OFFICE OF THE NATIONAL CYBER DIRECTOR

Request for Information – Cyber Workforce Development Strategy

SUBMITTED BY

Foundation for Defense of Democracies –
Center on Cyber and Technology Innovation

November 3, 2022

FOUNDATION FOR DEFENSE OF DEMOCRACIES

CSC 2.0

www.fdd.org

I. Introduction

The U.S. government needs to be coordinated, prioritized, and diversified in its approach to building the national cyber workforce. The congressionally mandated Cyberspace Solarium Commission published a white paper on the cyber workforce in September 2020, identifying systemic barriers stymieing existing workforce development efforts.[1] Expanding on those ideas, the CSC 2.0 project published the *Workforce Development Agenda for the National Cyber Director* in June 2022.[2] In this Request For Information, the CSC 2.0 project staff have highlighted key recommendations from the report as well as drawn on other research to address the challenges identified by the Office of the National Cyber Director.

These recommendations focus on solutions not only for the federal government but also for the federal and national cyber workforce and include actions that would enable cyber workforce development efforts within the private sector.

The RFI is organized into three major parts to provide the following recommendations:

Area: Cyber Workforce; Sub-Area: Recruitment and Hiring

- **Challenge**: Enhance opportunities for entry-level members of the cyber workforce, including new entrants and people pursuing reskilling or upskilling
- **Recommendation 1:** Create partnerships to ensure new graduates have the qualifications necessary to secure an entry-level job in cybersecurity
- **Recommendation 2**: Conduct both budgetary and policy reviews of cyber workforce programs to assess their holistic effectiveness

Area: Cyber Workforce; Sub-Area: Career Development and Retention

- **Challenge**: Enable career progression within the cyber workforce, in both the public and private sectors
- **Recommendation 3**: Provide incentives to develop entry-level employees into mid-career talent
- **Recommendation 4**: Establish a Federal Cyber Workforce Development Institute for an early-career development program for the federal cyber workforce
- **Recommendation 5**: Leverage the new cadre of HR Specialists for record-keeping and metrics analysis

Area: Diversity, Equity, Inclusion, and Accessibility (DEIA); Sub-Area: DEIA in the Cyber Workforce

- **Challenge**: Identify best practices and strategies that are uniquely applicable to DEIA and a diverse cyber workforce
- **Recommendation 6**: Leverage the new cadre of HR Specialists for outreach and engagement

[1] U.S. Cyberspace Solarium Commission, "Growing a Stronger Federal Cyber Workforce," September 2020. (https://www.cybersolarium.org/public-communications/workforce-white-paper)

[2] Laura Bate and Mark Montgomery, "Workforce Development Agenda for the National Cyber Director," June 2022. (https://cybersolarium.org/wp-content/uploads/2022/05/CSC2.0_Report_WorkforceDevelopmentAgenda_FullText.pdf)

Recommendation 1 provides an overview of how to close the gap between qualified cyber workforce and qualifications and skills sought out by public and private employers. **Recommendation 2** explains the value of a strategic and budgetary review of cyber workforce development programs. **Recommendation 3** describes ways the federal government can incentivize private sector employers to enable hiring and investing in early-career professionals. **Recommendation 4** provides an overview of the Federal Cyber Workforce Development Institute. Lastly, **Recommendations 5** and **6** expand on ways to leverage HR Specialists to assess metrics and collect data (**Recommendation 5**) and to engage underrepresented communities (**Recommendation 6**).

II. Cyber Workforce - Recruitment and Hiring

The following section provides ways to help the NCD address the challenges of **enhancing opportunities for entry-level members of the cyber workforce, including new entrants and people pursuing reskilling or upskilling**.

Recommendation 1: Create partnerships to ensure new graduates have the qualifications necessary to secure an entry-level job in cybersecurity

Employers' reluctance to hire and train early-career candidates creates a subsequent shortage of experienced professionals. There is a higher demand for certifications relevant to mid- and late-career professionals than those for early-career professionals.[3] This creates a disconnect between the qualifications of the cyber talent pool and the experience and qualifications employers seek.

