

Congress of the United States
Washington, DC 20515

April 26, 2022

The Honorable Rosa DeLauro
Chairwoman
House Committee on Appropriations
H-405, The Capitol
Washington, DC 20515

The Honorable Kay Granger
Ranking Member
House Committee on Appropriations
H-405, The Capitol
Washington, DC 20515

Dear Chairwoman DeLauro and Ranking Member Granger:

In March 2020, the Cyberspace Solarium Commission published recommendations for defending the United States in cyberspace. As a result of Congress's determined attention to cybersecurity issues in the intervening two years, more than 80 percent of the Commission's original recommendations have seen significant progress, and almost half of them are implemented or nearly so. However, the implementation of a recommendation – codifying it in law, establishment through executive order, or otherwise – does not guarantee success. In order to have a meaningful impact on cybersecurity, these efforts must now be resourced appropriately. Accordingly, we are seeking your support for the funding recommendations below.

The Cyberspace Solarium Commission was established by the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 as a bipartisan, intergovernmental, and public-private body charged with evaluating approaches to defending the United States in cyberspace and driving consensus toward a comprehensive cyber strategy. Composed of cyber experts, private-sector leaders, Members of Congress, and senior officials from the executive branch, the Commission made 82 individual recommendations in its March 2020 report, which include legislative, executive, and private sector solutions that will improve the United States' footing in cyberspace. Subsequent white papers account for an additional 33 recommendations, addressing the information and communications technology supply chain, the cybersecurity workforce, lessons learned from the COVID-19 pandemic, and countering foreign disinformation.

Drawing on this body of work, we have outlined below recommended budget changes and report language. We ask that you support these requests to ensure that Congress's recent work on cybersecurity leads to lasting improvements in defending the United States in cyberspace.

Commerce, Justice, Science, and Related Agencies

- With almost 40,000 open cybersecurity jobs, the public sector suffers from a significant shortage in its cyber workforce. Upon entering government, cybersecurity personnel must also have

rewarding career paths and the education and training opportunities necessary to keep their skills relevant and up to date within a rapidly changing field. The CyberCorps®: Scholarship for Service (SFS) program, managed by the National Science Foundation in conjunction with the Department of Homeland Security and the Office of Personnel Management, awards scholarships to university students studying cybersecurity and, in return, requires the recipients to work for a federal, state, local, or tribal government organization in a position related to cybersecurity, or for a SFS school, upon graduation. **We recommend funding for the CyberCorps® program be set at \$80 million in FY23, \$5 million above the request.**

We note our strong opinion that this funding should not be divided or diminished to fund a replication of the Scholarship for Service model in any other fields of emerging technology. While such programs are critical in their importance, their development should not come at the expense of the public sector cyber workforce's development through the CyberCorps® program. Rather, these emerging technologies could be incorporated into the CyberCorps® program as they pertain to cybersecurity (e.g. data scientists in cybersecurity, securing intelligent systems).

Relatedly, this funding should not be divided or diminished to support the expansion of K-12 cybersecurity education. Though a critical priority, K-12 efforts are best addressed in their current organizational placements (at DHS, and to an extent in different funding categories at NSF). Though the President's budget suggests the relocation of K-12 cybersecurity efforts to NSF, we emphatically recommend that the Committee seeks greater clarification about the impacts and rationale for such a move before supporting any relocation of the efforts. For this purpose, we have provided recommended language in the Homeland Security section of this letter. **We further request the following report language:**

“CyberCorps®: Scholarship for Service (SFS).— The Committee provides no less than \$80,000,000 for the CyberCorps®: Scholarship for Service program. The National Science Foundation is encouraged to use the additional funding to increase the number of scholarships awarded at participating institutions and to increase the number of institutions that receive grants to participate in the program.”

- **Four of the Commission's recommendations impact the National Institute of Standards and Technology (NIST),** reflecting the significance of this agency's work in promoting a secure cyberspace:

1) Through its leadership, coordination, and participation in standards development, NIST plays a critical role in national and international **standards development organizations**. These standards organizations are pivotal in determining the future development of cyberspace, and participation in and contributions to these bodies are vital to American economic and security interests. In order to participate most effectively, NIST needs depth of technical expertise, understanding of the affected industries, knowledge of the standards organizations, and active and consistent participation in these bodies.

2) **NIST's core cybersecurity and privacy activities** include maintaining the National Vulnerabilities Database, establishing review processes and standards for new cryptographic approaches, providing critical tools to advance software security nationwide, and offering frameworks for risk management and privacy. Because the need for these functions is constantly growing as digital connectivity expands, NIST requires additional resources to continue to provide these core services. Meanwhile, new developments and evolving technologies have

necessitated drastically scaling up existing projects, for example, in Internet infrastructure and Internet of Things (IoT) standards development. The President’s budget requests funding for certain elements of NIST’s work – supply chain security, next generation telecommunications, identity management, privacy engineering, and some workforce issues – but, particularly when divided across all these priorities, the \$18 million increase in the President’s request is insufficient for the recent expansions in the work required in these areas, and the request leaves many other priority areas unaddressed.

3) Section 9401 of the FY21 NDAA authorized a program for **regional cybersecurity workforce development programs** administered by the National Initiative for Cybersecurity Education within NIST. The regional alliances and multi-stakeholder partnerships authorized in the legislation require a series of cooperative agreements with local partners, which may include funding. This mandate, and others implemented in Sections 9401 and 9407 of the FY21 NDAA on the cybersecurity workforce, require funding to enable implementation.

