Congress of the United States
Washington, DC 20515

The Honorable Patty Murray
Chair
Senate Committee on Appropriations
S-128, The Capitol
Washington, DC 20510

The Honorable Susan Collins
Vice Chair
House Committee on Appropriations
S-128, The Capitol
Washington, DC 20510

March 24, 2023

Dear Chairwoman Murray and Vice Chair Collins:

In March 2020, the Cyberspace Solarium Commission[1] published recommendations for defending the United States in cyberspace. As a result of Congress's determined attention to cybersecurity issues in the intervening three years, more than 80 percent of the Commission's original recommendations have seen significant progress, and almost 60 percent 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 for Fiscal Year 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 recommended budget changes and report language below. For each request, the corresponding Commission recommendation is referenced in *italics*. 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.

[1] https://cybersolarium.org/wp-content/uploads/2022/05/CSC-Final-Report.pdf

Agriculture, Rural Development, Food and Drug Administration, and Related Agencies

- As the 2021 JBS ransomware attack demonstrated, cybersecurity risks to the food and agriculture sector can have far-reaching and highly disruptive effects on American society. As the co-Sector Risk Management Agency for the agricultural sector, the USDA is responsible for coordinating across the sector to address and mitigate these risks. USDA has delegated this responsibility to its Office of Homeland Security, which currently lacks resources specifically appropriated for SRMA activities. Without sufficient funding, OHS will face challenges coordinating its work across a highly distributed and diverse community of agricultural stakeholders, including more than two million farms. Therefore, **we recommend an increase of $750,000 over the administration's request for Food and Agriculture Sector Support within the USDA Office of Homeland Security.**

Commerce, Justice, Science, and Related Agencies

- With tens of thousands of open cybersecurity jobs, the public sector suffers from a significant shortage in its cyber workforce. Cybersecurity personnel also need 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 an SFS school, upon graduation. **We recommend funding for the CyberCorps® program be set at $80 million in Fiscal Year 2024,** $6 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. 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). **In addition, we 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." *(Recommendation 1.5)*

- **Three 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) NIST is at the forefront of our national **research efforts into critical and emerging technologies,** such as artificial intelligence, quantum information science, and next-generation

communications technologies. While such technologies show enormous potential economic, societal, and national security benefits, more research, testing, and measurement of such technologies are required to responsibly deploy or commercialize them. NIST's work is essential in this regard. Moreover, NIST plays a critical role as a leader, coordinator, and participant in international standards development. The data and insights of its research and its close partnerships with industry consortia and other non-federal stakeholders will be essential to maintaining U.S. leadership in international standards development for critical and emerging technologies, especially the deployment of next-generation communications technologies.

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 CHIPS and Science Act has also authorized new lines of effort for NIST in critical cybersecurity areas, such as open-source software security and the design, adoption, and deployment of cloud computing services. NIST must have the means to effectively execute each of these lines of work.

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.

To facilitate hiring scientists, engineers, and subject matter experts who can meet the increasing demands across multiple emerging technologies and to provide the necessary support for those added positions, **we recommend an increase of $40.5 million over the request for NIST Cybersecurity and Privacy portfolio, and we support the $20 million program increase requested in the President's budget for Advancing Research in Critical and Emerging Technologies**. **We further recommend the following report language:**

"*Advancing Research in Critical and Emerging Technologies.*— The Committee recognizes NIST's important research role across areas of critical and emerging technologies. NIST's work to evaluate, measure, and develop standards around such technologies is essential to the responsible and effective deployment of these technologies in commercial and national security environments. This work will only grow in importance through the coming years, particularly as the People's Republic of China redoubles its own efforts to deploy such technologies for its strategic advantage. To that end, the Committee recommends that not less than $20,000,000 be made available for Advancing Research in Critical and Emerging Technologies." *(Recommendation 4.6.2)*

"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: $1,000,000 for vulnerability management, $1,500,000 for cryptography programs, $5,000,000 for privacy programs, $1,500,000 for identity and access management, $3,000,000 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 $3,000,000 for Internet of Things security." *(Recommendation 4.1.2)*

"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 the 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)." *(Recommendation 3.5)*

- 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 the FBI's capacity to work with international partners to counter cyber threat actors abroad, **we support the administration's requested increase of $63.4 million in funding for FBI cyber over FY2023 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, in the U.S. and working at key overseas missions.