Various existing public and private sector programs work to increase the number of cybersecurity professionals entering the workforce. Other programs, meanwhile, bolster K–12 cyber education, and others still focus on recruitment from Historically Black Colleges and Universities (HBCU).[4] While each of these programs helps increase the cyber talent pool, they may not necessarily address the real lack of sufficiently qualified and certified candidates for cyber jobs in the federal government and industry. The problem can be a mismatch between the qualifications that graduates receive and those that employers require.

Even for entry-level positions, employers often require certifications that demonstrate knowledge in security infrastructure, risk mitigation, or threat recognition as well as knowledge and sector-specific certifications. NCD can partner with academic institutions, training programs, and technology companies to help identify the proper qualifications and certifications and ensure that those entering the workforce are more likely to have the requisite qualifications to secure a meaningful entry-level position, and even transition to mid-level positions, once they have the workforce experience. These partnerships should include the following:

[3] See, "Cybersecurity Supply/Demand Heat Map," *CyberSeek*. (https://www.cyberseek.org/heatmap.html)

[4] Dr. Georgianna Shea and Matthew Brockie, "Washington must act to build capable federal cybersecurity workforce," *Federal Times*, September 6, 2022. (https://www.federaltimes.com/thought-leadership/2022/09/06/washington-must-act-to-build-capable-federal-cybersecurity-workforce/)

- **Academic Institutions**: As technology and adversary techniques advance, so do the technical skills that employers seek in a given year. Employers often require industry-specific skills and certifications that are not currently available or accessible for recent graduates in cybersecurity. The NCD should create partnerships with colleges and universities to help ensure their curriculum provides students with the technical skills required by the workforce at all levels, not just entry-level positions. Qualifications and skills employers are looking for may be overshadowed by new requirements every year, and thus these partnerships will need regular updates to ensure they align with the skills and technical know-how employers require.
- **Trade Schools and Community Colleges**: Critical infrastructure owners and other large companies often have partnerships with local community colleges that create a pipeline of qualified workers in other fields. The NCD should work with schools and with companies to replicate successful programs like the lineman programs for the energy sector.
- **Technology and Equipment Producers**: Some vendor-specific technology manufacturers offer select, free training on their products. The NCD should work with these companies and others to expand existing programs and develop new ones that will enable students, new graduates, and second-career professionals to access the certifications they need to secure a job in cybersecurity.
- **Asset Owners and Operators**: With limited upskilling and reskilling, the existing critical infrastructure workforce could become an essential component of the cyber workforce. Many of these employees — for example, relay technicians in the electricity subsector — already have some exposure to cybersecurity issues and may already be responsible for cybersecurity-adjacent issues. The NCD should work with employers to identify the training these current employees need and work with training providers to develop affordable ways to upskill the current workforce.

There are great programs that would increase the cyber talent pool. The NCD should remain focused on closing the gap between the skills of recent graduates or early-career cyber professionals and the qualifications employers are seeking.

Recommendation 2: Conduct both budgetary and policy reviews of cyber workforce programs to assess their holistic effectiveness

Successful implementation of cyber workforce development programs requires budgetary reviews and quantitative assessments to identify misalignments between strategic goals, outcomes, and current expenditures. The NCD is required by law to monitor and assess "the effectiveness, including cost-effectiveness," of cybersecurity policies and review the annual budget proposals of federal departments and agencies.[5] The NCD's perspective and a firm grasp of the strategic cybersecurity landscape are critical in accurately quantifying the return on investment for cyber workforce programs.

[5] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 3388, codified as amended at 6 U.S.C. §1752 (c)(1)(C)(iii). (https://www.congress.gov/bill/116th-congress/house-bill/6395/text)

The NCD must identify appropriate metrics that would measure the effectiveness of cyber workforce development programs that align with the NCD's priorities. These metrics and measurements can provide insights that accurately represent the return on investment of cyber workforce development programs based on the NCD's priorities.

The NCD's role is vital for identifying appropriate levels of investment in the cyber workforce programs that would provide opportunities for the underrepresented cyber workforce to join the cyber workforce. Several existing programs have the potential to provide long-term benefits to both the public and private cyber workforce but have historically been underfunded. Analytical reviews of cyber workforce programs could capture programs' effectiveness, allowing the NCD to better explain the connection between funding and strategic goals to congressional appropriators.