4) NIST most recently issued **guidance on vulnerability patching implementation** in 2013 in Special Publication 800-40. Given the pace of change in the cyber domain – and the fact that unpatched systems remain a major point of entry for malicious cyber actors – the guidance is due to be updated.

5) The Commission recommends many steps for improving cybersecurity for industrial control systems (ICS), key technical elements of critical infrastructure. An underlying barrier to implementation of these recommendations is the lack of clear, widely accepted criteria for ICS cybersecurity, which is to say the technical and non-technical cybersecurity outcomes that are expected of secure ICS devices. However, the Internet of Things Cybersecurity Improvement Act of 2020 authorized work that can be used to meet this purpose. Pursuant to that legislation, the National Institute of Standards and Technology has produced cybersecurity requirements for federal use of Internet of Things (IoT) devices (NIST SP 800-213/A). IoT devices share major similarities with industrial control systems (ICS) devices, as both are digital components characterized by a sensor or actuator that allows them to interact with the real world. Because devices procured by the federal government must comply with NIST SP 800-213, per the IoT Cybersecurity Improvement Act of 2020, a **certification system to guide federal procurement of ICS devices** will be both practically necessary and very useful as a means of establishing a standard that could be used in the private sector as well.

To facilitate hiring scientists, engineers, and subject matter experts who can meet the increasing demands across multiple emerging technologies and to provide necessary support for those added positions, **we recommend an increase of \$54 million over the request for NIST Cybersecurity and Privacy portfolio, and we support the \$14.03 million increase requested in the President’s budget for Standards Coordination and Special Programs within the Measurement Science, Services, and Programs activity. We further recommend the following report language:**

“International Standards.—The Committee recognizes NIST’s important role in U.S. engagement on standards development across areas of critical and emerging technologies. NIST’s partnership with the private sector and international standards coordination bodies, its work to drive information sharing across the federal government related to emerging standards issues, and its critical contributions to the development of a National Strategy for Critical and Emerging Technologies will only grow in importance throughout the coming years, particularly as the

People’s Republic of China grows its engagement in international standard-setting fora. To that end, the Committee recommends that not less than \$14,030,000 be made available for Standards Coordination and Special Programs.”

*“Cybersecurity and Privacy Standards.—*The Committee provides increases above the request of not less than the specified amounts above the request in the following areas within NIST’s Cybersecurity and Privacy activity for purposes including increasing personnel and contracting resources: \$2,000,000 for vulnerability management, \$2,000,000 for cryptography programs, \$8,000,000 for privacy programs, \$1,500,000 for identity and access management, \$6,000,000 for software security, \$2,500,000 for infrastructure with a particular focus on Domain Name System and Border Gateway Protocol security, \$3,000,000 for the National Initiative for Cybersecurity Education with a particular focus on expanding office and personnel capacity to support the workforce requirements authorized in Section 9401 and 9407 of the Fiscal Year 2021 National Defense Authorization Act, and \$6,000,000 for Internet of Things security.”

*“Cybersecurity Education.—*The Committee strongly supports the amendments made to the Cybersecurity Enhancement Act of 2014 as part of the Fiscal Year 2021 National Defense Authorization Act, particularly with respect to cybersecurity challenge programs, as well as regional alliances and multi-stakeholder partnerships. Therefore, the Committee recommends that an increase above the request of not less than \$5,000,000 of the funds made available for National Institute of Standards and Technology Cybersecurity and Privacy portfolio be used for activities under section 401(f) of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7451), as amended. The Committee further recommends that, of funds made available for National Institute of Standards and Technology Cybersecurity and Privacy Efforts, not less than \$15,000,000 be used for activities under section 205 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7432).”

*“Vulnerability Patching Guidance.—*The Committee notes that NIST last updated Special Publication 800-40, ‘Guide to Enterprise Patch Management Technologies,’ in 2013. Given the importance of timely patching to organizations maintaining a robust cybersecurity posture, no later than 120 days after the enactment of this Act, the National Institute of Standards and Technology is directed to report to the Committee about its plans to revise and update the Special Publication.”

*“Federal Industrial Control Systems Cybersecurity.—*The Committee provides \$3,000,000 above the request to develop criteria – technical and non-technical expected outcomes – for the cybersecurity of industrial control systems (ICS) devices procured by the Federal government. The Committee encourages NIST to carry out this provision in such a way that criteria may also inform cybersecurity considerations in the procurement of ICS devices in different contexts, including in critical infrastructure owned or operated by the private sector. Within 270 days of the enactment of this Act, NIST is directed to report to the Committee on the viability of developing the criteria into a certification system and any authorities or resources necessary to support widespread, including international, adoption of the criteria developed and any subsequent certification systems.”

