and prioritized incident response activities during an extended period of intensified malicious activity.[18, 19]

During severe cyber incidents, the general public and private sector expect the government to take a more prominent role in coordination and cyber incident response, ensuring the safety of government operations and the nation's critical infrastructure. The problem with this expectation is that even if hiring, training, and retaining cybersecurity personnel were not an issue, the small number of

CAD design for new facility for Cybersecurity and Infrastructure Security Agency. Source: Government Services Agency

government personnel with the skillset needed for DFIR operations makes it highly unlikely the federal government will ever be able to undertake incident response activities at scale. In the Fiscal Year 2021 enacted budget, CISA had 607 positions designated for cyber operations programs, projects, and activities. Threat Hunting, which includes the hunt and incident response services provided by CISA, comprised 181 of these positions.[20] The number within Threat Hunting that could undertake incident response services is smaller. Threat Hunting's workforce is supplemented by contractors that provide the added technical capability. Still, the small numbers highlight how challenging it could be for CISA to respond to incidents within federal networks during severe cyber incidents, let alone incidents at critical infrastructure entities.

The Department of Defense (DOD) also retains DFIR capabilities that may assist during severe cyber incidents outside of conflict. During a conflict, however, DoD is unlikely to have the personnel to perform DFIR activities for key critical infrastructure partners. As of 2022, U.S. Cyber Command's Cyber Mission Force comprises 133 teams, a subset of which are Cyber Protection Teams intended to defend the Department of Defense Information Network and critical infrastructure.[21] The National Guard's cyber force has over 2,200 personnel and has previously assisted in critical infrastructure cyber defense, though the number able to participate in DFIR operations is a smaller subset.[22] During a conflict, DOD network defenders will have to respond to increased malicious activity against DOD networks, limiting the availability of DOD cybersecurity personnel to respond to cybersecurity incidents at critical infrastructure entities.

The federal government, like practically all organizations in the public and private sectors, has been attempting to overcome an acute cybersecurity workforce shortage. According to a 2022 Federal Cyber Workforce Management and Coordinating Working Group report, over 700,000 cybersecurity positions remain unfilled in the United States, including approximately 40,000 vacancies in the public sector.[23] This high number of vacancies in the U.S. cyber workforce includes the highly technical personnel needed for DFIR activities. The federal government and other organizations have understood the growing workforce shortage for years, but despite numerous efforts, they still need to close the workforce gap.[24] On top of this, the federal government's cybersecurity workforce skews older: less than 6 percent are under 30, while over 30 percent are over 55.[25]

The reasons for this workforce shortage in the federal government are discernible. Private sector employers typically offer higher salaries and can hire employees quickly.[26] Federal wages are typically lower, and a candidate can take months or years to be hired after the initial job offer, depending upon the bureaucratic and security requirements of the position. For example, a 2022 report from CISA's Cybersecurity Advisory Committee found that the agency took an average of 198 days to complete the onboarding process after a candidate received an offer.[27] Once government agencies hire and train cybersecurity personnel, retaining this workforce presents difficulties, with higher salaries and appealing opportunities within the private sector enticing many to leave.

CISA and other agencies are taking steps to improve the development and retention of a cybersecurity workforce, with mixed results. It is not likely, however, that the federal government will be able to develop and maintain the capability to respond to the increased malicious cyber activity likely to occur during a severe cyber incident. The federal government will need to rely extensively on private sector capacity to secure the nation's critical infrastructure. Nevertheless, there is currently little infrastructure to increase the government's DFIR capabilities through coordinating and directing private sector capabilities during a severe cyber incident.

DEPLOYING PRIVATE SECTOR CAPABILITY THROUGH A CRP

Given the small size of the federal government's DFIR capability and the likelihood that improving hiring and retainment practices, while helpful, will not resolve the problem, other means of obtaining the capacity needed during a severe cyber incident must be considered, and this requires looking to cybersecurity vendors in the private sector. Rather than trying another hiring or personnel retention program that only marginally improves the situation, a Cybersecurity Retainer Program would allow the government to maintain an extensive incident response capacity for severe cyber incidents that can be deployed rapidly and sustained at a relatively low cost.