The following programs should be assessed to determine if they need increased funding to ensure the country can realize the full benefits of each program:

- **Cybersecurity Education and Training Assistance Program (CETAP)** equips K–12 educators with resources to teach students about cybersecurity. Cyber.org, one of the CETAP grant recipients, has reached over 26,800 educators across the country with its content platform, with 21,270 educators trained to teach cybersecurity skills to students.[6] Unfortunately, this is only a fraction of the 400,000 teachers that the program needs to reach each year (based on 1.2 million K–12 STEM teachers being trained every three years). While routinely praised by CISA leaders as a model program, the president's budget request has repeatedly eliminated funding for this program, thus making the necessary program growth impossible.[7] The estimate to grow the CETAP program from 6,000 teachers a year to 400,000 teachers a year is an increase in budget from $6M to $20M a year.
- **The National Initiative for Cybersecurity Education (NICE) Regional Alliances and Multistakeholder Partnerships (RAMPS) Program** is a multistakeholder partnership that organizes a group of employers to focus on cyber workforce development to meet the needs of a local or regional workforce.[8] The program was not included in the White House's FY22 budget request, and the FY23 budget request asked for only about half of what the CBO estimated the project would cost.[9]

[6] "About Us," *Cyber.org*, accessed November 2, 2022. (https://cyber.org/about-us)

[7] U.S. Department of Commerce, "National Institute of Standards and Technology, National Technical Information Service, Fiscal Year 2022 Budget Submission to Congress," 2021. (https://www.commerce.gov/sites/default/files/2021-06/fy2022_nist_congressional_budget_justification.pdf); U.S. Department of Commerce, "National Institute of Standards and Technology, National Technical Information Service, Fiscal Year 2023 Budget Submission to Congress," 2022, page 37. (https://www.commerce.gov/sites/default/files/2022-03/FY2023-NIST-NTIS-Congressional-Budget-Submission.pdf)

[8] "National Initiative For Cybersecurity Education (NICE)," *National Institute of Science and Technology*, accessed November 2, 2022. (https://www.nist.gov/itl/applied-cybersecurity/nice/regional-alliances-and-multistakeholder-partnerships-stimulate-ramps)

[9] U.S. Congressional Budget Office, "Cost Estimate: S.2775, HACKED Act of 2019," January 31, 2020. (https://www.cbo.gov/system/files/2020-01/s2775.pdf)

- **CyberCorps: Scholarship for Service program** provides cybersecurity educational programs to a diverse talent pool. The U.S. government pays for a student's education in exchange for a future commitment to federal cyber service. The program has become one of the mainstays of public sector cybersecurity workforce development and recruitment programs, providing scholarships for more than 400 students per year at nearly 100 universities, colleges, and community colleges across the country. This program also addresses the national cyber workforce challenge by developing and sustaining cybersecurity programs at all of these institutions, thus supporting the private sector workforce as well. Despite its far-reaching impact, the program has seen limited funding growth for decades.[10]

By assessing the return on investment of current cyber workforce development programs, the NCD can work to ensure that successful programs are expanded, and unsuccessful programs are retooled or eliminated, freeing up additional funding for successful programs.

III. Cyber Workforce - Career Development and Retention

The following section expands on the first recommendation on ways to help the NCD address the challenges of **enabling career progression within the cyber workforce in both the public and private sectors**.

Recommendation 3: Provide incentives to develop entry-level employees into mid-career talent

The lack of incentives — whether financial or development opportunities — leads to high employee turnover when skilled employees get poached. To create a pipeline of mid-career, experienced professionals, employers must invest in hiring and developing early-career professionals by providing additional educational and training opportunities. The NCD can lead in this effort by working with congressional committees to implement programs that incentivize employers to hire and invest in early-career professionals to increase the talent pool of future mid-career professionals.