- A comprehensive understanding of cyber threats requires extensive **identification and tracking of foreign adversaries operating domestically**, generally accomplished through intelligence gathering; evidence collection; technical and human operations; and the cooperation of victims and third-party providers. The Federal Bureau of Investigation’s (FBI) cyber mission has a unique

dual responsibility: To gather and leverage intelligence in order to prevent harm to national security and to enforce federal laws as the nation’s primary federal law enforcement agency. Both roles are essential to investigating and countering cyber threats to the nation and are critical to whole-of-government campaigns supporting layered cyber deterrence, the strategic framework agreed upon by the Commission. Moreover, the FBI plays a key role in intelligence sharing and joint cyber operations with partners around the world through its Cyber Assistant Legal Attachés (cyber ALATs). The Commission strongly believes in the effectiveness of these personnel and supports increased funding to allow more cyber ALATs to be positioned at embassies of interest. To ensure that the FBI is properly resourced to carry out its cyber mission and perform attribution; to strengthen whole-of-government counter-threat campaigns and enable other agency missions in support of national strategic objectives; and to strengthen FBI’s capacity to work with international partners to counter cyber threat actors abroad, **we recommend an increase of \$52.0 million in funding for FBI cyber over FY22 enacted levels. We also recommend the following report language:**

“Cyber Assistant Legal Attachés.—The Committee strongly supports the FBI’s Cyber Assistant Legal Attaché (cyber ALAT) Program, which facilitates intelligence sharing and helps coordinate joint law enforcement investigations. Eliminating safe havens for cyber criminals is a key priority, and international cooperation is essential to holding bad actors accountable. Accordingly, the Committee supports the use of this funding to grow the cyber ALAT program in support of the Bureau’s mission as the lead agency for cyber threat response.”

- In order to support the creation and maintenance of federal programs designed to better recruit, develop, and retain cyber talent, policymakers need accurate, up-to-date data. In particular, **more research on the current state of the cyber workforce**, paths to entry, and demographics can help ensure that federal hiring programs progress in innovating recruitment, enhancing the workforce, and retaining top talent. Much of this research can be done using existing authorizations for the National Center for Science and Engineering Statistics (NCSES), which is tasked with providing statistical data on the U.S. science and engineering enterprise. To enable data-driven policy approaches to bolstering cybersecurity education, **we recommend an increase in appropriations for the NCSES of \$4.75 million and the following report language:**

“Cybersecurity Workforce.—The Committee recommends an increase for the National Center for Science and Engineering Statistics (NCSES) of \$4,750,000 to undertake a study to identify, compile, and analyze existing nationwide data and conduct survey research as necessary to better understand the national cyber workforce. Noting the already low ratio of personnel to budget at NCSES relative to other federal statistical agencies, the Committee encourages expenditure of appropriated funds to support additional personnel, which may include statisticians, economists, research scientists, and other statistical and support staff as needed, to ensure adequate staffing for this research.”

- Across a wide range of issues, the increasing prevalence of foreign disinformation spread online continues to undermine public confidence in critical institutions and the effectiveness of public messaging during times of crisis. Researchers, civil society organizations, and other nongovernmental organizations are already working to better understand and counter these threats. **We recommend that an increase of \$3 million be appropriated to support the Department of Justice’s Office of Justice Programs in providing grants to these organizations and the following report language:**

“Foreign Disinformation Research Grants.—Of the funding appropriated for the Office of Justice Programs, not less than \$3,000,000 will be used for research grants to nonprofit organizations seeking to identify, expose, and explain malign foreign influence campaigns to the American public. Grants may be administered by a component of the Office of Justice Programs. The Committee encourages the administering office to work in consultation with the Department of Homeland Security and the National Science Foundation.”

- The international telecommunications market is currently watching the race to develop **Fifth Generation (5G) technology**. However, maintaining competitiveness in the market for future generations of telecommunications technology will rely heavily on current investment in research and development in both the technologies themselves and the radio frequency spectrum management needed to enable next generation communications use. To support this investment in innovation, **we recommend an increase of \$4.12 million over the Fiscal Year 2023 request for Advanced Communications Research at the National Telecommunications and Information Administration and the following report language.**

“Next Generation Communications Research.—The Committee provides an increase of \$4,120,000 for Advanced Communications Research at the Institute for Telecommunication Sciences to expand research and development in radio frequency spectrum management to allow next generation communications use and to ensure that 5G networks and the broader telecommunications supply chain are secure, including through vendor diversity.”

- A pillar of the Commission’s strategy of layered cyber deterrence is denying adversaries the benefits of attacking the United States in cyberspace by reshaping the cyber ecosystem towards greater security. The **National Telecommunications and Information Administration** plays a key role in this effort through its coordination of multi-stakeholder efforts to develop market-based and risk-based cybersecurity guidance that improve transparency, security, and resilience across the ecosystem. These and other NTIA efforts must evolve with the broader U.S. government effort to promote and protect standards that align with U.S. values for the future of telecommunications. Accordingly, NTIA must have sufficient personnel capacity to engage, particularly in the International Telecommunications Union, in the development of international communication standards, especially those relevant to emerging technologies. **Accordingly, we support the administration’s requested increase of \$2,036,000 for the Domestic and International Policies program at NTIA.**

Defense

- Investing in the efforts of our international partners and allies to strengthen their cyber defenses improves the United States’ ability to shape the behavior of other actors in cyberspace and pursue collective security in cyberspace with partners and allies. The Defense Security Cooperation Agency, through Regional Centers for Security Studies and the Institute for Security Governance, is a key implementer of institutional capacity-building programs. The Regional Centers for Security Studies provide courses and training to partner nations on cybersecurity and cyber defense, and the administration specifically referenced the George C. Marshall European Center for Security Studies as a provider of training on cyber incident attribution and cyber norms in

response to harmful foreign activities of the Russian government.¹ **Accordingly, we recommend the following report language:**

“Regional Centers for Security Studies.—Of the funds appropriated to the Regional Centers at the Defense Security Cooperation Agency, not less than \$6,000,000 shall support efforts conducted by Regional Centers for Security Studies to build cyber capacity, cooperation, and interoperability with international partners and allies. In particular, the Committee strongly supports the administration’s 2021 commitment to provide training for foreign policymakers and diplomats on the policy and technical aspects of public attribution and on the applicability of international law in cyberspace offered at the George C. Marshall European Center for Security Studies.”