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." *(Recommendation 2.1.4)*

- 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, 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 support the requested increase of $11,350,000 for the NCSES and further recommend the following report language:**

  "National Center for Science and Engineering Statistics.—The Committee funds the National Center for Science and Engineering Statistics (NCSES) to the requested level and supports the use of this funding 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." *(Workforce White Paper Recommendation 7)*

- 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 $1.25 million over the administration's 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 $1,250,000 over the request 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." *(Supply Chain White Paper Recommendation 3.1)*

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.[2] **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."

Energy & Water Development

- The Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) leads DOE's efforts to strengthen the cybersecurity and resilience of the energy sector, and carries out the Sector Risk Management Agency responsibilities of the Department. This mandate is all the more essential because the energy sector is designated as a lifeline sector, and as such, a disruption to energy production or delivery could have cascading disruptive consequences on one or more other critical infrastructure sectors. The national and economic security imperatives of its work necessitate that CESER is appropriately resourced for its various lines of effort to understand, mitigate, and respond to cyber and physical risks across the sector. Furthermore, a fully-resourced CESER can serve as a model for other SRMAs, establishing a common baseline of effective performance across government and helping close the maturity gap among SRMAs. **To that end, we support the administration's requested increase to the Office of Cybersecurity, Energy Security, and Emergency Response.**

Financial Services and General Government

- Since its establishment pursuant to Section 1752 of the William M. (Mac) Thornberry National

[2] 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/

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. ONCD led the development of the National Cybersecurity Strategy, and will now play a critical role in finalizing an implementation plan for the Strategy. At the same time, ONCD must also continue its vital work to grow and strengthen America's cyber workforce, and to align cybersecurity budgets and priorities across the federal enterprise. To sustain this critical mission, **we support the President's budget request of $22,586,000 for salaries and expenses at the Office of the National Cyber Director.**

- 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." *(Recommendation 1.5)*

- Supporting the Federal Government's migration towards a **zero trust architecture (ZTA)** is 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 $43,232,000 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 $200 million for the Technology Modernization Fund.**

- 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, 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 on U.S. adversaries put 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 that the Office of Cybersecurity and Critical Infrastructure Protection receive $25 million in FY24,** 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 $25,000,000 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 further improve resilience to cyberattacks by expanding 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, including 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." *(Recommendation 4.6.3)*

Interior, Environment, and Related Agencies

- As the Sector Risk Management Agency for the Water and Wastewater Systems Sector, the Environmental Protection Agency is responsible for coordinating across one of the most diverse, distributed, and resource-constrained critical infrastructure sectors in the United States. The Water and Wastewater Systems Sector's status as a lifeline sector should make EPA's SRMA funding an urgent priority, yet EPA has until now lacked the resources to effectively execute its mission. This lack of funding is severely out of balance with the potential consequences of cybersecurity threats to our drinking water and wastewater; Congress must not miss this opportunity to act. **As such we strongly recommend an increase of $5 million over the FY24 request for the Science and Technology appropriations at the Environmental Protection Agency, together with the following report language:**

  "Sector Risk Management Agency.— The Committee provides $5 million above the request to enhance the Agency's capacity to fulfill its Sector Risk Management Agency obligations and support the cybersecurity of the water and wastewater sector."

Homeland Security

- CISA's proposal for a new Cyber Analytics and Data System represents a significant step forward in the Agency's efforts to enhance partnerships across the cybersecurity ecosystem through timely and effective information sharing. It will operationalize the technical capabilities to analyze and cross-correlate cyber threat indicators at the speed and scale necessary for rapid detection and identification of such threats. This is an essential capability to develop if we are to achieve truly shared situational awareness of cybersecurity risks and cybersecurity threats across the ecosystem. **Accordingly, we strongly support the administration's request of $424,906,000 for a Cyber Analytics and Data Protection System at CISA. We further support the administration's request for the Joint Collaborative Environment PPA.**