Such employer incentives can take various forms:

- **Award grants to employers that invest in cyber training programs for early-career professionals**. Non-traditional programs with a beneficial proof-of-concept for other employees could be prioritized in receiving such grants to incentivize other employers to implement similar programs.
- **Direct funding to training partners to subsidize participation costs that serve to catalyze the growth of experienced partners**. Providing more readily available and less costly training options to private-sector employers will enable a wider range of employers in the industry to support the professional development of their entry-level employees. Additionally, providing

[10] Mark Montgomery, "Critical cybersecurity education program turns 21," *Federal News Network*, January 8, 2021. (https://federalnewsnetwork.com/commentary/2021/01/critical-cybersecurity-education-program-turns-21)

these professional development opportunities as part of a broader retention strategy may help reduce employee turnover.[11]

- **Award federal contracting preference to private companies that prioritize investing in cyber training capabilities and programs**.

Simply put, providing incentives to employers for hiring and investing in early-career employees is a way to increase the future pool of mid-career professionals, addressing one of the most intractable challenges in developing entry-level employees into mid-career professionals. The next recommendation will expand on how the federal government could invest in its own early-career professionals.

Recommendation 4: Establish a Federal Cyber Workforce Development Institute for an early-career development program for the federal cyber workforce

Similar to their private-sector counterparts, federal employers would also benefit from investing in early-career cyber professionals through talent development programs. To address this challenge, the NCD should work with relevant congressional committees to authorize and establish the Federal Cyber Workforce Development Institute ("the Institute") for early-career talent development. The Institute would enable human capital officers across the government to draw on shared resources for employee education and professional development, which they could augment with additional options tailored to their organization's specific mission and needs.

The Institute would provide work role-specific training, with hands-on learning and skill-based assessments, to the federal cyber workforce for upskilling and reskilling. The Institute would prioritize entry-level positions for curriculum and training, enabling career progression within the federal cyber workforce. It would incorporate work-based learning in personnel training and develop a system to communicate the qualification and proficiency of individuals who successfully complete training through the Institute. The idea is to enable career progression within the cyber workforce through continuous learning and professional development. The goal of prioritizing early-career professionals is to grow the mid-career talent pool and create a strong national cyber workforce.

Furthermore, the Institute could train Human Resources (HR) Specialists to lead talent management and recruitment initiatives for the federal cyber workforce. As experts on the cyber workforce and talent pool, these newly trained HR Specialists would create a virtuous cycle by becoming one of the most important stakeholders in informing the Institute's policies and objectives, such as outreach programs. As the connective tissue between departments and agencies to the strategic priorities, HR Specialists could ensure the success of existing programs. HR Specialists would have an invaluable role in knowledge transfer throughout the federal government. **Recommendations 5** and **6** will expand on the roles and responsibilities of HR Specialists.

[11] Dr. Georgianna Shea and Matthew Brockie, "Washington must act to build capable federal cybersecurity workforce," *Federal Times*, September 6, 2022. (https://www.federaltimes.com/thought-leadership/2022/09/06/washington-must-act-to-build-capable-federal-cybersecurity-workforce/)

Recommendation 5: Develop and leverage the new cadre of HR Specialists for record-keeping and metrics analysis

The inconsistent cyber talent development efforts and lack of data collection on the current cyber workforce pose various challenges. The inability to accurately assess the skill sets to fill cyber-related positions hinders the federal government from gaining a comprehensive picture of the skill sets needed to enable the smooth functioning of cyber activities in each department and agency.

Human Resources Specialists are at the heart of many of the solutions for building and expanding the cyber workforce. The policies that shape the future workforce should be based on clear data and consistent metrics. HR Specialists ensure consistent data collection.

These same hiring managers in all departments and agencies are the ones who will need to exercise agility and flexibility in hiring team members and determining compensation. HR Specialists ensure employees can move fluidly between different agencies and follow career paths that cross back and forth between the private and public sectors. Finally, and critically, HR Specialists help ensure that individuals can take a wide variety of pathways into government jobs. These jobs will need to draw in seasoned cyber veterans, entry-level candidates with enthusiasm for the work, and the myriad of professionals from diverse backgrounds that land in between.