A CRP would function similarly to the retainer services provided by cybersecurity vendors and other industries, with some differences. The federal government, through CISA or another agency, provides annual funding to selected cybersecurity vendors via approved contractual processes. These vendors then provide DFIR response capabilities when requested. Unlike typical retainers, CRP funding ensures that cybersecurity vendors maintain the DFIR capability needed by the government during a severe cyber incident. DFIR teams would be available for rapid deployment to the government for extended periods that could last months or even years.

Similar federal programs allow the government to retain services for times of conflict that would otherwise be unavailable. One example is the Maritime Security Program (MSP), run by the Department of Transportation's Maritime Administration (MARAD). While Military Sealift Command and MARAD maintain cargo vessels to support military operations, maintaining a cargo fleet large enough to sustain operations during a large-scale conflict would be extremely expensive without any certainty that the ships would ever be used. Rather than pay large sums to build and maintain such a fleet, MARAD provides ship operators with a financial retainer for 60 ships; in return, the operators will provide the ship to the U.S. government during times of war or national emergency.[28, 29] A 2009 study of the program ordered by the Department of Transportation, 13 years after the beginning of the program, found that the MSP had a clear positive impact on the number of U.S.-flagged vessels and their availability for military use, as well as the availability of mariners to operate these vessels.[30]

While cybersecurity and maritime shipping may seem completely different, they share two fundamental similarities: the cost of maintaining the capability is high, and most of the capacity is in the private sector. MSP is a prime example of using government funding to ensure capacity during a time of need while avoiding the higher cost of owning the capacity during peacetime. A cybersecurity retainer program would provide a similar solution, providing the government with a way of increasing capacity that can be quickly deployed against threats and incidents.

Establishing a CRP will incentivize private sector partners to work with the federal government to maintain DFIR teams optimized for national security incident response services. These teams will benefit from working together before any severe cyber incident occurs, allowing them to respond more effectively when called upon by the government. While the CRP, unlike the MSP, is not needed to maintain sufficient capacity in the private sector, it could be used to incentivize the maintenance and growth of private sector capabilities valuable during a severe cyber incident.

Another benefit of the CRP for both the private sector and the government is the ability to regularly conduct cybersecurity exercises by combined government and CRP DFIR teams. Research shows that regularly exercising cyber security incident response plans and other scenarios helps DFIR teams improve overall readiness to respond to incidents, including improving collaboration and coordination between team members.[31] For example, incorporating CRP

DFIR teams into CISA's biennial Cyber Storm Exercise—the most extensive government-sponsored cybersecurity exercise—would provide the CRP DFIR teams with a holistic introduction to working with federal, state, local, territorial, and tribal partners.[32] Although the government may only fully activate CRP DFIR teams during a severe cyber incident, exercising different scenarios will provide CRP DFIR teams with needed context and familiarity by coordinating with thousands of stakeholders across the government.

ALTERNATIVES TO CRP PROVIDE FEWER BENEFITS

Voluntary and compulsory options exist for the federal government to tap into private sector capabilities during a conflict. We will discuss below two CRP alternatives: the development of a civilian cybersecurity reserve and the use of the Defense Production Act during a conflict. While these options provide benefits, neither offers the same ability as the CRP to rapidly scale and deploy DFIR capabilities at the outset of a severe cyber incident.