- 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)." *(Recommendation 3.2)*

- 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 support the administration's requested increase for Security Advisors within the Regional Operations Activity. We further recommend the following report language**:

  "*Cybersecurity Advisors (CSAs).*— Recognizing CISA's commitment in its Strategic Plan to strengthen its regional presence, the Committee supports the use of funds appropriated 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." *(Recommendation 1.4)*

- 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." *(Recommendation 5.3)*

- 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 that the program be expanded, enabling it to reach more classrooms nationwide, because 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. We also recommend the following report language:

"*Cybersecurity Education and Training Assistance Program (CETAP).*—The Committee 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." *(Recommendation 1.5.1)*

- 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. Congress recognized the value of this program and appropriated $3 million to it in FY23. Yet CISA has marked this program for defunding in its budget request, citing a lack of plans to award grants in FY2024. Given the shortage of cybersecurity talent facing the country, it seems counterproductive to reduce opportunities to incentivize the development of programs that create new pathways into the cyber workforce. As such, we encourage the committee to sustain funding for NTTP grants until CISA provides a clear explanation of its future plans for the program, or if no such plans exist, its intentions to refocus internal efforts to otherwise achieve the intent of the program. **Specifically, we recommend an increase of $3 million above the request to Cyber Defense Education & Training within the Cyber Operations/Capacity Building activity at CISA and the following report language:**

  "Non-Traditional Training Providers.— The Committee rejects the proposed decrease to NTTP grant funding included in the request, and directs CISA to report to the committee not less than 270 days after the date of enactment of this Act on its plans to award future grants to non-traditional training providers, or on its plans to refocus its resources or programming in a manner that sustains the objectives of this grant program."

- Just over one year ago, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). The law requires CISA to develop and implement requirements for covered entities to report covered cyber incidents to CISA. CISA must also develop the technical means to quickly ingest these incident reports and apply their insights to its cyber defense operations. To ensure that this critical legislation is implemented swiftly and effectively, **we support the administration's request of $97,709,000 to carry out the requirements of the Cyber Incident Reporting for Critical Infrastructure Act.**

- The Transportation Security Administration, as co-Sector Risk Management Agency for the Transportation Systems Sector, has critical responsibilities for the cybersecurity and resilience of many transportation subsectors, including the Aviation, Highway and Motor Carrier, Pipeline Systems, Mass Transit and Passenger Rail, Freight Rail, and Postal and Shipping subsectors. TSA requires the resources necessary to fulfill this broad mandate. **As such, we strongly**

support the administration's requested increase of $2,791,000 to the Mission Support PPA and $4,209,000 to the Other Operations and Enforcement PPA for cybersecurity.

- The ransomware attack on the Colonial Pipeline revealed an urgent need to improve the security and resilience of pipeline systems across the United States. TSA has led this mission through the issuance of security directives for pipeline companies, but the Agency requires additional staff to effectively monitor implementation of and compliance with these directives. **To that end, we support the requested increase of $3,385,000 for the annualization of pipeline security staffing.**

- The cybersecurity of the maritime transportation system (MTS) is of critical importance to securely facilitating U.S. and global trade. As the co-Sector Risk Management Agency, the United States Coast Guard is central to federal cybersecurity efforts across the MTS, but it continues to suffer from a shortage of personnel, including cybersecurity personnel. To build a pool of sector-specific cybersecurity expertise of the MTS within the U.S. Coast Guard to ensure that the Service is able to meet its mission needs for the MTS subsector, **we support the administration's requested program increase of $11,978,000 for Workforce Recruiting and Accessions.**

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 foreign disinformation by funding research on improving media literacy, digital civic engagement, and academic outcomes in civics and history, with a particular emphasis on our Constitution and founding documents. **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 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, with a particular emphasis on our Constitution and founding documents; improve the ability of participants to collaborate with others to solve local and global problems; expand awareness of foreign 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." *(Recommendation 3.5)*