“Institute for Security Governance (ISG).—Of funds appropriated to the Security Cooperation Act at the Defense Security Cooperation Agency, not less than \$10,000,000 shall support the ISG’s efforts as the primary implementer of Department of Defense institutional capacity-building programs and the ISG’s focus on the priority area of cybersecurity.”

Financial Services and General Government

- Since its establishment pursuant to Section 1752 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, the Office of the National Cyber Director has rapidly grown to meet its mandate to serve as the lead for national-level coordination of U.S. cyber strategy and policy implementation. **We support the President’s budget request of \$23,000,000 for salaries and expenses at the Office of the National Cyber Director** to fund remaining office establishment and operational expenses and to provide continued growth to full staffing levels.
- The Office of Personnel Management has issued government-wide direct hire authority for certain cybersecurity positions, and continues to provide compensation flexibilities including special rates, recruitment, retention and relocation incentives to attract and retain cybersecurity talent. However, these tools are not widely utilized or understood in many hiring offices across the federal government. Enhanced OPM support to federal hiring offices would ensure existing cybersecurity compensation flexibilities and direct hire authorities are used to the fullest extent possible. Accordingly, **we recommend an increase of \$3,000,000 above the request to the Employee Services account at the Office of Personnel Management to enhance the Federal Government’s strategic workforce planning and talent acquisition. We also recommend the following report language:**

“Cybersecurity Workforce - The Committee provides an increase of \$3,000,000 above the request to enhance the Federal Government’s strategic workforce planning and talent acquisition. OPM is directed to expand efforts to teach federal personnel responsible for hiring, retention, and employee development programs governmentwide to more effectively utilize existing hiring authorities, compensation flexibilities, employee development programs, and other resources for federal cyber workforce development.”

- Supporting the Federal Government’s migration towards a **zero trust architecture (ZTA)** is

¹ FACT SHEET: “Imposing Costs for Harmful Foreign Activities by the Russian Government”

<https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/>

essential to improving the nation's cybersecurity in the face of increasingly sophisticated and persistent cyber threats. Per guidance issued in early 2021, federal agencies are subject to specific requirements, such as the development of centralized identity management systems, that will together support a government-wide move to ZTA in the coming years. Implementing these requirements will necessitate significant investments on the part of agencies. As such, it is imperative that the Committee seize opportunities to fund appropriations requests in support of ZTA migration, particularly requests that could propel an agency's rapid advancement along the path of ZTA implementation and provide a maturation model for other agencies to follow. **To that effect, we strongly support the Department of the Treasury's requested increase to its Cybersecurity Enhancement Account, which includes \$86,452,000 for Zero Trust Architecture Implementation.**

We also recognize that different agencies have different capacities and resources to put towards ZTA migration. Certain agencies may require greater supplementary funding assistance in sustaining the technology modernization investments required for the transition to Zero Trust Architecture. The General Services Administration's Technology Modernization Fund (TMF) is a key source of such supplementary funding that helps agencies overcome budgetary constraints to fulfill information technology modernization projects and address urgent cybersecurity needs. Agencies are already working through the TMF to fund zero-trust modernization efforts, and ensuring that the TMF is adequately resourced will ensure its ability to support additional agencies on ZTA modernization in the coming years. **Accordingly, we support the administration's request of \$300 million for the Technology Modernization Fund.**

- Trust in the cybersecurity of the electoral system is critical for the functioning of American democracy. The Election Assistance Commission's (EAC) mission is to help election officials improve the administration of elections and improve voter participation, yet it suffers from chronic funding and personnel shortages that prevent it from accomplishing those goals. Increased funding will allow it to assist states and localities in defense of the digital election infrastructure that underpins federal elections and to ensure the widest use of voter-verifiable, auditable, and paper-based voting systems. We support the President's budget request for salaries and expenses for the EAC for FY23, and **accordingly recommend an appropriation of \$30.087 million**, which would represent an increase of \$10.087 million above the amount specified in the Consolidated Appropriations Act, 2022.
- The Department of the Treasury's **Office of Cybersecurity and Critical Infrastructure Protection** serves as the Sector Risk Management Agency (SRMA) for the financial services sector. As such, the office manages much of the day-to-day engagement on cybersecurity issues between the federal government and private-sector entities by, for example, by facilitating information sharing, advocating for the use of best-practice security measures, and helping critical infrastructure owners and operators respond to significant incidents. This mission is distinct from ongoing efforts to enhance the Department of the Treasury's own cybersecurity posture, but responds to similar risks. Just as unfolding geopolitical events and increased sanctions pressure puts the Department of the Treasury at risk of cyber attack, they also invite additional risks for privately owned financial sector critical infrastructure. OCCIP helps the private sector assess and respond to that risk. Because of the globally interconnected nature of finance, the office also supports bilateral and multilateral efforts to improve financial sector cybersecurity. However, as the cybersecurity risks to the financial services sector grow and

uptake of the office's SRMA functions increases, the budget for the office has not kept pace. Therefore, **we recommend an increase of \$11.505 above the FY22 request for the Office of Cybersecurity and Critical Infrastructure Protection** to increase funding available for additional personnel in order to support communication and coordination with the financial services sector. We also recommend the following report language:

"Financial Sector Cybersecurity.—The Committee provides an increase of \$11,505,000 above the request to improve financial services sector critical infrastructure resilience to cybersecurity attacks through the Office of Cybersecurity and Critical Infrastructure Protection (OCCIP). The Committee encourages OCCIP to expand risk assessment and mitigation capabilities as a part of its role as a Sector Risk Management Agency. The office is further encouraged to engage in efforts to map third party dependencies in the financial sector, provide analysis of domestic and international cybersecurity threats and vulnerabilities, and support bilateral and multilateral engagement on financial sector cybersecurity in strategically important regions like Eastern Europe and East Asia."

- The Commission supports strengthening the capacity of the **Committee on Foreign Investment in the United States (CFIUS)**. Specifically, the Commission raised concerns about the adequacy of CFIUS reviews of bankruptcy buyouts and restructuring, as well as early-stage venture capital and private equity investment in companies of interest. Federal bankruptcy judges are a key component to this recommendation. **Therefore, we recommend the following report language:**

"Education and Training of Judges.—The Committee recognizes the importance of national security considerations in reviewing bankruptcy and investment transactions, and encourages the Federal Judicial Center to educate bankruptcy judges on the Committee on Foreign Investment in the United States process and how bankruptcy court decisions impact this process and national security. Not later than 180 days after the enactment of this Act, the Center is directed to report to the Committee on its plans to incorporate national security considerations into bankruptcy judge educational activities."

Homeland Security

- The budget justification for the Cybersecurity and Infrastructure Security Agency for FY23 does not reflect the Committee's historic investments in cybersecurity that were included in the Consolidated Appropriations Act, 2022. We note this divergence on many issues in which the FY22 appropriation addressed the Commission's recommendations for that year, including **sector risk management agencies, national critical functions, federal civilian and non-federal threat hunting, cyber exercises, vulnerability management infrastructure, and voluntary threat detection programs including CyberSentry**. In cases where CISA's budget justification proposes an increase for FY23 above the annualized continuing resolution (CR) amount for FY22, **we recommend that appropriators consider the FY22 appropriation, rather than CISA's annualized CR, as the baseline on which to build an increase**. In other words, recognizing the atypical timeline for the FY22 appropriation, we recommend that the Committee builds on last year's investment in cybersecurity as it is reflected in the FY22 appropriation, rather than interpreting the President's FY23 budget as a request for a funding decrease in these critical areas. **We further recommend the following report language:**

“Cyber Budget Continuity.—CISA is directed to update its Fiscal Year 2023 budget request to incorporate and continue funding appropriated by the Committee for Fiscal Year 2022, including for sector risk management agencies, national critical functions, federal civilian and non-federal threat hunting, cyber exercises, vulnerability management infrastructure, and voluntary threat detection programs including CyberSentry. The Committee expects to see this investment in cybersecurity reflected in the coming year’s budget request, including CISA’s funding plan to expand and build on funding appropriated for Fiscal Year 2022 and continued in this Act.”

- Section 1715 of the FY21 NDAA authorized the creation of a Joint Cyber Planning Office (JCPO) within the Cybersecurity and Infrastructure Security Agency (CISA) to coordinate cybersecurity planning and readiness across the federal government and between public and private sectors for significant cyber incidents and malicious cyber campaigns. The JCPO became an integral part of the **Joint Cyber Defense Collaborative (JCDC)** in operationalizing this mandate. Yet the JCDC’s mission extends beyond planning and readiness, and encompasses CISA’s broader effort to foster operational cybersecurity collaboration between the public and private sector. This, in turn, requires improved combined public-private situational awareness of cyber threats to better support government and private-sector cyber defense efforts. CISA has taken meaningful steps towards this goal by leveraging the JCDC as a vehicle for increased and improved cyber threat information sharing. The next step in the maturation process towards truly shared situational awareness will be developing the technical means to enable the cross-correlation of this information at the speed and scale necessary for rapid detection and identification of threats. **Accordingly, we recommend the following report language:**

“Collaborative Analysis of Cyber Threat Indicators.—The Committee recognizes the need to develop shared situational awareness of cybersecurity risks and cybersecurity threats across the public and private sectors. Therefore, the Committee supports the use of funds appropriated to the Joint Cyber Defense Collaborative (JCDC) for the identification, purchase, development, and deployment of tools and analytical software that can be applied and shared across the JCDC and interagency to query, receive, manipulate, transform, and display data and information on cybersecurity risks and cybersecurity threats, to enable collaborative analysis and cross-correlation of such data and information at the speed and scale necessary for rapid detection and identification.”