Civilian Cyber Reserve

The Civilian Cyber Security Reserve Act was a bipartisan bill introduced in 2021 that proposed permitting CISA to create a pilot civilian reserve program. CISA would develop a reserve of up to 30 members to activate during a severe cyber incident. When activated, civilians in the program would be considered members of the federal civil service.[33]

Given the program's small size and the status of reservists as federal civil servants, CISA's probable goal would be to integrate those in the reserve program into CISA operations, boosting existing technical teams, including DFIR teams. The bill represented a novel approach to increasing government capacity during a time of need and built off a military reserve model with various degrees of international success.[34]

If fully staffed with effective technical personnel who can quickly integrate into CISA operations—far from a given—reserve personnel could improve CISA capabilities to a limited degree. Even with the understanding that the program put forward in the Civilian Cyber Security Reserve Act is a pilot program, it seems highly unlikely that an even more extensive program would put a dent in the capability needed to defend private, state, and local government networks during a severe cyber incident. This added capacity will likely be needed to defend federal networks, limiting their availability for critical infrastructure network defense. Any incident response-focused reservists would also be leaving their respective private sector teams during a conflict, affecting the capability of those private sector organizations to provide DFIR services.

The difficulty of integrating reserve personnel into existing operations could also hinder the effectiveness of a reserve program. Technical personnel within CISA already have demanding, high-tempo positions, which reduces available time to work with reservists, understand their capabilities and personalities, and determine how they can best be deployed when activated. This issue becomes more acute as the size of any reserve program increases, especially for an agency such as CISA beginning with limited technical staffing.

Finally, while the reserve program did not allocate any additional funds, the cost of a cyber reserve program needs to be considered. Given the current recruitment issues due in part to the higher salaries in the private sector, any cyber reservist would likely require pay commensurate with the time required. Between individual income, additional administrative costs such as travel, equipment, and security clearances, and uncertainty about the scalability and effectiveness of the program, it is unclear if the return on investment would be comparable to other programs such as the CRP.

Defense Production Act

As noted in the Cyberspace Solarium Commission's report, the Defense Production Act (DPA) provides the President with expansive authority to prioritize resources and services to promote the national defense. However, current DPA planning does not account for cybersecurity services.[35,36] Congress added critical infrastructure protection and restoration to the definition of national defense within the Defense Production Act in 2003.[37]

Utilizing the DPA to ensure private cybersecurity vendors prioritize government contracts would scale government capability. The DPA does not conflict with the idea of a CRP and can complement it by providing additional capacity if needed. Relying solely on the DPA will prevent the government from rapidly scaling incident response capacity during a severe cyber incident or in the lead-up to and beginning of a conflict. Once the decision is made to invoke the DPA, the government will need to identify which cybersecurity vendors to call upon, assess the capabilities of these organizations, and determine how to deploy and coordinate the DFIR teams and other services provided by these vendors. This will take time. Given the rapid pace at which cyber operations may unfold at the beginning of an armed conflict, opportunities to limit operational impacts from malicious cyber activity may be missed.

Some of this activity, such as identifying vendors and coordination mechanisms, can be undertaken before a conflict. The Cyberspace Solarium Commission recommended a similar path, suggesting that the government convene incident response vendors to understand their capacity and procure standby contracts.[38] While this recommendation is a vital step forward, it is effectively like developing a CRP without the additional coordination and capability development a formal program provides. The government will still be able to utilize the DPA to increase DFIR capacity. However, maintaining a CRP will give the government the increased resource capacity to shape, coordinate ahead of any severe cyber incident, and rapidly deploy.

DEVELOPING THE WAY FORWARD

While the authors believe that a Cybersecurity Retainer Program can optimally provide the expanded capacity the federal government would require during severe cyber incidents, further work is needed to understand the associated requirements, costs, and potential risks.

The government must decide what kind of incident response capacity is required and how many incident response teams to include in the CRP. For example, the government will want to maintain an incident response capacity specializing in industrial control systems and operational technology. Ultimately, the size and composition of the CRP will be determined by several factors, including funds provided by Congress, threats as determined by the Intelligence Community, identified risks to U.S. critical infrastructure, and private sector capabilities.

While decisions on the kind and size of the incident response capacity will ultimately drive costs per DFIR team, the CRP can be cost-beneficial compared to the government's civilian cybersecurity budget. For comparison, as of 2022, the Maritime Security Program pays companies $5.3 million per vessel for 60 vessels, totaling $318 million.[39] The MSP provides funds to maintain the sealift capacity and employment for approximately 2,400 merchant mariners. The CRP would be a fraction of this cost, as it is not needed to maintain any physical infrastructure, nor are the funds necessary to support what is already a robust market. Instead, CRP funding is intended to solely maintain DFIR teams that will be prioritized for government use when needed.