- Among the sixteen critical infrastructure sectors, the Healthcare and Public Health Sector is among the most heavily targeted by cyber threat actors. These attacks impact patient care and could even cause loss of life; as such, mitigating cybersecurity risks to the sector is of critical importance. Performing the Department of Health and Human Services' Sector Risk Management Agency responsibilities is the Administration for Strategic Preparedness and Response's Office of Critical Infrastructure Protection (ASPR CIP). HHS reported to GAO that it planned to request $6.5 million in FY2024 to support its SRMA responsibilities.[3] Yet within the President's FY24 budget request, ASPR CIP would share a portion of a $4,222,000 increase, along with two other ASPR readiness programs and activities. By HHS' own reporting to GAO, this increase is insufficient to meet HHS' SRMA needs. Accordingly, **we recommend a $6.5 million increase over FY23 enacted levels for the Administration for Strategic Preparedness and Response and the following report language**:

  "Sector Risk Management Agency.—The Committee notes its significant concerns with cybersecurity threats to the Healthcare and Public Health Sector, and provides $6,500,000 above the request to the Administration for Strategic Preparedness and Response's Office of Critical Infrastructure Protection to support the Department of Health and Human Services' duties as the Sector Risk Management Agency for the Sector." *(Recommendation 3.1)*

State, Foreign Operations, and Related Programs

- The establishment and subsequent codification of the **Bureau of Cyberspace and Digital Policy** (CDP) at the Department of State was a major step forward in the prioritization of international cyberspace policy and diplomacy, which had suffered from bureaucratic and resource constraints in the preceding years. Widespread international engagement, for example on key votes in multilateral organizations, had been hampered by a lack of available personnel. Similarly, programs to reinforce the effectiveness of cyberspace norms had been limited. Congress took the first steps towards addressing these issues by codifying CDP and providing its first appropriations. To build on this momentum and ensure that the State Department's newest bureau is staffed appropriately, **we recommend a $1.5 million dollar increase above the request for the Bureau of Cyberspace and Digital Policy.**

- **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

[3] U.S. Government Accountability Office (2023, February). *Critical Infrastructure Protection: Time Frames to Complete DHS Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities*. (Publication No. GAO-23-105806). Retrieved from: https://www.gao.gov/assets/gao-23-105806.pdf

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 appropriations to four funds that support different aspects of international cybersecurity capacity building *(Recommendation 2.1.3)*:

1) **$10 million increase above the FY24 request 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 influence and aggression.

2) **$18.4 million increase above FY23 enacted levels, in line with the FY24 request, for the International Narcotics Control and Law Enforcement Fund.** This line of funding is critical for countering cybercrime and intellectual property theft. It supports the development and expansion of projects designed to strengthen cooperation among law enforcement and other criminal justice sector professionals on cybercrime issues.

2) **$5 million increase above the FY24 request for the Digital Connectivity and Cybersecurity Partnership** to support the partnership's focus on enhancing cybersecurity.

3) **$15 million increase above the FY24 request 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.*—The Committee supports the use of funding appropriated for the International Narcotics Control and Law Enforcement Fund 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 $39 million be made available to the Bureau of Cyberspace and Digital Policy from ESF for information and communications technology (ICT) and cyber capacity building programming. The request would allocate a further $40.7 million from the International Technology Security and Innovation Fund to Economic Support Fund, to be administered by the Bureau of Cyberspace and Digital Policy in order to promote the development and adoption of secure ICT networks and services **We support these requests, and we further recommend the following language**:

  "*International Cybersecurity Capacity Building.*—The agreement includes requested funding for the Economic Support Fund to be administered by the Bureau of Cyberspace and Digital Policy. The Committee supports the proposed application of ISTI funding for the development of secure and trustworthy information and communications technology. The use of the remaining funds available to the Bureau through the Economic Support Fund shall include international cybersecurity capacity-building efforts that strengthen civilian cybersecurity through support to countries and organizations, including national and regional institutions."

- As countries with less mature information communication technology (ICT) infrastructure race to advance their digital ecosystem, any donor nation offering support may be welcome. China, 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 Chinese-centric 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 support the administration's request of $139,128,000 in Development Assistance Funding 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." *(Supply Chain White Paper Recommendation 5.1)*

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

Sincerely,

ANGUS KING
U.S. Senator

MIKE GALLAGHER
Member of Congress