- Section 9603 of the FY21 NDAA requires the development of a **Continuity of the Economy Plan**, a plan to maintain and restore the economy of the United States in response to a significant event. While CISA can leverage many existing efforts to operationalize and maintain this planning effort, some elements of the plan will require significantly greater depth and scope of effort. To produce an effective plan every three years as required, CISA will need to collect and analyze information at a very granular level on issues as diverse as industrial control networks, raw materials, transport and delivery networks, personnel, federal response authorities, and much more. Producing this triennial plan will require additional, ongoing staff support. Accordingly, **we recommend an increase in appropriations of \$1,000,000 for Continuity of the Economy planning and the following report language:**

“Continuity of the Economy Plan.—The agreement provides \$1,000,000 above the request for the development of a Continuity of the Economy Plan, as required by section 9603 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public

Law 116-283).”

- CISA’s **Cybersecurity Advisors (CSAs)** operate via CISA’s existing network of ten regional offices to bring critical cybersecurity expertise to underserved geographic areas and stakeholder bases. Section 1717 of the FY21 NDAA authorized the appointment of a cybersecurity coordinator for each state, which expanded the program’s geographic coverage. However, in locations that are home to a high density to critical infrastructure, a single coordinator will be insufficient to meet the requirements to provide a more mature risk analysis and measurements capability outside of the federal network and provide an increased ability to support special projects and national level events. To meet regional needs for cybersecurity advisory services, **we recommend an increase of \$8 million over the request for the Regional Operations Activity and the following report language:**

“Cybersecurity Advisors (CSAs).—Of funds appropriated, no less than \$8,000,000 shall be used to support additional cybersecurity advisors in the ten CISA regional offices. These advisors will be in addition to the state cybersecurity coordinators established in furtherance of Section 1717 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, in order to supplement regional capability in areas of high demand or particular national security importance.”

- Section 1731 of the FY21 NDAA authorized planning for an **Integrated Cyber Center (ICC)** within CISA to help the agency accomplish its mission of bolstering the resilience and security of American critical infrastructure. The ICC would draw on expanded capabilities across existing programs within CISA’s Cybersecurity Division. Per that legislation, a report detailing the plan to create the ICC was due January 1, 2022, one year from the date of enactment of the FY21 NDAA. Accordingly, **we recommend the following report language:**

“Integrated Cyber Center.—In furtherance of Section 1731 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, the Committee awaits receipt of the study required on the potential for better coordination of Federal cybersecurity efforts at an integrated cybersecurity center within the Cybersecurity and Infrastructure Security Agency.”

- Section 1719 of the FY21 NDAA codified CISA’s **Cybersecurity Education Training Assistance Program (CETAP)**, which supports cybersecurity curriculum development, “train-the-trainer” resources for elementary and secondary school teachers, and other classroom resources. We recommend the program for expansion, enabling it to reach more classrooms nationwide. However, the CISA budget justifications for FY22 and FY23 indicate a non-recur of this program, despite its FY21 authorization. The FY23 request comments further that CISA will work with the National Science Foundation (NSF) to “build and strengthen the national cybersecurity workforce to include K-12 programs,” but at present no obvious parallel teacher training or curriculum development effort exists at NSF. To the contrary, CISA has both the subject matter expertise needed and established history operating this grant successfully. The program should stay at CISA to avoid losing ground in this critical project. Moreover, in its current home, investment in CETAP scales well, meaning that each increase in funding expands outreach to include more educators and students. **To expand support for K-12 cybersecurity education, we recommend an appropriation of \$10 million for CETAP through the Cyber Operations/Capacity Building activity, an increase of \$3.2 million over the Consolidated**

Appropriations Act, 2022 and \$10 million over the request. We believe that this increase will enable the program to impact an additional 30,000 teachers and 3,660,000 students annually at a minimum. **We also recommend the following report language:**

“Cybersecurity Education and Training Assistance Program (CETAP).—The Committee rejects the proposed \$4,300,000 reduction for CETAP and provides \$10,000,000 to enhance CETAP, a program that improves education delivery methods for K–12 students, teachers, counselors, and post-secondary institutions and encourages students to pursue cybersecurity careers. Any proposed reductions to cybersecurity education will not be considered unless CISA provides a clear plan for how the previously funded activities of educator training and curriculum development would be fully realigned within other agencies in a manner that sustains the objectives of this critical effort. CISA is directed to work in collaboration with the National Cyber Director, Office of Management and Budget, and other agencies as needed to develop a strategy for addressing these requirements in future budget requests and to brief the Committee not later than 90 days after the enactment of this Act regarding such strategy.”

- Insurance can incentivize organizational cybersecurity behavior, but the market for cyber insurance is nascent and limited by a lack of quality datasets and models needed to understand, appropriately price, and mitigate cyber risk. A public-private **cybersecurity insurance working group** established within CISA can help develop frameworks and models for understanding and pricing cyber risk and identify areas of interest for pooling public and private sector data that can inform better, more accurate risk models. Accordingly, we recommend the following report language:

“Cybersecurity Insurance Working Group.—The Committee supports the creation of a public private working group housed within CISA to help develop frameworks and models for understanding and pricing cyber risk and to identify areas of interest for pooling public and private sector data that can inform better, more accurate risk models.”