HR Specialists could work with the NCD to help departments and agencies identify specific skill sets and talents needed to advance their mission by identifying appropriate metrics and maintaining proper data. HR Specialists' roles in managing the Institute would include establishing a system for consistent and accurate data collection and identifying appropriate metrics to measure the Institute's success. An immediate concern is the pending expiration of the Federal Cybersecurity Workforce Assessment Act, which requires agencies to identify and code positions using the NICE Framework and identify critical cybersecurity roles and report them annually.[12] The NCD should work with Congress to extend the requirements in this legislation.[13]

Developing and maintaining a system to record consistent data would inform future cyber workforce development plans and a holistic view of the skill sets needed to fill cyber-related positions and develop, implement, and improve cyber workforce development programs.

[12] "Policy, Data, Oversight: Human Capital Management," *U.S. Office of Personnel Management*, accessed November 2, 2022. (https://www.opm.gov/policy-data-oversight/human-capital-management/cybersecurity/)

[13] Laura Bate and Mark Montgomery, "Workforce Development Agenda for the National Cyber Director," June 2022, page 19. (https://cybersolarium.org/wp-content/uploads/2022/05/CSC2.0_Report_WorkforceDevelopmentAgenda_FullText.pdf)

IV. Diversity, Equity, Inclusion, and Accessibility - DEIA in the Cyber Workforce

The following section provides ways to help the NCD address the challenges of **attracting people from underrepresented communities in cybersecurity and providing them opportunities to join the cyber workforce**.

Recommendation 6: Leverage the new cadre of HR Specialists for outreach and engagement with underrepresented communities

Providing sources of learning and professional experience to a demographically and geographically diverse workforce is essential to developing a strong cyber workforce for the nation. Ensuring the availability of sustained funding and resources, however, is a more effective primary driver of program growth over the overall strategic impact of cyber workforce programs. HR Specialists can provide the NCD with insights and analysis to ensure that effective cyber workforce development programs that target the underrepresented communities receive sustained funding for continued outreach and engagement programs.

There are existing programs that directly serve and attract people from underrepresented communities in cybersecurity. For example, Cyber.org, a CETAP grant recipient, launched a recruitment initiative called Project REACH that aims to bolster the nation's cyber workforce by providing high school students with resources and training to pursue undergraduate degrees in cybersecurity.[14] Project REACH brings awareness of and access to cybersecurity education for underrepresented students, especially Black K–12 students. Recently, Project REACH expanded its program to 10 additional HBCUs.[15]

HR Specialists should prioritize outreach and engagement to bring awareness to the resources and incentives available to potential beneficiaries, especially underserved communities. HR Specialists should expand the federal government's outreach programs to underrepresented and underserved communities while ensuring that program beneficiaries gain the experience, certifications, and other qualifications most needed and helpful for their career progression.

As mentioned in **Recommendation 2**, the NCD should assess the effectiveness of cyber workforce development programs as part of its budgetary review authorities. To the greatest extent possible, evidence and data should inform the NCD's assessment of strategically aligned and impactful programs. Impactful programs also include those that support specific, often underserved or underrepresented communities and aim for long-term impact rather than short-term return. The current ecosystem of programs benefits from this diversity of efforts and approaches.

Thus, budget reviews and program assessments must adopt a flexible approach to enable sustained or even enhanced funding. These reviews would have a cascading effect; with appropriate funding,

[14] "Project REACH," *Cyber.org*, accessed November 2, 2022. (https://cyber.org/initiatives/project-reach)

[15] Jonathan Greig, "CISA funds expanding access to cybersecurity programs at HBCUs, K-12 schools," *The Record*, October 31, 2022. (https://therecord.media/cisa-funding-expanding-access-to-cybersecurity-programs-at-hbcus-k-12-schools/)

programs like CETAP will be able to reach a larger community and expand the program offerings to a more diverse population.

V. Conclusion

The recommendations in this RFI are selected with a vision for a coordinated, prioritized, and diversified national cyber workforce. Clear data and consistent metrics will inform and drive the policies that shape the future cyber workforce. The NCD can spearhead a viable national cyber workforce development plan by breaking down structural barriers to entry with a flexible approach to reviewing and analyzing the effectiveness of cyber workforce development programs. The federal government has a responsibility to model cyber workforce development efforts and can incentivize private sector employers to invest in and hire early-career cyber professionals to grow a robust national cyber workforce.