Like all government programs, oversight will be crucial to maintaining the effectiveness of the

CRP. The government will need to ensure that those wanting to join the program can provide the skillsets and capacity required and will continue to do so. Program administrators must also decide on various administrative requirements, such as any security requirements associated with DFIR team members. The CRP will require similar oversight to other programs, with the government specifying the program's requirements and vendors demonstrating regularly how these requirements are being met.

The government will also need to make clear what entities would qualify for assistance from CRP vendors during a severe cyber incident. The goal of the CRP is not to replace existing private sector DFIR capacity but to ensure some of this capacity is available and prioritized for those organizations whose disruption could have national security impacts. CISA is currently undertaking efforts to identify "Systemically Important Entities," which can be a first step to identifying those organizations to prioritize for CRP assistance during a severe cyber incident.[40] A CRP would also incentivize entities designated as systemically important to collaborate with the government.

Entities receiving CRP assistance would need to be reassured that their sensitive information is being protected and that the government is not seeking to use a CRP vendor's access to investigate or otherwise examine them. To affirm that the role of the CRP is to assist critical infrastructure entities—not to investigate or punish them—it will be vital to develop data safeguard measures such as standard liability releases, confidentiality protections, and vendor prohibitions on sharing CRP recipient's non-essential, voluntarily-provided information with the federal government. The government should develop a methodology for deciding the share of the cost of DFIR services paid for by the victim of a severe cyber incident. Government expenditures during an armed conflict, for example, would increase dramatically, and saving even small amounts can ensure the longevity and flexibility of the program. Some organizations, such as Fortune 500 companies, can bear the costs of access to the CRP if such access is even needed. Other organizations may face ruinous costs if not given assistance, and cybersecurity insurance may not be able or willing to cover severe incidents, especially acts of war.[41, 42] Although beyond the scope of this article, a well-developed methodology for deciding cost-sharing will reduce government expenses while ensuring systemically important entities receive the DFIR services necessary to restore operations at a reasonable cost.

CONCLUSION

Preparing to defend the homeland in cyberspace during a severe cyber incident requires the government to have the capacity to respond to cybersecurity incidents on its networks and the networks of critical infrastructure operators. As laid out in this article, it seems unlikely that the government will be able to scale its limited DFIR capacity in the near future and will rely on the private sector to provide this capacity.

Ensuring the government has the capacity needed during severe cyber incidents requires efforts beyond the baseline government-private sector collaboration consisting of information sharing and coordination done today. A CRP would provide the government with the DFIR capacity needed during a national emergency, promote its maintenance in the private sector during peacetime, and provide an avenue to plan better and exercise this DFIR capacity. While the best future is one where this capability is never needed, a CRP provides the government the capacity to respond to cyber incidents, building the collective, collaborative defense that will improve the nation's resiliency. PRISM

Notes

[1] Chris Inglis and Harry Krejsa, "The Cyber Social Contract: How to Rebuild Trust in a Digital World," *Foreign Affairs*, February 21, 2022, https://www.foreignaffairs.com/articles/united-states/2022-02-21/cyber-social-contract.

[2] The CISS is a scale used by CISA to provide a repeatable and consistent mechanism for evaluating the risk severity of an incident. The scale has a 0-5 scale, with 0 being the least severe and 5 the most severe. Level 4 are severe incidents. Level 5 are emergency incidents described as "an imminent threat to the provision of wide-scale critical infrastructure services, national government security, or the lives of US citizens."

[3] Department of Homeland Security, "National Cyber Incident Response Plan," December 2016, 8, www.cisa.gov/uscert/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

[4] Cybersecurity and Infrastructure Security Agency, "CISA National Cyber Incident Scoring System (NCISS) | CISA," September 30, 2020, https://www.cisa.gov/news-events/news/cisa-national-cyber-incident-scoring-system-nciss.