- CISA’s role in protecting American cybersecurity has expanded dramatically in recent years, both in terms of its authorizing legislation and increased budget authority. CISA must hire additional personnel urgently in order to meet this expanded role. As a necessary precursor, **human resources teams within CISA’s mission support services** must be staffed adequately in order to bring on the influx of talent needed across the agency. **Accordingly, we recommend the following report language:**

“Talent Management Mission Support.— The Committee supports ongoing efforts to expand the cyber workforce within CISA, and notes that ambitious hiring goals will only be possible if the agency has the mission support services for talent management needed to process a greatly increased number of hiring actions in a timely manner. Drawing on funding appropriated to Mission Support at CISA, the Committee expects increased personnel to support hiring, including through the accelerated implementation of the Cyber Talent Management System.”

- To support cybersecurity workforce development in FY21, CISA awarded grants under the new **Non-Traditional Training Provider (NTTP) grant program** designed to foster the development of three-year pilot programs. Through apprenticeships, certification programs, and other learning opportunities, the NTTP program helps to catalyze investment in early-career

employees, thus creating pathways for new employees to gain their first crucial years of experience. **We recommend an increase of \$8 million to Cyber Defense Education & Training within the Cyber Operations/Capacity Building activity at CISA and the following report language:**

“Non-Traditional Training Providers.— The appropriation includes \$8,000,000 above the request to support the development of non-traditional training providers in cyber workforce development. The Cybersecurity and Infrastructure Security Agency is encouraged to increase the number of grants targeted at incentivizing and expanding employer-supported efforts to bridge the gap between entry-level and mid-career professionals. Incentivizing the development of programs that provide initial professional experience and hands-on training should be among the key priorities of the grantmaking efforts.”

Labor, Health and Human Services, Education, and Related Agencies

- To counter cyber-enabled information operations, Americans must have the digital literacy tools needed to evaluate the trustworthiness of information spread on online platforms. Furthermore, because the intent of so many cyber-enabled information operations is to cause Americans to distrust or lose faith in the institutions of democracy, digital literacy should be coupled with civics education explaining what democracy is, how individuals can hold their leadership accountable, and why democracy must be nurtured and protected. **To increase the quality of civics education, we recommend establishing a National Education Research and Development Center within the Institute for Education Sciences with \$10,000,000 in funding** dedicated to improving resilience to misinformation and foreign disinformation by funding research on improving media literacy, digital civic engagement, and academic outcomes in civics and history. **We further support the following report language:**

*“Improving Civics Education.—*The Committee applauds the work of the Institute for Education Sciences (IES) and their efforts to identify which pedagogical methods and curricula improve learning outcomes. Civics education is a topic of growing importance, but many programs do not incorporate practices for civic engagement in the digital environment. Students must understand concepts such as media literacy, responsible content sharing, and the prevalence of malicious online influence in order to effectively participate in our democracy and public discourse. Therefore, the Committee directs the Director of IES to establish a National Education Research and Development Center, within the National Center for Education Research, dedicated to improving young and adult learners’ resilience to misinformation and foreign disinformation. This center shall research which educational activities improve critical thinking, media literacy, and digital citizenship; enhance understanding of voting and other forms of political and civic engagement; increase awareness and interest in employment and careers in public service; improve understanding of United States law, history, and government, to include our Constitution and founding documents; improve the ability of participants to collaborate with others to solve local and global problems; expand awareness of malign influence; and strengthen participants’ ability to evaluate the perspective, accuracy, and validity of information. Of the funds appropriated for IES, not less than \$10,000,000 shall be used for this purpose.”

State, Foreign Operations, and Related Programs

- **International cyberspace policy and diplomacy at the Department of State** has historically suffered from bureaucratic and resource constraints. Widespread international engagement, for example on key votes in multilateral organizations, has been hampered by a lack of available personnel. Similarly, programs to reinforce the effectiveness of cyberspace norms have been limited. Moreover, without an appropriately ranked leader to advocate for cyberspace diplomacy equities at an interagency level – and limited official prominence to represent U.S. values abroad – international engagement on cyberspace policy issues have been deprioritized. State Department’s recent establishment of the Bureau of Cyberspace and Digital Policy (CDP) has created an opportunity to address these issues, but overcoming the constraints of limited staffing is an urgent priority that exceeds the seven additional positions specified in the request. Accordingly, to ensure that the new CDP bureau is staffed appropriately, **we recommend an \$2.1 million dollar increase above the request for the CDP bureau, and the following report language:**

“Bureau of Cyberspace and Digital Policy.—The agreement includes not less than \$2,100,000 above the request to increase the number of new positions in the Bureau of Cyberspace and Digital Policy. Not later than 180 days after the enactment of this Act, the Secretary of State is further directed to submit a staffing plan to the Committees on Appropriations that specifies the hiring targets needed to reach full staffing capacity for the Bureau of Cyberspace and Digital Policy, and the steps the Department is planning to take to meet these requirements.”

- **Investing in the efforts of our international partners and allies** to strengthen their cyber capabilities improves our own cybersecurity. It also creates an incentive for these countries to continue collaborating with the United States to shape behavior and impose consequences for malign activity in cyberspace. Current U.S. capacity-building efforts draw from a range of programs and funds. In order to allow the expansion of international cybersecurity capacity building across different geographic regions and for varied purposes we recommend the following increases above the FY23 request to four funds that support different aspects of international cybersecurity capacity building:

1) **\$10 million increase for the Assistance for Europe, Eurasia, and Central Asia Fund for cyber capacity building.** Cyber capacity building efforts in this region would improve security in the region and cybersecurity globally by strengthening allies’ and partners’ capability to counter Russian Federation and Chinese Communist Party influence and aggression.