VI. Appendix

Organizational Background

The Center on Cyber and Technology Innovation (CCTI) at the Foundation for Defense of Democracies (FDD) conducts actionable research and develops innovative solutions for policymakers, the defense industrial base, and the average citizen in the quest to defend the evolving U.S. interests in cyberspace.

CCTI seeks to advance U.S. prosperity and security through technology innovation while countering cyber threats that seek to diminish it. CCTI promotes a greater understanding within the U.S. government, private sector, and allied countries of the threats and opportunities to national security posed by the rapidly expanding technological environment. CCTI conducts actionable research and develops innovative solutions for policymakers, the defense industrial base, and the average citizen in the quest to defend the evolving U.S. interests in cyberspace. We combine rigorous academic research of adversaries' strategies and capabilities with scientific experimentation and interdisciplinary study to unlock technological, governance, and policy solutions.

About CSC 2.0 Project

Congress created the Cyberspace Solarium Commission (CSC) in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." CSC operated successfully for three years, publishing its flagship report in March 2020 and subsequent white papers. The Commission provided recommendations to policymakers on how to better organize the U.S. government to succeed in the domain, improve collaboration with the private sector so that industry can better protect itself, and coordinate with U.S. allies to strengthen norms in cyberspace and attribute and punish those that violate them.

As the Commission was reaching the end of its planned term in December 2021, the Commission co-Chairs, Sen. Angus King (I-ME) and Rep. Mike Gallagher (R-WI), determined with the other commissioners that despite their successes, there was more work to be done. And thus CSC 2.0 was born. All former commissioners (including the four members of Congress who served on the commission) have agreed to continue serving the mission as distinguished advisors to the new initiative, and Sen. King and Rep. Gallagher continue to serve as co-chairs.

CSC 2.0's mission is to 1) support continued implementation of outstanding CSC recommendations, 2) provide annual assessments of the adoption and implementation of recommendations, and 3) conduct research and analysis on several outstanding issues the Commission identified during its tenure. Additionally, in its early months, the key task of the CSC 2.0 project was to create a new website, www.cybersolarium.org, to house and make easily accessible the CSC's work product and preserve the CSC's legacy.

To that end, CSC 2.0 released an annual assessment (here) earlier this fall. The authors note that, of the Commission's original 82 recommendations, nearly 60 percent are fully implemented or nearing implementation, with an additional 25 percent on track to implementation. At this time last year, roughly

35 percent were fully implemented or nearing implementation, with 45 percent on track. This adoption level is largely unprecedented. Historically, commissions not created in response to a disaster (such as the 9/11 Commission) have about 31 percent of their recommendations subsequently adopted in full by the U.S. government.

As part of the report rollout, CSC 2.0 hosted Sen. King and Rep. Gallagher in discussion with Tim Starks of *The Washington Post* to talk about progress towards enhancing national cyber resilience. Among other topics, they discussed the importance of the Office of the National Cyber Director and what they hope to see in the forthcoming National Cyber Strategy. A video and transcript of the event are available here.

To continue the research launched by the Commission, CSC 2.0 is focused on expanding the size and make-up of the cybersecurity workforce. The nation needs three times as many cyber personnel as are currently employed. In a white paper on federal cyber workforce development, the Cyberspace Solarium Commission observed that "there is a dearth of information needed to inform sound cyber workforce policy."

CSC 2.0 is researching policy solutions to aid the federal government better understand workforce shortages and better train and compensate federal cyber employees. Earlier this summer, CSC 2.0 published a report (here) outlining these findings and offering concrete recommendations for the National Cyber Director, Congress, and the private sector. As part of the rollout of this report, CSC 2.0 hosted an event (video and transcript available here) with National Cyber Director Chris Inglis, who commented that the report included "eminently sensible recommendations." The report was featured in *The Washington Post*'s Cybersecurity 202 which summarized the findings and noted, "Efforts are already underway to get the report's recommendations enacted." The event also received coverage in Politico's Morning Cybersecurity, FCW, and Inside Cybersecurity, and aired on C-SPAN television and radio.