[5] The word "competition" is used 44 times in the 2022 *National Security Strategy*, with the first section being called "the competition for what comes next." See: White House, *National Security Strategy*, October 2022, 6, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

[6] "Presidential Policy Directive—Critical Infrastructure Security and Resilience," February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[7] For an explanation of DFIR, see: Crowdstrike, "Digital Forensics and Incident Response Explained," October 12, 2022, https://www.crowdstrike.com/cybersecurity-101/digital-forensics-and-incident-response-dfir/.

[8] Federal Cyber Workforce Management and Coordinating Working Group, *State of the Federal Cyber Workforce: A Call for Collective Action*, September 2022, 6, https://www.cisa.gov/sites/default/files/publications/State_of_the_Federal_Cyber_Workforce_Report_09.14.2022.pdf.

[9] Prateek Bhajanka and Wam Voster, "Market Guide for Digital Forensics and Incident Response Services," *Gartner*, September 21, 2021, https://www.gartner.com/doc/reprints?id=1-27NMS8JH&ct=211015&st=sb.

[10] Department of Homeland Security, "National Cyber Incident Response Plan," December 2016, 15, www.cisa.gov/uscert/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

[11] The White House, "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," July 19, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/.

[12] United Kingdom National Cyber Security Centre, "U.K. and allies hold Chinese state responsible for pervasive pattern of hacking," July 19, 2021, www.ncsc.gov.uk/news/uk-allies-hold-chinese-state-responsible-for-pervasive-pattern-of-hacking.

[13] Cybersecurity and Infrastructure Security Agency, "Alert (AA21-201A), Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013," Department of Homeland Security, last revised July 21, 2021, https://www.cisa.gov/uscert/ncas/alerts/aa21-201a.

[14] China Aerospace Studies Institute, trans. *Science of Military Strategy*. National Defense University of the People's Liberation Army (PLA), 2022, 235, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2022-01-26%202020%20Science%20of%20Military%20Strategy.pdf.

[15] Elsa B. Kania and John Costello, "Seizing the commanding heights: PLA Strategic Support Force in Chinese military power," *Journal of Strategic Studies* 44:2 (2021), 226.

[16] Joe McReynolds, "China's Military Strategy for Network Warfare," In Joe McReynolds, ed., *China's Evolving Military Strategy*, Washington, DC: The Jamestown Foundation, 2017, 209.

[17] China Aerospace Studies Institute, trans. *Science of Military Strategy*. National Defense University of the PLA, 2022, 151-152, 263, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2022-01-26%202020%20Science%20of%20Military%20Strategy.pdf.

[18] "National Council of ISACs | About ISACs," n.d. https://www.nationalisacs.org/about-isacs.

[19] "Joint Cyber Defense Collaborative | CISA," n.d. https://www.cisa.gov/jcdc.

[20] Department of Homeland Security, *Cybersecurity and Infrastructure Security Agency Budget Overview, Fiscal Year 2023 Congressional Justification*, 2022, 114, https://www.dhs.gov/sites/default/files/2022-03/Cybersecurity%20and%20Infrastructure%20Security%20Agency%20%28CISA%29_Remediated.pdf.

[21] U.S. Cyber Command, "Cyber 101—Cyber Mission Force," November 1, 2022, https://www.cybercom.mil/Media/News/Article/3206393/cyber-101-cyber-mission-force/#:~:text=The%20Cyber%20Mission%20Force%20(CMF,defense%20of%20U.S.%20national%20interests.

[22] Whitney Hughes, "National Guard provides critical cybersecurity for midterm elections," U.S. Army, November 7, 2022, https://www.army.mil/article/261806/national_guard_provides_critical_cybersecurity_for_midterm_elections.

[23] Federal Cyber Workforce Management and Coordinating Working Group, *State of the Federal Cyber Workforce: A Call for Collective Action*, September 2022, 6, https://www.cisa.gov/sites/default/files/publications/State_of_the_Federal_Cyber_Workforce_Report_09.14.2022.pdf.