2) **\$7.5 million increase for the International Narcotics Control and Law Enforcement Fund** for countering cybercrime and intellectual property theft. This recommended increase would support the development and expansion of projects designed to strengthen cooperation among law enforcement and other criminal justice sector professionals on cybercrime issues.

3) **\$5 million increase for the Digital Connectivity and Cybersecurity Partnership** to support the partnership's focus on enhancing cybersecurity.

4) **\$15 million increase for Foreign Military Financing** for bolstering allies’ and partners’ capability to provide for their own defense in cyberspace.

We further recommend the following report language:

*“Building Cybersecurity Capacity in Eastern Europe.—*The Committee recommendation provides not less than \$10,000,000 under this heading for international cybersecurity capacity-building efforts to strengthen collective commitments to security in cyberspace, improve incident response and remediation capabilities, train appropriate personnel on the applicability of international law in cyberspace and the policy and technical aspects of attribution of cyber incidents.”

*“Countering International Cybercrime.—*Of funding appropriated for the International Narcotics Control and Law Enforcement Fund, not less than \$17,500,000 shall be used for capacity building efforts to counter cybercrime, which may include strengthening the ability of foreign policymakers to develop, revise, and implement national laws, policies, and procedures to address cybercrime and strengthening the ability of law enforcement to hold malign actors accountable.”

*“Digital Connectivity and Cybersecurity Partnership.—*The Committee recommends an increase of not less than \$5,000,000 over the request for the Digital Connectivity and Cybersecurity Partnership. The Trade and Development Agency shall support international cybersecurity capacity building efforts that foster government-industry cooperation on cybersecurity, building cultures of cybersecurity within citizen populations, and strengthening capacity to curtail cybercrime.”

*“Military Cybersecurity Capacity Building.—*Of funding appropriated for Foreign Military Financing, not less than \$15,000,000 will be used for international cybersecurity capacity building efforts that strengthen the resilience and readiness of military cyber defenses and encourage regional cooperation against nation-state cyber threats like those emanating from Russia and China.”

*“Capacity Building Administration.—*The Committee recognizes the growing importance of cybersecurity capacity building and the need for personnel experienced in cybersecurity issues to carry out the national cybersecurity strategy. Therefore, the Committee recommends the Department expand efforts to hire experienced personnel to support international cybersecurity capacity building.”

- Enabling allies and partners to strengthen their domestic cybersecurity not only improves global security writ large, it improves U.S. security by creating a community of capable, secure, like-minded countries. The **Economic Support Fund is an important resource for this international cyber capacity building**, and the FY23 budget requests that \$37 million be made available to the new Bureau of Cyberspace and Digital Policy from ESF. Whether or not this funding makes meaningful improvements to international cybersecurity capacity building depends on the extent to which that \$37 million represents existing projects that were realigned from elsewhere in the ESF budget to bring them under the heading of the new bureau, or whether it represents a real increase in funding available for international cybersecurity capacity building. To ensure that international cybersecurity capacity building remains a growing priority in the ESF budget, **we recommend the following language:**

*“International Cybersecurity Capacity Building.—*The agreement includes funding for the

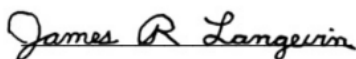
Economic Support Fund to be administered by the Bureau of Cyberspace and Digital Policy. The use of these funds shall include international cybersecurity capacity-building efforts that strengthen civilian cybersecurity through support to countries and organizations, including national and regional institutions. Not later than 180 days from the date of enactment of this Act, the Secretary is instructed to brief the Committees on Appropriations on the projects for which ESF funding through CDP is used, and the extent to which this funding is used for new, expanded, or previously funded projects.”

- As countries with less mature information communication technology (ICT) infrastructure race to advance their digital ecosystem, any donor nation offering support may be welcome. The Chinese Communist Party (CCP) in particular, often supports the development of ICT infrastructure abroad in order to advance its malign interests. However, not all donations of ICT infrastructure are created equal, and the expansion of CCP-backed ICT infrastructure poses a direct threat to an open, interoperable, reliable, and secure global Internet. To enable countries to be discerning in their ICT infrastructure development projects, the Commission has recommended the development of a **digital risk impact assessment**. To allow the United States Agency for International Development to begin work on developing and implementing digital risk impact assessments for U.S. foreign assistance programs, **we recommend an increase of \$5 million for the Bureau for Development, Democracy, and Innovation’s Innovation, Technology, and Research hub**, and the following report language:

“*Digital Risk Impact Assessments*.—Of amounts appropriated to the Bureau for Development Democracy and Innovation at the United States Agency for International Development through the Democracy Fund, not less than \$5,000,000 will be used to develop tools and methods to aid in evaluating the risk incurred through information communication technology development projects.”

Thank you for your consideration of these requests and for your continued commitment to strengthening our nation’s cybersecurity.

Sincerely,



JAMES R. LANGEVIN
Member of Congress



MIKE GALLAGHER
Member of Congress

CC: Hon. Matt Cartwright
Hon. Robert B. Aderholt
Hon. Betty McCollum
Hon. Ken Calvert
Hon. Mike Quigley
Hon. Steve Womack

Hon. Lucille Roybal-Allard

Hon. Chuck Fleischmann

Hon. Tom Cole

Hon. Barbara Lee

Hon. Hal Rogers