Center on Cyber and Technology Innovation Team

CSC 2.0 is housed at the Foundation for Defense of Democracies' (FDD) Center on Cyber and Technology Innovation (CCTI). CCTI seeks to advance U.S. prosperity and security through technology innovation while countering threats to the U.S. government, private sector, and allied countries. FDD is a Washington, DC-based, nonpartisan 501(c)(3) research institute focusing on national security and foreign policy. FDD is funded exclusively by U.S. philanthropies and philanthropists and accepts no foreign government or corporate donations.

Dr. Samantha Ravich is the chairman of FDD's Center on Cyber and Technology Innovation (CCTI) and its Transformative Cyber Innovation Lab (TCIL) and the principal investigator on FDD's Cyber-Enabled Economic Warfare project. She serves as a member of the U.S. Secret Service's Cyber Investigation Advisory Board. Most recently, she also served as a commissioner on the congressionally mandated Cyberspace Solarium Commission. She previously served as vice chair of the President's Intelligence Advisory Board (PIAB), co-chair of the Artificial Intelligence Working Group of the Secretary of Energy Advisory Board, and the Republican co-chair of the congressionally mandated National Commission for Review of Research and Development Programs in the United States Intelligence Community. Samantha was deputy national security advisor for Vice President Cheney, focusing on Asia and Middle East Affairs as well as on counter-terrorism and counter-proliferation. She is an advisor on cyber and geo-political threats and trends to numerous technology, manufacturing, and services companies; a managing partner of A2P, a social data analytics firm; and on the board of directors for International Game Technology (NYSE: IGT).

Mark Montgomery is the senior director of FDD's Center on Cyber and Technology Innovation (CCTI) and an FDD Senior Fellow. Mark also directs CSC 2.0, an initiative that works to implement the recommendations of the congressionally mandated Cyberspace Solarium Commission, where he served as executive director. Previously, Mark served as policy director for the Senate Armed Services Committee under the leadership of Senator John S. McCain, coordinating policy efforts on national security strategy, capabilities and requirements, and cyber policy. Mark served for 32 years in the U.S. Navy as a nuclear-trained surface warfare officer, retiring as a rear admiral in 2017. His flag officer assignments included director of operations (J3) at U.S. Pacific Command; commander of Carrier Strike Group 5, embarked on the USS George Washington, stationed in Japan; and deputy director for plans, policy, and strategy (J5) at U.S. European Command. He was assigned to the National Security Council from 1998 to 2000, serving as director for transnational threats.

Dr. Georgianna "George" Shea is the Chief Technologist for FDD's Center on Cyber and Technology Innovation (CCTI) and Transformative Cyber Innovation Lab (TCIL). Prior to coming to FDD, George spent 20 years spearheading cyber initiatives throughout the Department of Defense and other government organizations. Most recently, she served as a subject matter expert and consultant to the Office of the Secretary of Defense, where she led multiple efforts to improve cyber resiliency and advance the practice of cybersecurity testing and evaluation by providing deep cyber resilience analysis, guidance, and engagements with Army, Navy, USMC, Air Force, and Space Force programs within the acquisition process. Prior to working on cybersecurity test and evaluation, she specialized in cyber operations capability development, implementation, and execution for the Department of Defense, Department of Justice, and the Department of Energy. George is a member of the Cybersecurity Canon at The Ohio State University and the Global Resilience Federation's Operational Resilience Framework Working Group.

Annie Fixler is the deputy director of FDD's Center on Cyber and Technology Innovation (CCTI) and a research fellow at FDD. She works on issues related to the national security implications of cyberattacks on economic targets, adversarial strategies and capabilities, and U.S. cyber resilience. She also contributes to the work of FDD's Center on Economic and Financial Power (CEFP) on offensive and defensive tools of economic coercion.

Jiwon Ma is a program analyst at FDD's Center on Cyber and Technology Innovation (CCTI), where she contributes to the CSC 2.0 project. Her research focuses on the cyber threat landscape, adversarial strategies and capabilities, emerging technologies, cyber deterrence, and U.S. cyber and international security policies. Before joining FDD, she was the Editor-in-Chief of the Journal of International Affairs at Columbia University. She has contributed to cybersecurity reports published at the School of Public and International Affairs at Columbia University and the Belfer Center for Science and International Affairs.