[24] William Crumpler and James A. Lewis, *The Cybersecurity Workforce Gap*, Center for Strategic and International Studies, January 2019, 1–2, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf.

[25] Federal Cyber Workforce Management and Coordinating Working Group, *State of the Federal Cyber Workforce*, 6.

[26] Scott Rosenberg, "Cybersecurity's public-private salary gap," *Axios*, August 30, 2022, https://www.axios.com/2022/08/30/cybersecurity-public-private-salary-gap.

[27] CISA Cybersecurity Advisory Committee, *Report to the CISA Director: Transforming the Cyber Workforce*, June 22, 2022, 2, https://www.cisa.gov/sites/default/files/publications/June%202022%20CSAC%20Recommendations%20-%20TCW.pdf.

[28] "Part 296 – Maritime Security Program (MSP)," Code of Federal Regulations, Title 46 (2018): § 296, www.govinfo.gov/content/pkg/CFR-2018-title46-vol8/xml/CFR-2018-title46-vol8-part296.xml.

[29] Maritime Administration, "Maritime Security Program," Department of Transportation, last updated August 1, 2022, www.maritime.dot.gov/national-security/strategic-sealift/maritime-security-program-msp.

[30] Econometrica, Inc, *Final Report: Maritime Security Program Impact Evaluation*, Maritime Administration, July 2009, 1-3, www.maritime.dot.gov/sites/marad.dot.gov/files/docs/resources/3776/msprevisedfinalreport-transmitted07-24-09.pdf.

[31] Giddeon N. Angafor, Iryna Yevseyeva, and Ying He, "Game-based Learning: A Review of Tabletop Exercises for Cybersecurity Incident Response Training," *Security and Privacy* 3, no. 6 (November 2020), https://doi.org/10.1002/spy2.126.

[32] For more information on Cyber Storm, see: "Cyber Storm: Securing Cyber Space | CISA." Accessed January 18, 2023. https://www.cisa.gov/cyber-storm-securing-cyber-space.

[33] U.S. Senate, *Civilian Cybersecurity Reserve Act*, S 1324, 117th Congress, introduced in U.S. Senate April 22, 2021, www.congress.gov/bill/117th-congress/senate-bill/1324.

[34] Marie Baezner, *Study on using reserve forces in military cybersecurity: A comparative study of selected countries* (Zurich: Center for Security Studies, April 2020), https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-03-military-cybersecurity.pdf.

[35] Angus King and Mike Gallagher, *Cyberspace Solarium Commission*, March 2020, 63, https://www.solarium.gov/.

[36] *Defense Production Act*, U.S. Code 50, §4511, https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter55&edition=prelim.

[37] Defense Production Act Reauthorization of 2003, Public Law No. 108-195, 108th Congress, December 19, 2003, https://www.govinfo.gov/content/pkg/PLAW-108publ195/pdf/PLAW-108publ195.pdf.

[38] Angus King and Mike Gallagher, *Cyberspace Solarium Commission*, March 2020, 63.

[39] U.S. Department of Transportation, *Budget Estimate Fiscal Year 2023: Maritime Administration*, 2022, 5, https://www.transportation.gov/sites/dot.gov/files/2022-03/MARAD_Budget_Estimates_FY23.pdf.

[40] Sara Friedman, "Easterly: CISA plans to move forward with 'systemically important entities' work regardless of legislation," *Inside Cybersecurity*, January 8, 2023.

[41] The cybersecurity insurance industry has had difficulty maintaining current policies, with the Treasury Department looking into ways to shore up the industry. See: Daphne Zhang, "As Cyber Insurance Dries Up, Treasury Department Eyes a Backstop," *Bloomberg Law*, October 7, 2022, https://news.bloomberglaw.com/insurance/as-cyber-insurance-dries-up-treasury-department-eyes-a-backstop.

[42] Josephine Wolff, "Who Pays for an Act of Cyberwar?" *Wired*, August 30, 2022, https://www.wired.com/story/russia-ukraine-cyberwar-cyberinsurance/.